



सत्यमेव जयते



Test Schedule and Test Procedure (TSTP)

**ITSAR name: Optical Network Terminal
(ONT) - PON family Broadband
Equipment**

ITSAR No: ITSAR403012311

Disclaimer: This TSTP is intended to serve as a guide for testing various clauses outlined in the relevant ITSAR. The test methods described in this TSTP are not exhaustive and should not be considered as the sole approach to test any clause. The actual testing process and results may vary depending on how the OEMs implemented the clause in their equipment.

© रा.सं.सु.कें., २०२५

© NCCS, 2025

MTCTE के तहत जारी:

Issued under MTCTE by:

राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार

सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

National Centre for Communication Security (NCCS)

Department of Telecommunications

Ministry of Communications

Government of India

City Telephone Exchange, SR Nagar, Bangalore-560027, India

Table of Contents

Chapter-2 Common Security Requirements	4
Section 1: Access and Authorization	4
2.1.1 TSTP for Evaluation of Management Protocols Mutual Authentication.....	4
2.1.2 TSTP for Evaluation of Management Traffic Protection	12
2.1.3 TSTP for Evaluation of Role-Based access control	39
2.1.4 TSTP for Evaluation of User Authentication – Local and Remote	43
2.1.5 TSTP for Evaluation of Remote login restrictions for privileged users.....	47
2.1.6 TSTP for Evaluation of Unambiguous identification of the user & group accounts removal	50
Section 2: Authentication Attribute Management	56
2.2.1 TSTP for Evaluation of Authentication Policy	56
2.2.2 TSTP for Evaluation of Authentication support - External	60
2.2.3 TSTP for Evaluation of Protection against brute force and dictionary attacks.....	63
2.2.4 TSTP for Evaluation of Enforce Strong Password	70
2.2.5 TSTP for Evaluation of Inactive Session Timeout	74
2.2.6 TSTP for Evaluation of Password Changes	78
2.2.7 TSTP for Evaluation of Protected Authentication feedback.....	84
2.2.8 TSTP for Evaluation of Removal of predefined or default authentication attributes	94
Section 3: Software Security	100
2.3.1 TSTP for Evaluation of Secure Update.....	100
2.3.2 TSTP for Evaluation of Secure Upgrade.....	112
2.3.3 TSTP for Evaluation of Source code security assurance.....	124
2.3.4 TSTP for Evaluation of Known Malware and backdoor Check	128
2.3.5 TSTP for Evaluation of No Unused software	132
2.3.6 TSTP for Evaluation of Insecure Services/protocol Removal	137
2.3.7 TSTP for Evaluation of Restricting System Boot Source	150
2.3.8 TSTP for Evaluation of Secure Time Synchronization.....	156
2.3.9 TSTP for Evaluation of Restricted reachability of services	162
2.3.10 TSTP for Evaluation of Avoidance of Unspecified Mode of Access.....	171
Section 4: System Secure Execution Environment.....	175
2.4.1 TSTP for Evaluation of No unused functions.....	175
2.4.2 TSTP for Evaluation of No unsupported components.....	181
Section 5: User Audit	186
2.5.1 TSTP for Audit Event Generation	186
2.5.2 TSTP Evaluation for Secure Log Export.	213

Section 6: Data Protection	224
2.6.1 TSTP for Evaluation of Cryptographic Based Secure Communication with connecting entities	224
2.6.2 TSTP for Evaluation of Cryptographic Module Security Assurance.....	230
2.6.3 TSTP for Evaluation of Cryptographic Algorithms implementation Security Assurance	233
2.6.4 TSTP for Evaluation of Protecting data and information – Confidential System Internal Data	235
2.6.5 TSTP For Protecting data and information in storage	240
2.6.6 TSTP Report for Protection against Copy of Data	247
2.6.7 TSTP Report for Protection against Data Exfiltration - Overt Channel.....	252
2.6.8 TSTP Report for Protection against Data Exfiltration - Covert Channel	255
Section 7: Network Services	259
2.7.1 TSTP for Evaluation of Traffic Separation	259
2.7.2 TSTP Evaluation for Traffic Filtering – Network Level Requirement	263
2.7.3 TSTP for Evaluation Traffic Protection –Anti-Spoofing.....	276
Section 8: Attack Prevention Mechanisms.....	281
2.8.1 TSTP For Network Level and application-level DDoS.....	281
2.8.2 TSTP for Excessive Overload Protection.....	289
Section 9: Vulnerability Testing Requirements	297
2.9.1 TSTP for Evaluation of Fuzzing – Network and Application Level	297
2.9.2 TSTP for Evaluation of Port Scanning	306
2.9.3 TSTP for Evaluation of Vulnerability Scanning	312
Section 10: Operating System	318
2.10.1 TSTP Report for Evaluation Handling of ICMP	318
2.10.2 TSTP for Authentic Privilege Escalation Only	323
2.10.3 TSTP for System account identification.....	327
2.10.4 TSTP Report for Evaluation OS-Hardening	330
2.10.5 TSTP Report for Evaluation No automatic launch of removable media	333
2.10.6 TSTP Report for Evaluation Protection from buffer overflows	336
2.10.7 TSTP Report for External file system mount restrictions	339
2.10.8 TSTP Report for File-system Authorization privileges.....	343
Section 11: Web Servers	349
2.11.1 TSTP Evaluation for HTTP	349
2.11.2 TSTP for Evaluation of Web Server Logging	356
2.11.3 TSTP Report for Evaluation	363

2.11.4 TSTP for Evaluation No unused HTTPS methods	371
2.11.5 TSTP Report for Evaluation No unused add-ons	377
2.11.6 TSTP for Evaluation of No compiler, interpreter, or shell via CGI or other server-side scripting.....	383
2.11.7 TSTP for Evaluation of No CGI or other scripting for uploads.....	388
2.11.8 TSTP for Evaluation of No execution of system commands with SSI	393
2.11.9 TSTP for Evaluation of Access rights for web server configuration	398
2.11.10 TSTP for Evaluation of No Default Content	404
2.11.11 TSTP for Evaluation of No directory listings	409
2.11.12 TSTP for Evaluation of Web Server information in HTTPS headers	414
2.11.13 TSTP for Evaluation of Web server information in error pages	419
2.11.14 TSTP for Minimized file type mappings (not there in Wi Fi)	425
2.11.15 TSTP for Evaluation of Restricted file access.....	430
2.11.16 TSTP for Execute rights exclusive for CGI/Scripting directory	438
Section 12: Other Security requirements	445
2.12.1 TSTP for Evaluation of No System / Root Password Recovery	445
2.12.2 TSTP for Evaluation of Secure System Software Revocation.....	452
2.12.3 TSTP for Evaluation of Software Integrity Check – Boot	457
2.12.4 TSTP for Evaluation of Unused Physical and Logical Interfaces Disabling	462
2.12.5 TSTP for Evaluation of No Default Profile	468
Section 13 Specific Requirement	477
2.13.1 TSTL Report for Evaluation Registration with ONT	477
2.13.2 TSTL Report for Evaluation Secure data Communication on wireless media (Ex: Wi-Fi) for ONT	486
2.13.3 TSTP for Evaluation of MAC address filtering	491
2.13.4 Configuration and management of ONTs (Using OMCI/TR69 protocols)	495
2.13.5 TSTP for IGMP Filter	504
2.13.6 TSTP Evaluation for SSID Scanning	509
2.13.7 TSTP for Password Change for User Facility	520
2.13.8 TSTP for Evaluation of Key exchange mechanism	529
2.13.9 TSTP for Evaluation of of Rogue detection	538

Chapter-2 Common Security Requirements

Section 1: Access and Authorization

2.1.1 TSTP for Evaluation of Management Protocols Mutual Authentication

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.1.1
--	--------------------------	-----------------

<DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

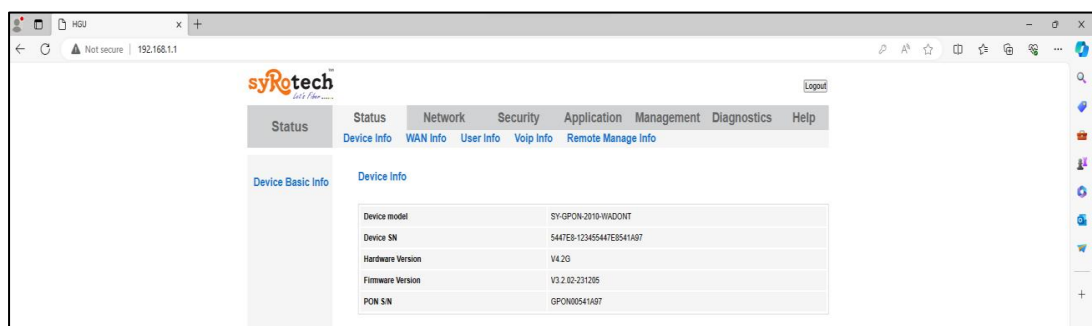
<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.1: Access and Authorization
2. **<Security Requirement No & Name >** 2.1.1: Management Protocol Mutual Authentication
3. **<Requirement Description:>** The protocols used for the ONU/ONT management and maintenance shall support mutual authentication mechanisms only Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” shall only be used for ONU/ONT management and maintenance.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. section 4.2.3.4.4.1]

4. DUT Confirmation Details:



5. DUT Configuration:

Configure SSH, HTTP/HTTPS, TACACS+, SNMP v3 and SFTP on Management Interface of DUT.

a) HTTP Configuration

- i. The Tester connects the DUT through LAN port and visits the default ip of the DUT which is `http://192.168.1.1`
- ii. verifies that no additional configuration is required to access the DUT as HTTP/HTTPS is pre-configured on the DUT.
- iii. HTTP secure server cipher suite specifies the encryption algorithm and digest algorithm to use on an SSL connection. Web browsers offer a list of supported cipher suite when connecting to the HTTPS server, and the client and server will negotiate the best encryption algorithm to use from those that are supported by both.

b) HTTPS Configuration

- i. The Tester connects the DUT through LAN port and visits the default ip of the DUT which is `https://192.168.1.1`
- ii. verifies that no additional configuration is required to access the DUT as HTTPS is pre-configured on the DUT.
- iii. For OLT configuration - Configure performance management settings on the OLT from PC2

6. Pre-Condition: Documentation that lists each of the management protocols supported by DUT and describes the authentication mechanism used for each one.

7. Test Objective: To check if the DUT supports mutual authentication for the supported management protocols

8. Test Plan

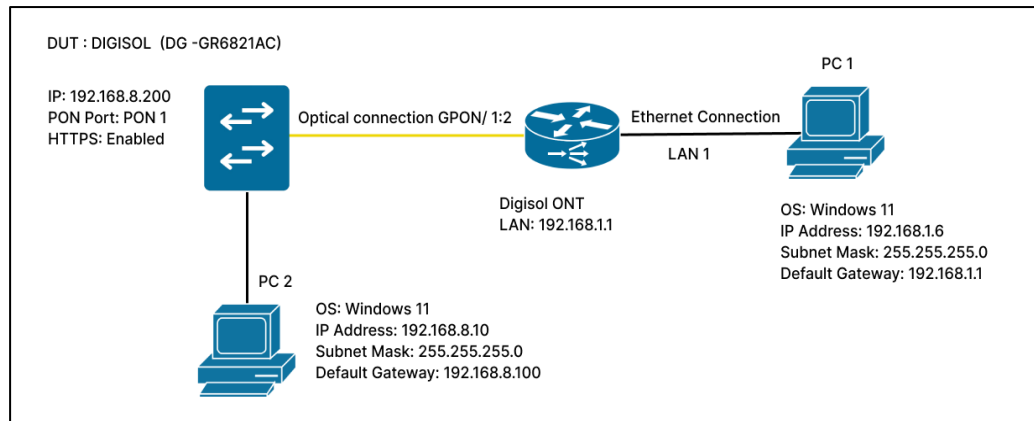
8.1 Number of Test Scenarios: 3

8.1.1 **Test Case 01:** Physical verification of available Interfaces & supported management protocols on DUT.

8.1.2 **Test case 02:** Establish connection between the Test machine and DUT using configured mutual authentication method for both positive and negative scenarios.

8.1.3 **Test case 03:** Ensure mutual authentication between ONT and OLT.

8.2 Test-bed diagram:



8.3 Tools required:

- i. Wireshark
- ii. Zenmap
- iii. GUI

8.4 Test Execution steps

- i. The tester shall attempt to access the DUT with configured management protocols
- ii. The Tester shall verify if mutual authentication exists between DUT and Test Machine for each management protocol supported by the DUT.
- iii. Tester shall verify the mutual authentication between OLT and ONT.

9. Expected Results for Pass: -

- i. The DUT and the tester machine shall mutually authenticate each other for all the management protocols supported by the DUT.
- ii. ONT and OLT should also support mutual authentication.

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test case Name:** Management protocol verification

11.1.2 **Test Case Description:** Physical verification of available Interfaces & supported management protocol on DUT using zenmap.

11.1.3 **Execution Steps:**

- i. The Tester should verify all the available physical interfaces on DUT and cross verify with OEM Documentation (below are front and side view of the DUT).



Fig: Front and side view of ONT

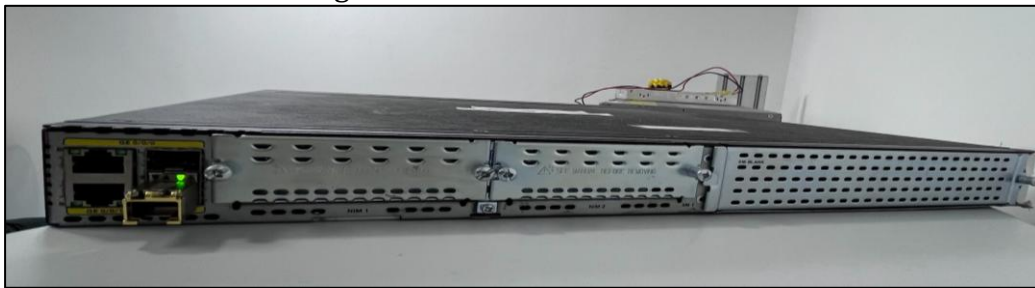
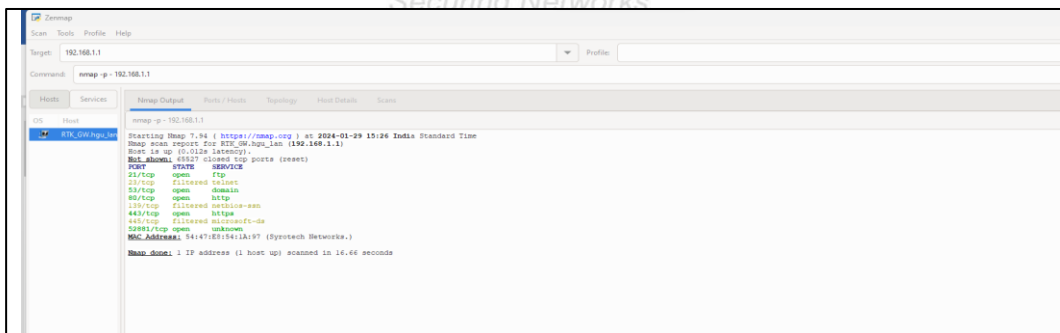


Fig: Rear view of OLT

ii. The Tester makes note of all management protocols supported by DUT in document provided by OEM and also verifies using zenmap

- » SSH
- » SSL/TLS
- » SNMP v3
- » HTTP/HTTPS
- » Telnet



11.2 Test Case Number: 02

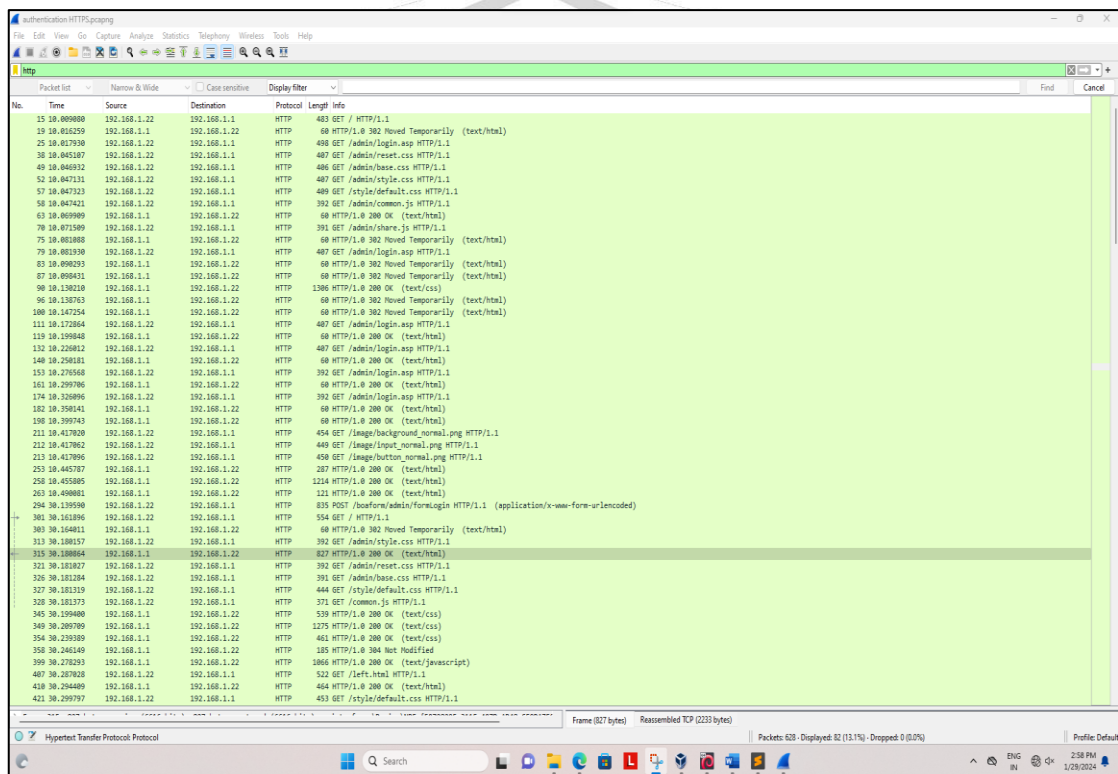
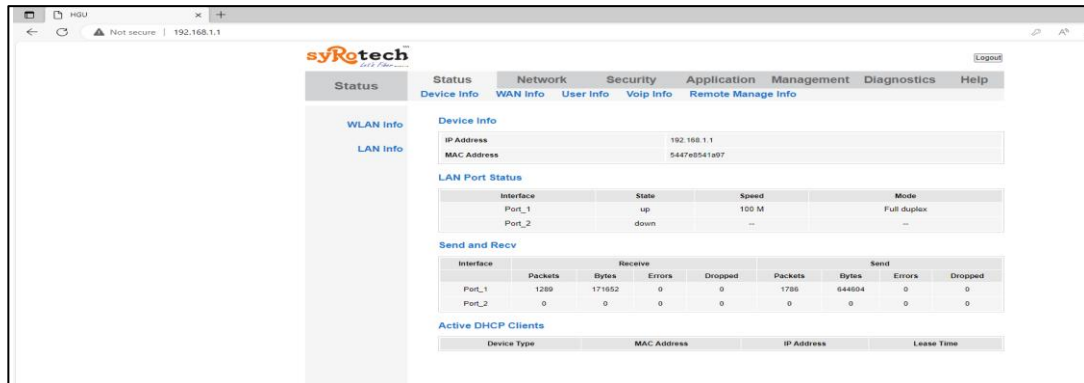
11.2.1 **Test case Name:** Mutual authentication for the configured management protocols

11.2.2 **Test Case Description:** Testing mutual authentication for the configured management protocols

11.2.3 **Execution Steps:**

a) HTTP Configuration:

- i. The tester opens the DUT's Web GUI (<http://192.168.1.1/>) in web browser of the test machine (192.168.1.22) and capture traffic between DUT and test machine in Wireshark to verify the mutual authentication between both the entities.



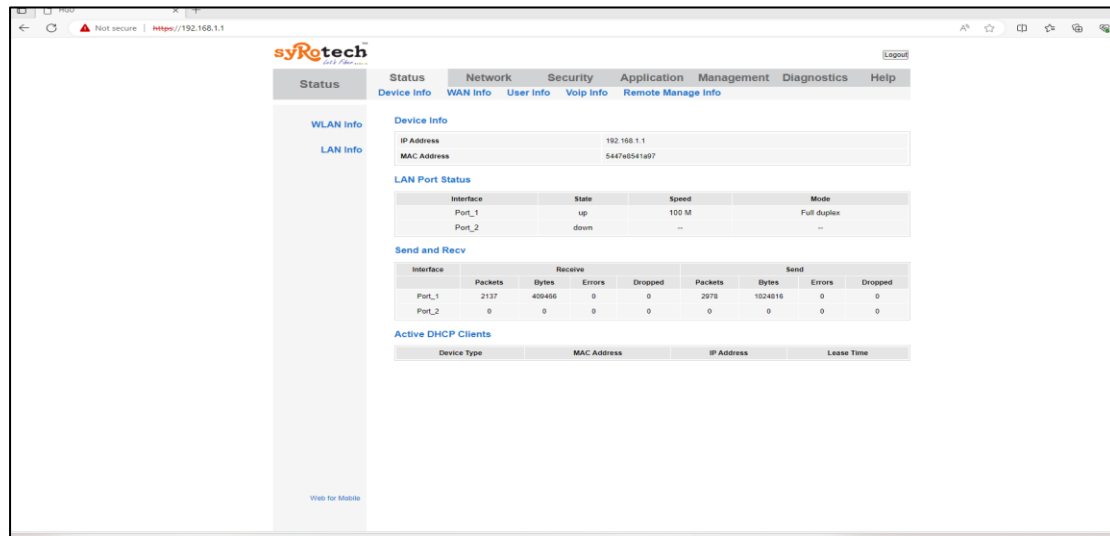
- ii. The tester observed that there is no mutual authentication between DUT and Test machine but the connection is established successfully.

b) HTTPS Configuration:

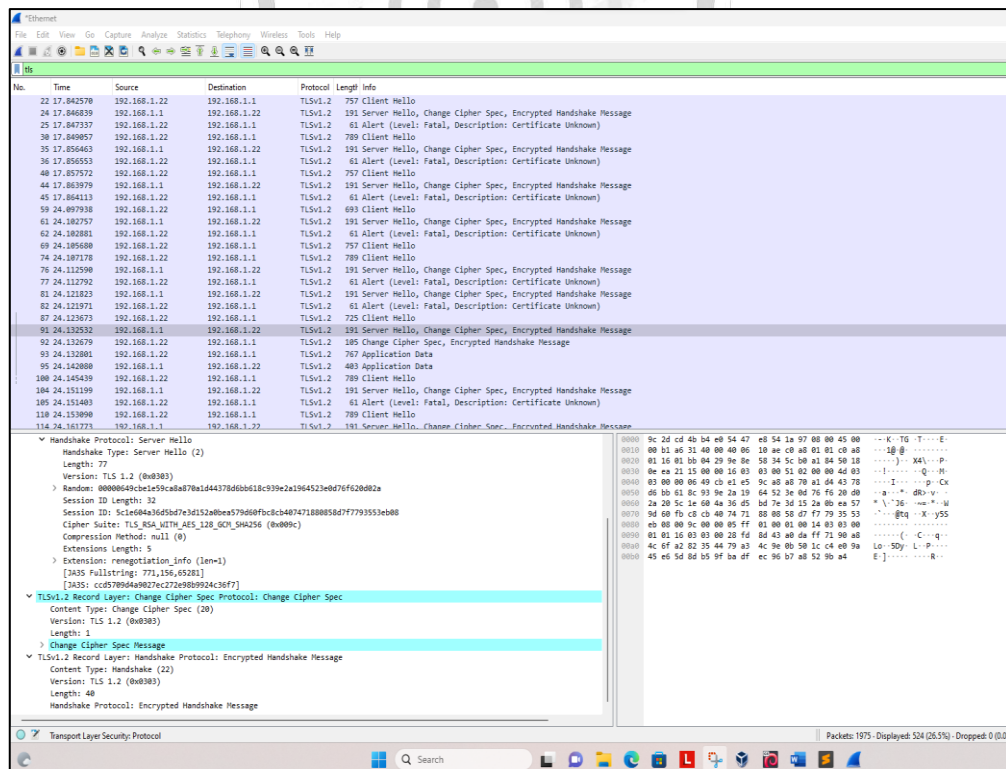
- i. Tester connects the DUT through LAN port and visits the default ip of the DUT which is <https://192.168.1.1>

HTTP secure server cipher suite specifies the encryption algorithm and digest algorithm to be used for an SSL connection. Web browsers offer a list of supported cipher suite when connecting to the HTTPS server, and the

client and server will negotiate the best encryption algorithm to use from those that are supported by both.

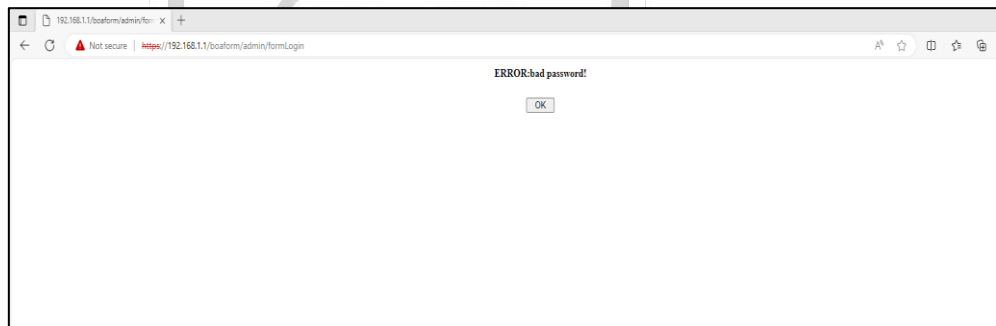


- ii. The tester opens the DUT's Web GUI (<http://192.168.1.1/>) in web browser of the test machine (192.168.1.22) and captured traffic between DUT and test machine in Wireshark to verify the mutual authentication between both the entities.



- iii. The tester observed that there is no mutual authentication between DUT and Test machine but the connection is established successfully. In Wireshark, can see Server and client exchanging the keys between each other but that cannot be considered mutual authentication.

- iv. To test the negative test case scenario (can only be tested from client side as server side doesn't offer any identity verification to the client), tester supplies the wrong password and observe the response of DUT.



- v. If the DUT supports Telnet: connect to the DUT using the telnet command
<screenshot connecting to DUT using telnet>

Check if there's mutual authentication using TELNET

- Upon entering the password, we get the access to the ONT
- Capture the same on wireshark
<wireshark screenshot>
- Observe if there is mutual authentication using TELNET

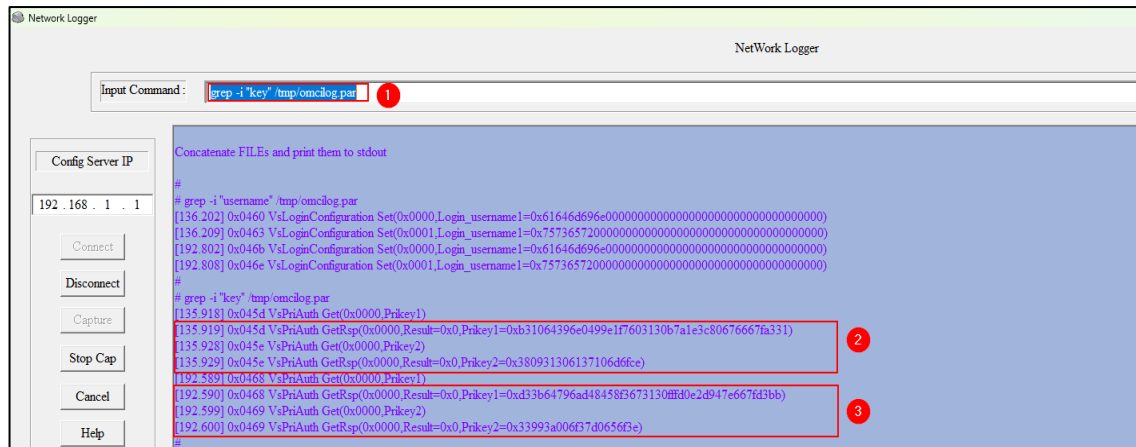
11.3 Test Case Number: 3

11.3.1 **Test case Name:** Mutual Authentication between ONT and OLT

11.3.2 **Test Case Description:** The tester verifies the mutual authentication between ONT and OLT

11.3.3 **Execution Steps**

- The OLT authenticates the ONT** by retrieving **Prikey1** and **Prikey2**, while the ONT authenticates the OLT, it's not showing in the log OEM need to provide.



- ii. Communication between OLT and ACS server running in PC2 can also be captured in wireshark to check if the encryption used is according to the Crypto control or not

11.3.4 Test Observations:

- i. **Test case01:** The tester verifies the available protocols using zenmap and verifies using OEM documentation
- ii. **Test case02:** The tester observed that there was no mutual authentication present when attempting to connect to client using HTTP and HTTPs.
- iii. **Test case03:** Tester observed that mutual authentication is taking place between ONT and OLT

11.3.5 Evidence Provided: Screenshots are attached above

12. Test Case Results:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Management protocol verification		
2	Mutual authentication for the configured management protocols		
3	Mutual Authentication between ONT and OLT		

2.1.2 TSTP for Evaluation of Management Traffic Protection

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.1.2
---	--------------------------	-----------------

<DUT Details: > **GPON-ONT**

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

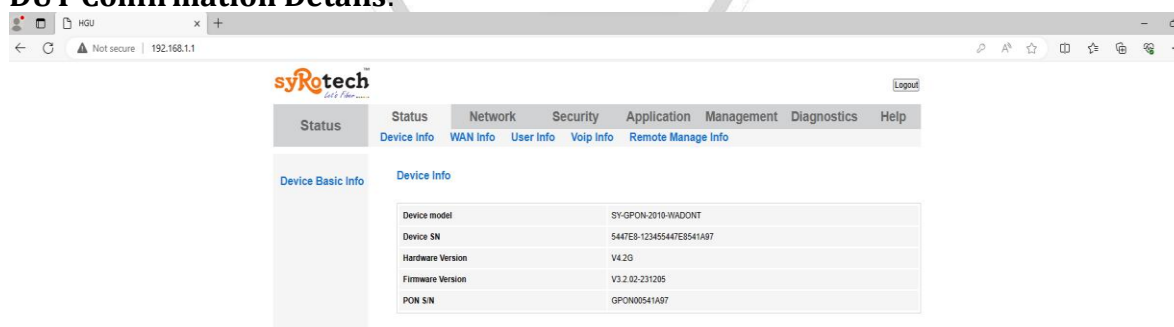
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.1: Access and Authorization
2. **<Security Requirement No & Name >** 2.1.2: Management Traffic Protection
3. **<Requirement Description:>** ONT management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.4]

4. DUT Confirmation Details:



5. **DUT Configuration:** Configure the DUT to enable the supported management protocols if needed
6. **Pre-Condition:**
 - i. Network product documentation containing information about supported OAM protocols provided by OEM.
 - ii. A peer implementing the security protocol configured by the OEM (e.g., SSH client supporting SSHv2 or HTTPS client) shall be available.
 - iii. For TLS, the tester shall base the tests on the profile defined by 3GPP in TS 33.310. For IKE and IPsec, the tester shall base the tests on the profile defined by 3GPP in TS 33.210. For protocols, for which 3GPP did not define a security profile, e.g., SSH, the

tester shall base the tests on a widely recognized and publicly available security profile.

7. **Test Objective:** To verify that DUT communicates with management entities using secure ciphers as per table 1 of cryptographic controls ITSAR.

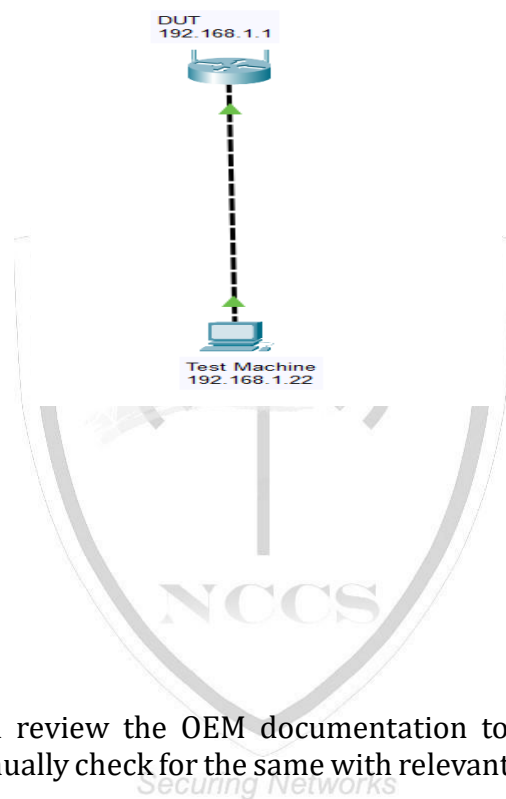
8. **Test Plan**

8.1 Number of Test Scenarios:2

8.1.1 **Test case01:** Secure cipher verification

8.1.2 **Test case02:** Weak cipher / null cipher test case

8.2 Test-bed Diagram:



8.3 Tools required:

- i. Wireshark
- ii. Zenmap
- iii. GUI
- iv. testssl

8.4 Test Execution

- i. The tester shall review the OEM documentation to check for the supported ciphers and manually check for the same with relevant commands for the ciphers supported
- ii. The DUT shall be accessed by the tester for all the supported management protocols and also capture the session on wireshark
- iii. The wireshark pcap file will be inspected to check for the supported ciphers used in the traffic between the DUT and test machine

9. **Expected Results for Pass:** - The DUT should support secure ciphers in accordance with the crypto controls in communication with the test machine

10. **Expected Format of Evidence:** Screenshots, pcap files

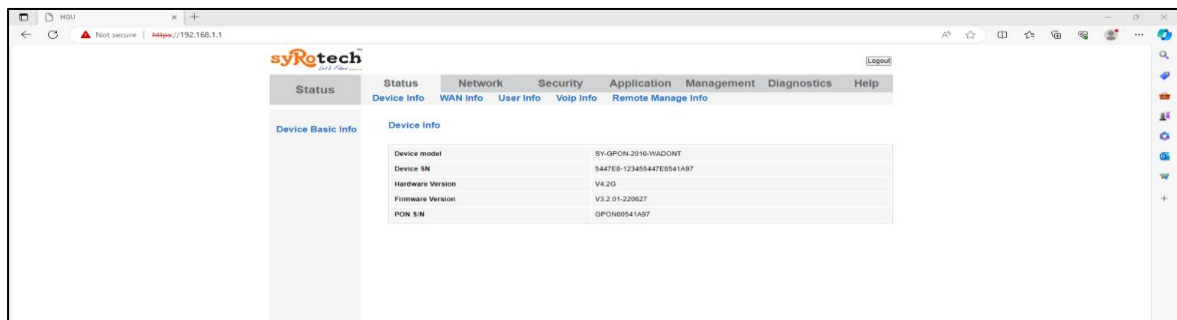
11. **Test Execution:**

11.1 **Test Case Number:** 1

11.1.1 **Test case Name:** Review the OEM documentation.

11.1.2 **Test Case Description:** Check the OEM document describing the secure communication services/protocols supported on the DUT, details of Crypto

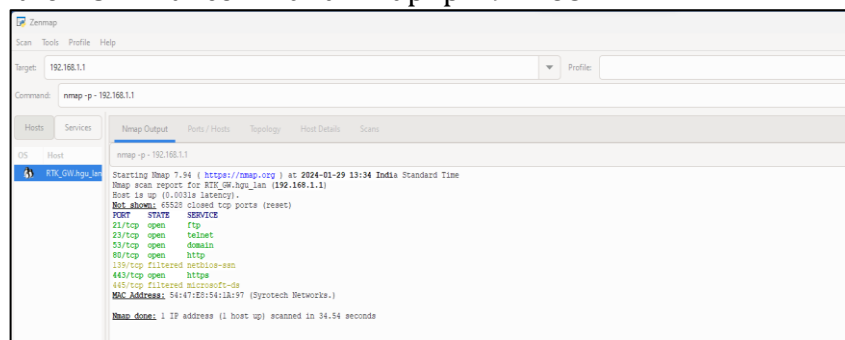
modules used, Cryptographic protocols and algorithms, command to verify



the related configuration in the DUT.

11.1.3 Execution Steps:

- i. Tester checks the supported protocols on the DUT by running nmap on the DUT with command `nmap -p-192.168.1.1`



- ii. The tester shall review the OEM documentation and verify if the ciphers supported by DUT are in compliance with cryptographic controls ITSAR.

11.2 Test Case Number: 2

11.2.1 Test case Name: Secure cipher verification

11.2.2 **Test Case Description:** Verify the traffic between DUT and test machine through HTTPS, HTTP and Telnet is exchanged using secure ciphers as per the cryptographic controls ITSAR.

11.2.3 Execution Steps:

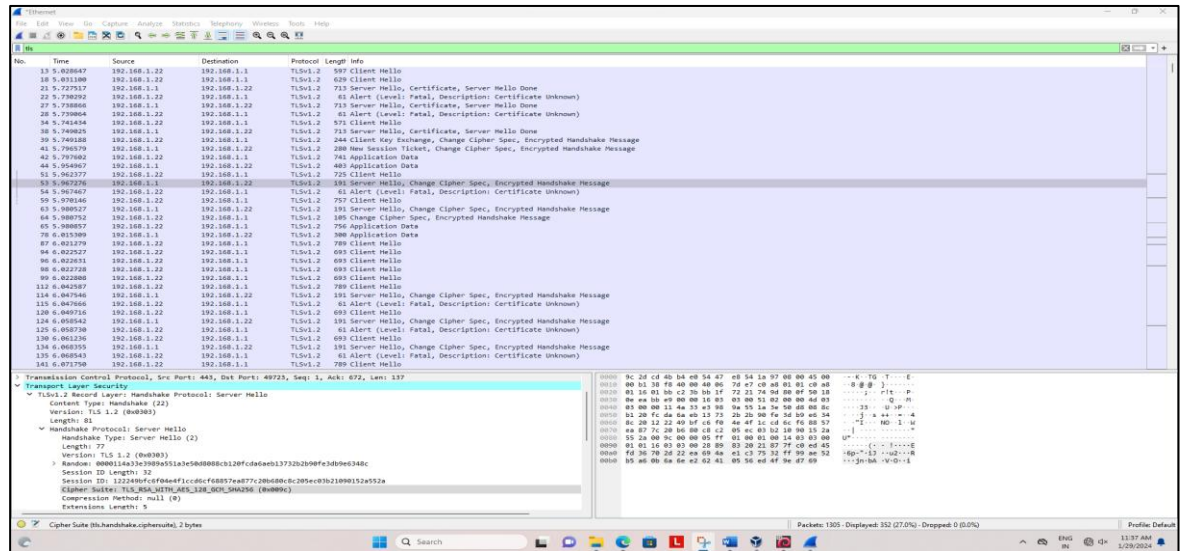
a) HTTPS:

- i. Tester opens web browser in test machine (192.168.1.22) to connect DUT (<https://192.168.1.1/>) through TLS v1.2 protocol.
- ii. Tester attempts to login DUT using “admin” account. The Tester created a “admin” account on DUT.
- iii. Tester enters the correct password and reach to DUT’s web browser.
- iv. Tester attempt to access the DUT and captured the network traffic between DUT and Test machine in Wireshark.
- v. Tester can verify the ciphers supported by DUT for HTTPS traffic using `./testssl.sh https://<DUT IP>` command

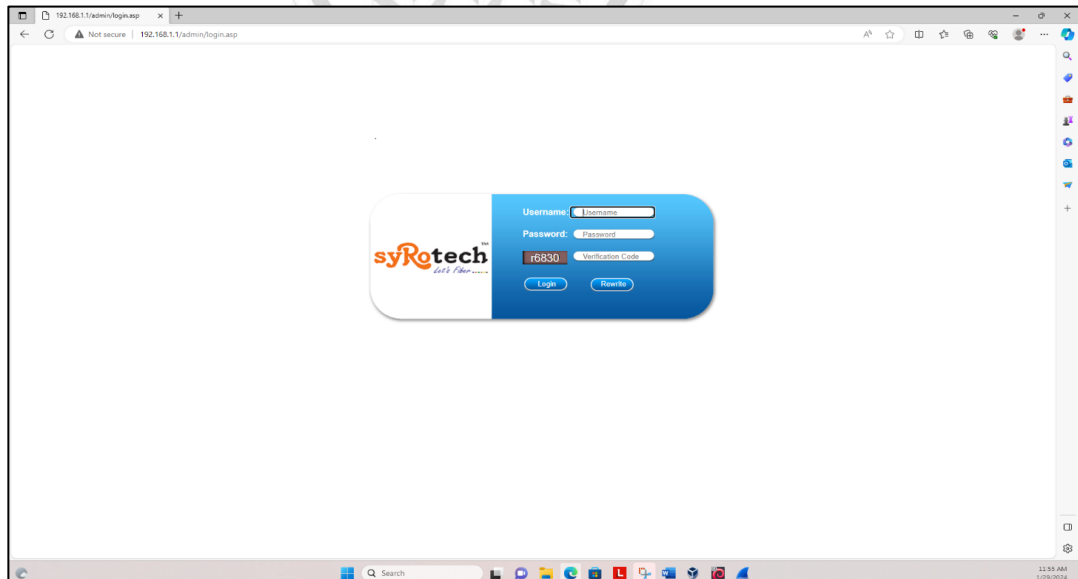
- vi. Tester should analyse the Wireshark output and observe that traffic is going in encrypted format on TLS v1.2 protocol.
- vii. Verify the mechanisms implemented to protect data and information in transfer to and from the DUT.

b) HTTP

- i. The Tester opens web browser in test machine (192.168.1.22) to connect DUT (http://192.168.1.1/) through http protocol.
- ii. The Tester attempts to login DUT using “admin” account. The Tester created a “admin” account on DUT.
- iii. The Tester enters correct password and reach to DUT’s web browser.



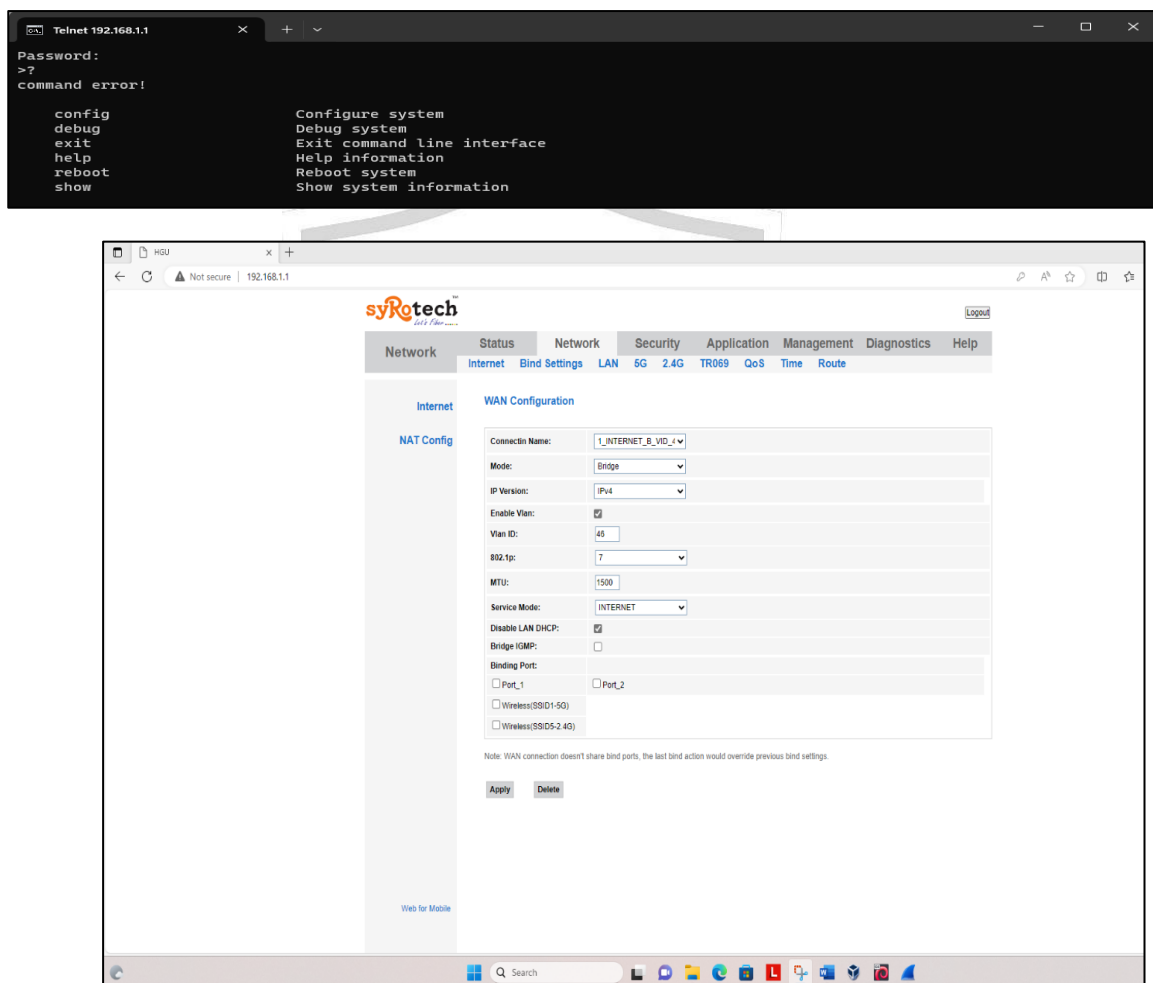
- iv. The Tester should attempt to access the DUT and captured the network traffic between DUT and Test machine in Wireshark.



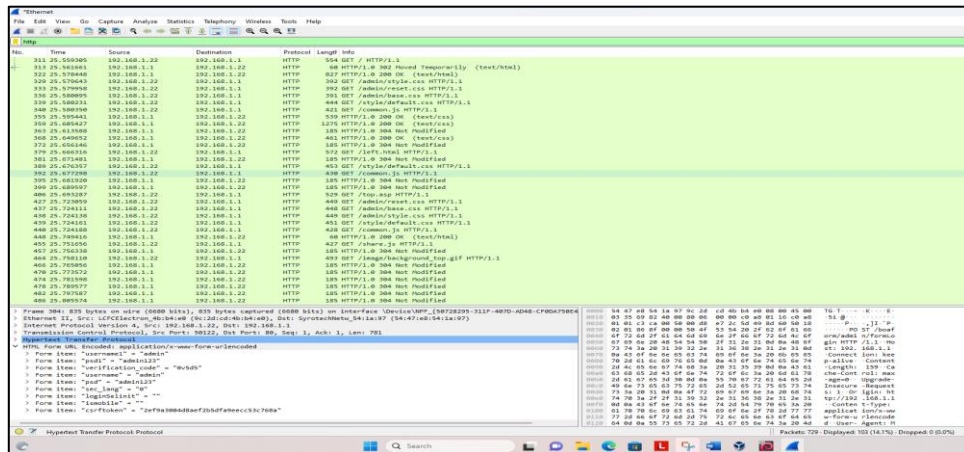
- v. Tester should analyse the Wireshark output and observe that traffic is going in encrypted format on TLS v1.2 protocol.
- vi. It is observed that the traffic to and from the device is not protected with secure ciphers.

c) Telnet

- i. Telnet is not enabled by default in the DUT, tester enables/configures the telnet protocol.
- ii. The Tester opens command line interface in test machine (192.168.1.22) to connect DUT (http://192.168.1.1/) through telnet protocol.
- iii. The Tester logs in with the correct credentials of the “admin” user to access the DUT via telnet.



- iv. The Tester attempt to access the DUT and captured the network traffic between DUT and Test machine in Wireshark.



- v. The Tester Verified that there are no mechanisms implemented to protect data in transfer to and from the DUT and it can be seen in the clear text.

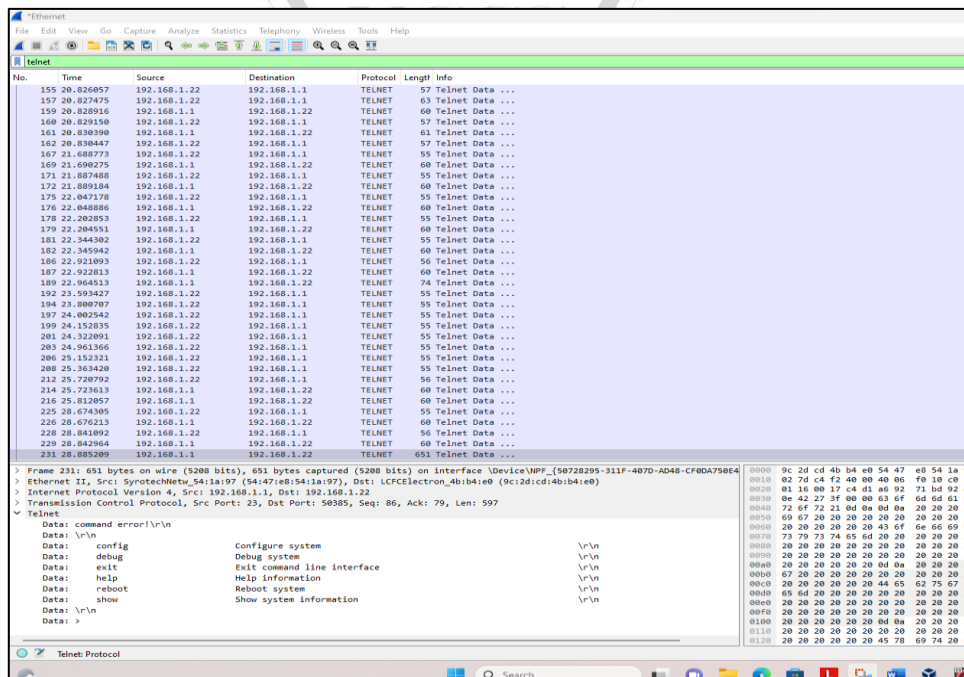
11.3 Test Case Number: 03

11.3.1 Test case Name: Weak cipher/ null cipher verification

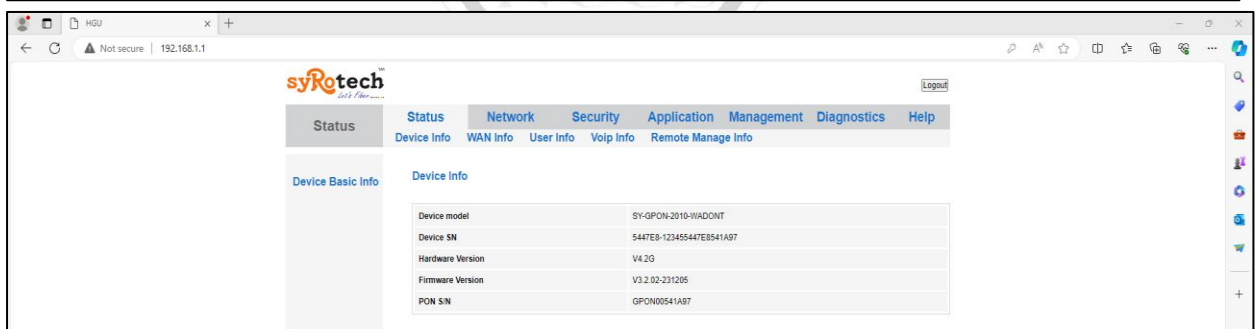
11.3.2 Test Case Description: Verify that the traffic between DUT and Test machine is not with null or weak ciphers.

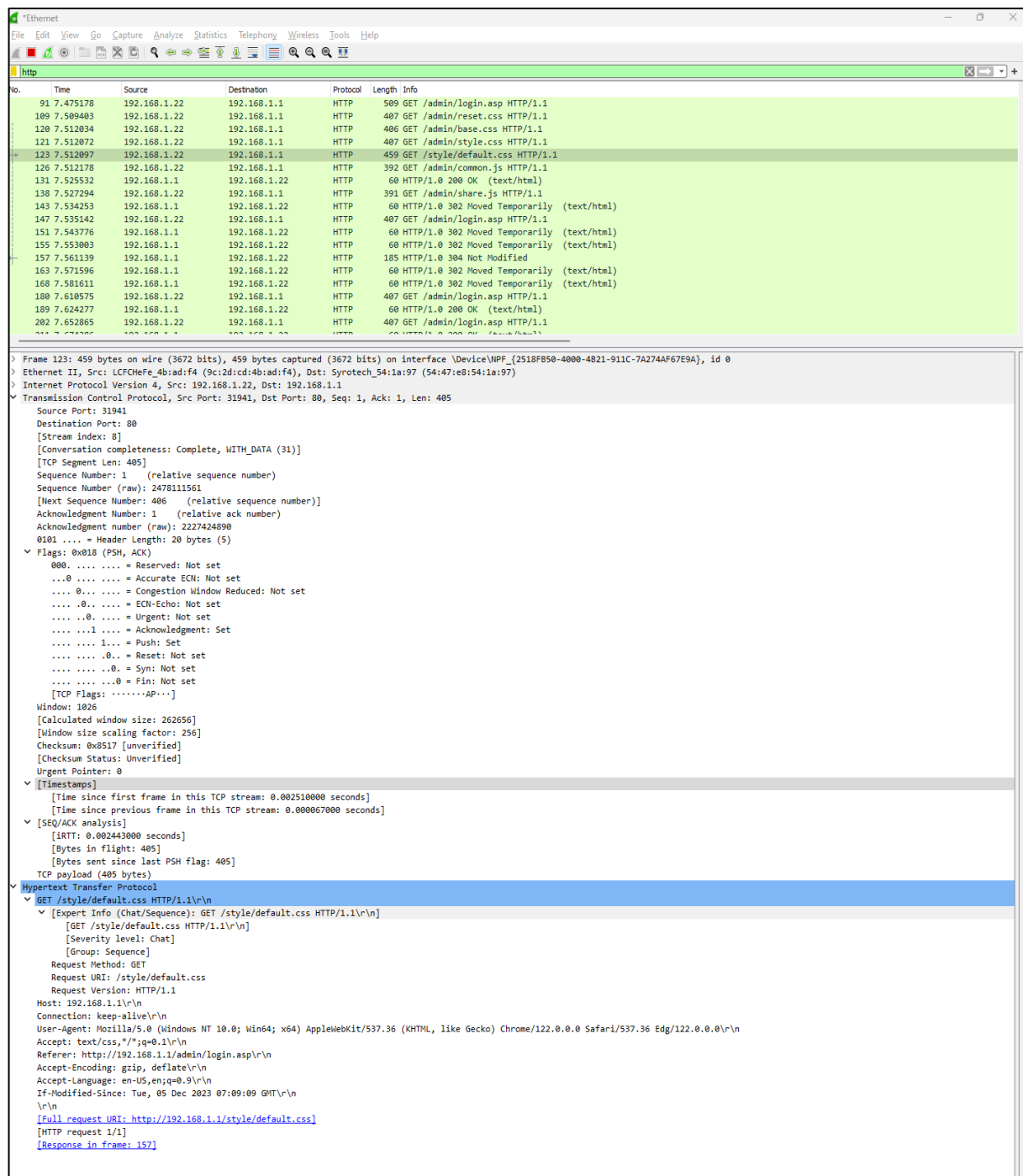
11.3.3 Execution Steps:

- To get full cipher suite supported by DUT, the Tester should use a suitable tool (such as testssl.sh) for automated discovery of supported Ciphers for TLS/SSL protocols.
- The Tester runs the testssl.sh <https://192.168.1.1> through Kali Linux - 192.168.217.128 virtually hosted on Test machine (192.168.1.22) and captured the response.



- ii. The Tester attempts to login DUT using “admin” account. The Tester created a “admin” account on DUT.
- iii. The Tester supplies the correct password and reach to DUT’s web browser.
- iv. The Tester attempt to access the DUT and captured the network traffic between DUT and Test machine in Wireshark.

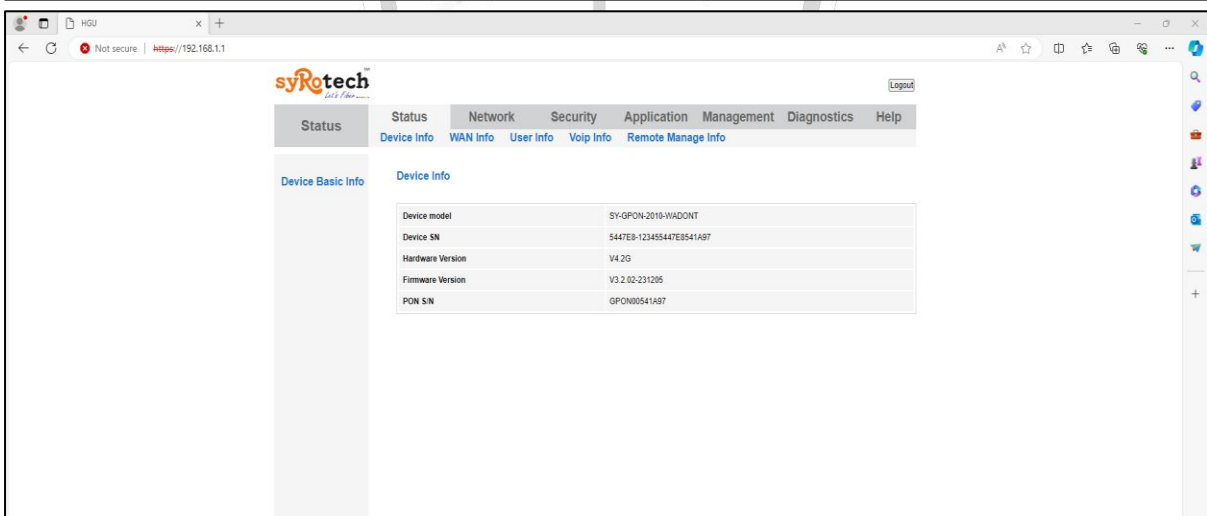




v. The Tester analysed the Wireshark output and observed that traffic is going in encrypted format on TLS v1.2 protocol.

b) HTTPS:

- The Tester opens web browser in test machine (192.168.1.22) to connect DUT (https://192.168.1.1/) through TLS v1.2 protocol.
- The Tester attempts to login DUT using “admin” account. The Tester created a “admin” account on DUT.
- The Tester supplies the correct password and reach to DUT’s web browser.
- The Tester attempt to access the DUT and captured the network traffic between DUT and Test machine in Wireshark.



- v. The Tester analysed the Wireshark output and observed that traffic is going in encrypted format on TLS v1.2 protocol.

Capturing from Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Current filter: !s						
No.	Time	Source	Destination	Protocol	Length	Info
39	15.829152	192.168.1.22	192.168.1.1	TLsv1.2	757	Client Hello
41	15.832045	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
42	15.832171	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
48	15.835305	192.168.1.22	192.168.1.1	TLsv1.2	789	Client Hello
52	15.836411	192.168.1.22	192.168.1.1	TLsv1.2	757	Client Hello
56	15.844623	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
57	15.844812	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
61	15.853997	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
62	15.854143	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
67	15.855535	192.168.1.22	192.168.1.1	TLsv1.2	725	Client Hello
71	15.865183	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
72	15.865342	192.168.1.22	192.168.1.1	TLsv1.2	105	Change Cipher Spec, Encrypted Handshake Message
73	15.865496	192.168.1.22	192.168.1.1	TLsv1.2	1120	Application Data
75	15.895740	192.168.1.1	192.168.1.22	TLsv1.2	373	Application Data
82	15.903033	192.168.1.22	192.168.1.1	TLsv1.2	693	Client Hello
84	15.906986	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
85	15.907222	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
90	15.909757	192.168.1.22	192.168.1.1	TLsv1.2	789	Client Hello
94	15.918043	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
95	15.918227	192.168.1.22	192.168.1.1	TLsv1.2	105	Change Cipher Spec, Encrypted Handshake Message
96	15.918369	192.168.1.22	192.168.1.1	TLsv1.2	832	Application Data
98	15.932276	192.168.1.1	192.168.1.22	TCP	1514	443 → 64492 [ACK] Seq=138 Ack=1565 Win=32232 Len=1460 [TCP segment of a reassembled PDU]
99	15.932276	192.168.1.1	192.168.1.22	TLsv1.2	1066	Application Data
113	15.941644	192.168.1.22	192.168.1.1	TLsv1.2	693	Client Hello
114	15.941789	192.168.1.22	192.168.1.1	TLsv1.2	725	Client Hello
121	15.942537	192.168.1.22	192.168.1.1	TLsv1.2	789	Client Hello
122	15.942660	192.168.1.22	192.168.1.1	TLsv1.2	693	Client Hello
123	15.942759	192.168.1.22	192.168.1.1	TLsv1.2	757	Client Hello
129	15.945797	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
130	15.945858	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
137	15.953410	192.168.1.22	192.168.1.1	TLsv1.2	725	Client Hello
139	15.956408	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
140	15.956507	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
145	15.958517	192.168.1.22	192.168.1.1	TLsv1.2	757	Client Hello
149	15.967468	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
150	15.967614	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
155	15.969407	192.168.1.22	192.168.1.1	TLsv1	693	Client Hello
159	15.978035	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
160	15.978138	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
165	15.979761	192.168.1.22	192.168.1.1	TLsv1	757	Client Hello
169	15.989065	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
170	15.990029	192.168.1.22	192.168.1.1	TLsv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
176	15.992127	192.168.1.22	192.168.1.1	TLsv1	757	Client Hello
180	16.000459	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
181	16.000682	192.168.1.22	192.168.1.1	TLsv1.2	105	Change Cipher Spec, Encrypted Handshake Message
182	16.000865	192.168.1.22	192.168.1.1	TLsv1.2	635	Application Data
185	16.014474	192.168.1.1	192.168.1.22	TLsv1.2	1304	Application Data
189	16.021442	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
190	16.021714	192.168.1.22	192.168.1.1	TLsv1.2	105	Change Cipher Spec, Encrypted Handshake Message
191	16.021919	192.168.1.22	192.168.1.1	TLsv1.2	634	Application Data
194	16.035917	192.168.1.1	192.168.1.22	TCP	1514	443 → 64499 [ACK] Seq=138 Ack=1335 Win=32016 Len=1460 [TCP segment of a reassembled PDU]
195	16.035917	192.168.1.1	192.168.1.22	TLsv1.2	490	Application Data
200	16.042459	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
201	16.042714	192.168.1.22	192.168.1.1	TLsv1.2	105	Change Cipher Spec, Encrypted Handshake Message
202	16.042902	192.168.1.22	192.168.1.1	TLsv1.2	687	Application Data
205	16.053621	192.168.1.1	192.168.1.22	TLsv1.2	214	Application Data
209	16.059962	192.168.1.1	192.168.1.22	TLsv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
210	16.060246	192.168.1.22	192.168.1.1	TLsv1.2	105	Change Cipher Spec, Encrypted Handshake Message
211	16.060465	192.168.1.22	192.168.1.1	TLsv1.2	635	Application Data
214	16.074892	192.168.1.1	192.168.1.22	TCP	1514	443 → 64501 [ACK] Seq=138 Ack=1336 Win=32016 Len=1460 [TCP segment of a reassembled PDU]
217	16.074992	192.168.1.1	192.168.1.22	TLsv1.2	1259	Application Data
218	16.079368	192.168.1.1	192.168.1.22	TCP	1514	443 → 64501 [ACK] Seq=4263 Ack=1336 Win=32016 Len=1460 [TCP segment of a reassembled PDU]

Frame 41: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface \Device\NPF_{2518F850-4000-4821-911C-7A274AF67E9A}, id 0

Ethernet II, Src: Syrotech_54:1e:97 (54:47:e8:54:1e:97), Dst: LcChFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.22

Transmission Control Protocol, Src Port: 443, Dst Port: 64487, Seq: 1, Ack: 704, Len: 137

Transport Layer Security

TLsv1.2 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 81

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 77

Version: TLS 1.2 (0x0303)

Random: 00003cad1908427b21c3502836098999947b6578dec1ed62145d42bb76dc4422

GMT Unix Time: Jan 1, 1970 09:48:53.000000000 India Standard Time

Random Bytes: 1908427b21c3502836098999947b6578dec1ed62145d42bb76dc4422

Session ID Length: 32

Session ID: 8306ee4424c63bf12b314a5c15e413bb5ab9fbd39131395049844d3e395123f5

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Compression Method: null (0)

Extensions Length: 5

Extension: renegotiation_info (len=1)

Type: renegotiation_info (65281)

Length: 1

Renegotiation Info extension

Renegotiation info extension length: 0

JA3S Fullstring: 771,156,65281

JA3S: ccd5709d4a9027ec272e98b9924c36f7

TLsv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

Content Type: Change Cipher Spec (20)

Version: TLS 1.2 (0x0303)

Length: 1

Change Cipher Spec Message

[Expert Info (Note/Sequence): This session reuses previously negotiated keys (Session resumption)]

TLsv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

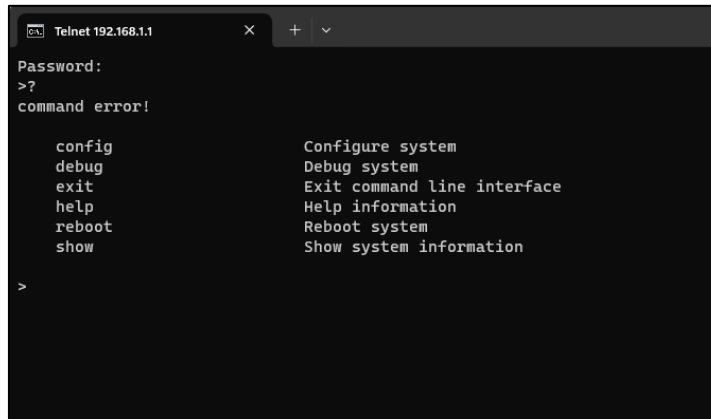
Length: 40

Handshake Protocol: Encrypted Handshake Message

vi. The Tester Verified the mechanisms implemented to protect data and information in transfer to and from the DUT.

c) Telnet:

- i. Telnet is not enabled by default, tester enables/configures the telnet protocol.
- ii. The Tester opens command line interface in test machine (192.168.1.22) to connect DUT (http://192.168.1.1/) through telnet protocol.
- iii. The Tester logs in with the correct credentials of the “admin” user to access the DUT via telnet.



```
Telnet 192.168.1.1
Password:
>?
command error!

config          Configure system
debug           Debug system
exit            Exit command line interface
help            Help information
reboot          Reboot system
show            Show system information

>
```

- iv. The Tester attempt to access the DUT and captured the network traffic between DUT and Test machine in Wireshark.

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.090250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.092164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

Frame 596: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518F850-4000-4E...}

Ethernet II, Src: LCFChEFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 59, Ack: 53, Len: 1

Telnet

Data: a

0000 54 47 e8 54 1a 97 9c 2d cd 4b ad f4 08 00 45 00 TG-T....K....E

0010 00 29 7c f0 40 00 08 06 00 00 c0 a8 01 16 c0 a8 .)|@.....

0020 01 01 7c ee 00 17 16 40 d5 e5 da 29 a3 9f 50 18 ..|...@....)-P

0030 04 02 83 83 00 00 61a

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 603: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518FB50-4000-4E...}

> Ethernet II, Src: LCFChEFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 60, Ack: 54, Len: 1

▼ Telnet

Data: d

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 08 00 45 00  T6:T...K...E
0010  00 29 7c f2 40 00 00 06  00 00 c0 a8 01 16 c0 a8  .)|@.....
0020  01 01 7c ee 00 17 16 40  d5 e6 da 29 a3 a0 50 18  ..|...@...P
0030  04 02 83 83 00 00 64

```

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.240993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 610: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518FB50-4000-4E60-8000-000000000000} on 0

> Ethernet II, Src: LcFCHEFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 61, Ack: 55, Len: 1

▼ Telnet

Data: m

```

0000  54 47 e8 54 1a 97 9c 2d cd 4b ad f4 08 00 45 00  TG-T...K...E
0010  00 29 7c f4 4b 00 80 06 00 00 c0 a8 01 16 c0 a8  .)|@.....
0020  01 01 7c ee 00 17 16 40 d5 e7 da 29 a3 a1 50 18  ..|...@...)-P-
0030  04 02 83 83 00 00 6d                                .....m

```

Securing Networks

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 615: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518F850-4000-46...}

> Ethernet II, Src: LCFHeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 62, Ack: 56, Len: 1

▼ Telnet

Data: i

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 08 00 45 00  TG-T....K....E
0010  00 29 7c f6 40 00 80 06  00 00 c0 a8 01 16 c0 a8  .)|@.....
0020  01 01 7c ee 00 17 16 40  d5 e8 da 29 a3 a2 50 18  ..|...@...P
0030  04 02 83 83 00 00 69      ....i
  
```

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626289	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.240993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 620: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518F850-4000-4E...}

> Ethernet II, Src: LCF0HeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 63, Ack: 57, Len: 1

▼ Telnet

Data: n

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 08 00 45 00  TG-T...-K...E-
0010  00 29 7c f8 40 00 80 06  00 00 c9 a8 01 16 c0 a8  }|@.....
0020  01 01 7c ee 00 17 16 40  d5 e9 da 29 a3 a3 50 18  ...@...)-P-
0030  04 02 83 83 00 00 6e      .....n

```


12-pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934188	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433388	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626289	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 655: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518FB50-4000-4000-8000-000000000000} on 192.168.1.1

> Ethernet II, Src: LFC0MeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 66, Ack: 80, Len: 1

✓ Telnet
Data: A

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 08 00 45 00  TG-T....K...E
0010  00 29 7c fd 40 00 80 06  00 00 c0 a8 01 16 c0 a8  ..|@.....
0020  01 01 7c ee 00 17 16 40  d5 ec da 29 a3 ba 50 18  ..[...@...)-P
0030  04 02 83 83 00 00 41          .....A

```

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296862	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 661: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518F850-4000-46...}

> Ethernet II, Src: LCFHeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 67, Ack: 80, Len: 1

▼ Telnet

Data: d

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 08 00 45 00  TG: T... .K...E...
0010  00 29 7c fe 40 00 80 06  00 00 c0 a8 01 16 c0 a8  .)|@.....
0020  01 01 7c ee 00 17 16 40  d5 ed da 29 a3 ba 50 18  ...@...P...
0030  04 02 83 83 00 00 64      .....d

```

Securing Networks

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 690: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518F850-4000-41E0-B000-000000000000} on interface 0

Ethernet II, Src: LCFChEfe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

Transmission Control Protocol, Src Port: 31902, Dst Port: 23, Seq: 68, Ack: 80, Len: 1

Telnet

Data: m

0000 54 47 e8 54 1a 97 9c 2d cd 4b ad f4 00 00 45 00 Tg: T... -K...E

0010 00 29 7c ff 40 00 00 06 00 00 c0 a8 01 16 c0 a8 :)|@... ..

0020 01 01 7c ee 00 17 16 40 d5 ee da 29 a3 ba 50 18 :|...@...)-P

0030 04 02 83 83 00 00 6d :...m

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 692: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518FB50-4000-4000-0000-00000000} (0:0:0:0:0:0) on interface 0

> Ethernet II, Src: LCFHeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 69, Ack: 80, Len: 1

▼ Telnet

Data: i

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 00 00 45 00  TG-T...-K...E-
0010  00 29 7d 00 40 00 80 06  00 00 c0 a8 01 16 c0 a8  .}}@.....
0020  01 01 7c ee 00 17 16 40  d5 ef da 29 a3 ba 50 18  .|...@...)-P-
0030  04 02 83 00 00 69

```

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626289	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 696: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF{2518FB50-4000-4000-0000-0000} (0:0:0:0:0:0)

> Ethernet II, Src: LCFHeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 70, Ack: 80, Len: 1

▼ Telnet

Data: n

```

0000 54 47 e8 54 1a 97 9c 2d cd 4b ad f4 08 00 45 00 TG-T-----K-----E
0010 00 29 7d 01 40 00 80 06 00 00 c0 a8 01 16 c0 a8 .)}@-----
0020 01 01 7c ee 00 17 16 40 d5 f0 da 29 a3 ba 50 18 ..|....@....P-
0030 04 02 83 83 00 00 6e .....n

```

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 701: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518FB50-4000-4000-0000-00000000} on 0:00:00:00:00:00

> Ethernet II, Src: LCFChFe4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 71, Ack: 80, Len: 1

▼ Telnet

Data: @

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 08 00 45 00  TG-T...-K...E
0010  00 29 7d 02 40 00 80 06  00 00 c0 a8 01 16 c0 a8  })@+.....
0020  01 01 7c ee 00 17 16 40  d5 f1 da 29 a3 ba 50 18  ..|...@....P
0030  04 02 83 83 00 00 40      .....@
  
```

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.583657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.825722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.827078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.296062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 708: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518FB50-4000-4...}

> Ethernet II, Src: LCFCHeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 72, Ack: 80, Len: 1

✓ Telnet

Data: 1

```

0000 54 47 e8 54 1a 97 9c 2d cd 4b ad f4 08 00 45 00  TG-T...-K...E-
0010 00 29 7d 03 40 00 00 06 00 00 c0 a8 01 16 c0 a8  })@.....
0020 01 01 7c ee 00 17 16 40 d5 f2 da 29 a3 ba 50 18  -[...@...)-P-
0030 04 02 83 83 00 00 31                               .....1

```

12.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
555	45.760384	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
556	45.760484	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
558	45.761191	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
559	45.761273	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
562	45.802428	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
563	45.803369	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
564	45.803544	192.168.1.22	192.168.1.1	TELNET	60	Telnet Data ...
566	45.841889	192.168.1.22	192.168.1.1	TELNET	64	Telnet Data ...
569	45.930610	192.168.1.1	192.168.1.22	TELNET	66	Telnet Data ...
571	45.930969	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
573	45.932877	192.168.1.22	192.168.1.1	TELNET	63	Telnet Data ...
575	45.933760	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
576	45.934108	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
577	45.934817	192.168.1.1	192.168.1.22	TELNET	61	Telnet Data ...
578	45.934886	192.168.1.22	192.168.1.1	TELNET	57	Telnet Data ...
596	47.890250	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
598	47.892164	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
603	48.096389	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
604	48.097525	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
610	48.337896	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
611	48.339283	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
615	48.433308	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
616	48.434369	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
620	48.626209	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
621	48.627414	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
635	50.040172	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
636	50.041394	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
638	50.092914	192.168.1.1	192.168.1.22	TELNET	74	Telnet Data ...
655	51.504004	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
661	51.921403	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
690	52.273494	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
692	52.378874	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
696	52.513923	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
701	52.930041	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
708	53.153618	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
712	53.353838	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
715	53.503657	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
723	54.032929	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
725	54.034552	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
729	54.126360	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
787	58.625722	192.168.1.22	192.168.1.1	TELNET	55	Telnet Data ...
788	58.627078	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
796	59.248993	192.168.1.22	192.168.1.1	TELNET	56	Telnet Data ...
797	59.250265	192.168.1.1	192.168.1.22	TELNET	60	Telnet Data ...
799	59.290062	192.168.1.1	192.168.1.22	TELNET	651	Telnet Data ...

> Frame 712: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{2518FB50-4000-4...}

> Ethernet II, Src: LCFHeFe_4b:ad:f4 (9c:2d:cd:4b:ad:f4), Dst: Syrotech_54:1a:97 (54:47:e8:54:1a:97)

> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 192.168.1.1

> Transmission Control Protocol, Src Port: 31982, Dst Port: 23, Seq: 73, Ack: 80, Len: 1

▼ Telnet

Data: 2

```

0000  54 47 e8 54 1a 97 9c 2d  cd 4b ad f4 08 00 45 00  TG-T...-K...E-
0010  00 29 7d 04 40 00 80 06  00 00 c0 a8 01 16 c0 a8  ..}}.....
0020  01 01 7c ee 00 17 16 40  d5 f3 da 29 a3 ba 50 18  ...|...@...-P-
0030  04 02 83 83 00 00 32

```


The image shows a Wireshark packet capture of Telnet traffic. The top pane displays a list of 799 packets, all of which are Telnet data. The bottom pane shows the details of frame 799, which is a Telnet command 'Data: command error!\r\n'. The packet bytes pane shows the raw data of the frame, which is a Telnet command 'Data: command error!\r\n'.

- v. The Tester Verified that there are no mechanisms implemented to protect data in transfer to and from the DUT and the username & password can be seen in the clear text.

11.3.4 TSTP Observation:

- Test case01:** The tester shall review the OEM documentation and verify if the ciphers supported by DUT **are** in compliance with cryptographic controls
- Test case02:** The Tester Verified in HTTPS the mechanisms implemented to protect data and information in transfer to and from the DUT. The Tester Verified in HTTP and Telnet there is no mechanisms implemented to protect data and information in transfer to and from the DUT.

iii. **Test case03:** DUT doesn't support encryption in HTTP/HTTPS/Telnet management protocols.

11.3.5 **Evidence Provided:** Screenshots are attached above

12. Test results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the OEM documentation		
2	Secure cipher verification		
3	Mutual Authentication between ONT and OLT		



2.1.3 TSTP for Evaluation of Role-Based access control

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.1.3
---	--------------------------	-----------------

DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

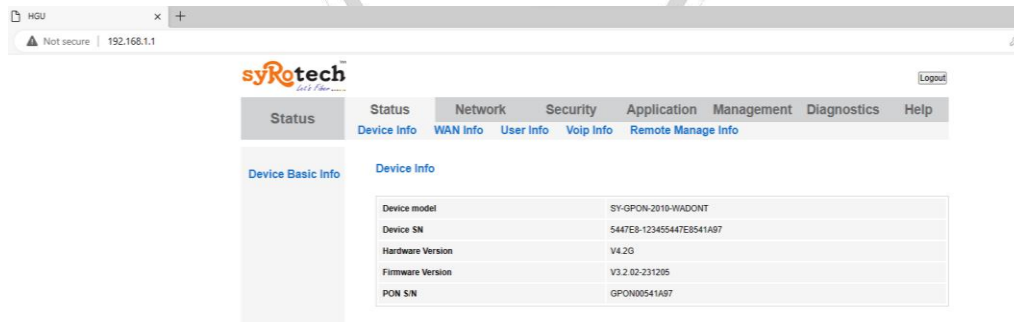
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **ITSAR Section No & Name> Section 1.1: Access and Authorization**
2. **Security Requirement No & Name > 2.1.3: Role-Based Access Control**
3. **<Requirement Description:>** ONU/ONT shall support Role-Based Access Control (RBAC) which provides at least three different access levels or domains to guarantee that individuals can only perform the operations that they are authorized for. The RBAC system controls how users are allowed access to the various domains and what type of operations.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.2]

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.
6. **Pre-Condition:** Documentation describing the role-based access control system including details on which user roles are defined.
7. **Test Objective:** To verify the RBAC supported by the DUT
8. **Test Plan**
 - 8.1 Number of Test Scenarios:
 - 8.1.1 Review the OEM documentation for the user roles supported by the DUT of different privileges

8.1.2 Creation of 3 user IDs with different privileges.

8.2 Test-bed Diagram:



8.3 **Tools required:** GUI or CLI

8.4 **Test Execution**

- i. The Tester shall review the OEM documentation for the user roles supported by the DUT
- ii. The Tester shall create user accounts for these roles
- iii. The tester shall check for the privileges for each user role

9. **Expected Result for Pass:** - The DUT supports at least 3 user roles with different privileges

10. **Expected Format of Evidence:** screenshots

11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test case Name:** Review the OEM documentation for user roles

11.1.2 **Test Case Description:** Review the OEM documentation for user roles with different privileges and verify that minimum 3 user roles exist

11.1.3 **Execution Steps:**

- i. Review the OEM documentation for user roles with different privileges and verify that minimum 3 user roles exist

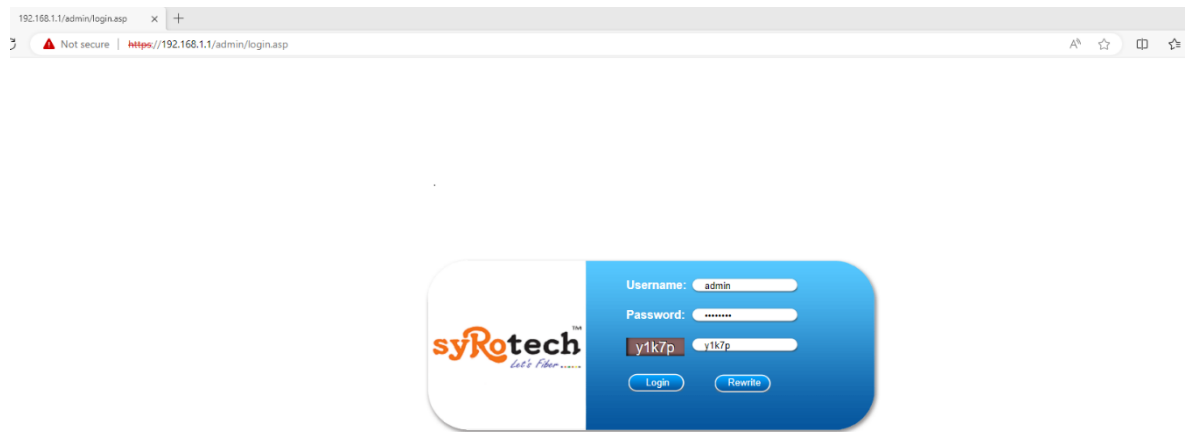
11.2 **Test Case Number:**02

11.2.1 **Test case Name:** Creation of 3 user IDs with different privileges.

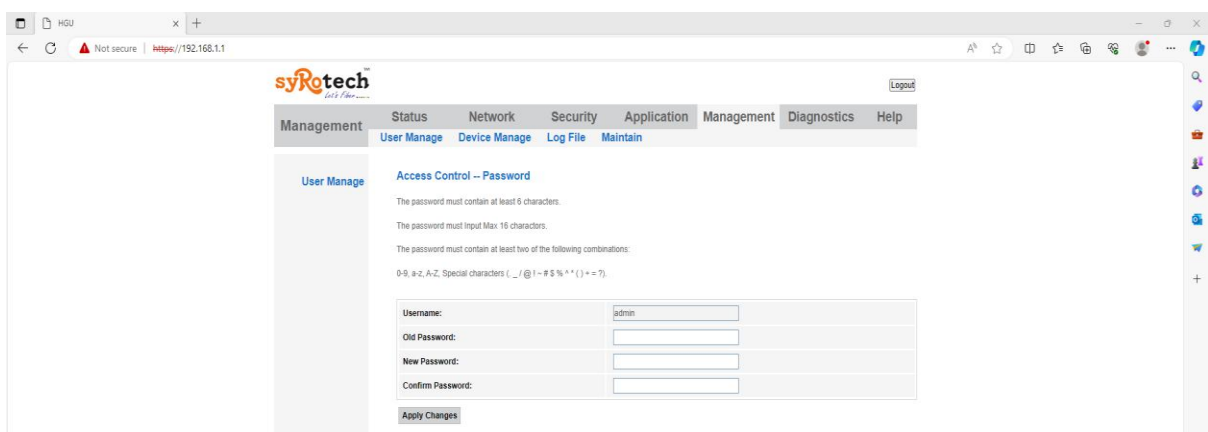
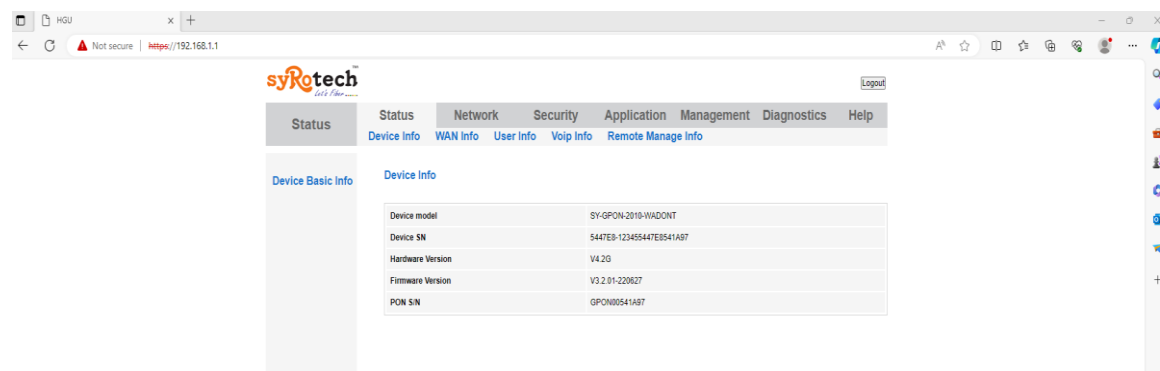
11.2.2 **Test Case Description:** Creation of 3 user IDs with different privileges.

11.2.3 **Execution Steps:**

- i. The Tester logged in to DUT through https with default admin privileged user.



- ii. Tester navigates to the management tab and selects the user management option.



- iii. The Tester observes that DUT supports only single user configuration, in this test case “admin” is the only and default user and its username can’t be modified.
- iv. The Tester also observed that there is no option to assign the privilege to the pre-configured user “admin”.
- **Note:** DUT comes with a pre-configured or a default user name “admin” and tester do not have any option to change the username or privilege level. This DUT does not provide the CLI access also.

11.2.4 **Test Observation:** Tester observed that DUT does not support the role-based access control and there is not option the create or delete the users.

11.2.5 **Evidence Provided:** Screenshots are attached above

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the OEM documentation for the user roles supported by the DUT of different privileges		
2	Creation of 3 user IDs with different privileges.		



2.1.4 TSTP for Evaluation of User Authentication – Local and Remote

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.1.4
---	--------------------------	-----------------

DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

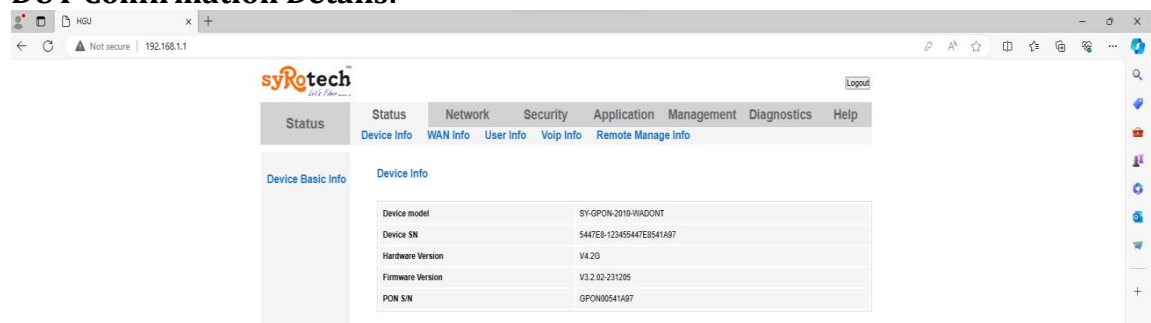
<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.1: Access and Authorization
2. **<Security Requirement No & Name>** 2.1.4: User Authentication – Local/Remote
3. **Requirement Description:** Local and Remote access to the ONU/ONT for configuration and maintenance purposes shall be granted only to authenticated users or machines using at least one authentication attribute. This authentication attribute when combined with the username shall enable unambiguous authentication and identification of the authorized user. No methods to exist providing authentication-bypass attacks to succeed under all combinations of interface / methods of authentication.
 - i. **Local access:** The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from ONU/ONT local hardware interface.
 - ii. **Remote access:** The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.

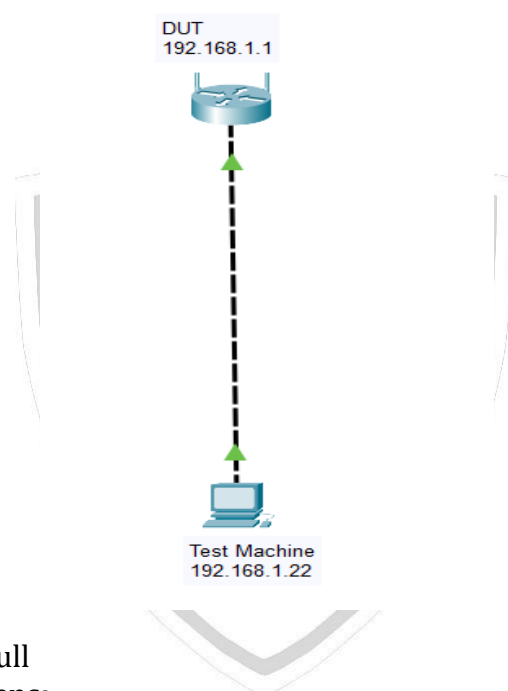
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. Section 4.2.3.4.2.1]

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.

6. **Pre-Condition:** OEM shall documentation stating the supported access methods into DUT
7. **Test Objective:** To verify that minimum two of the above authentication attributes shall be mandatorily combined for protecting all the accounts from misuse and for local access and machine accounts, at least one authentication attribute shall be supported
8. **Test Plan**
 - 8.1 Number of test scenarios:
 - 8.1.1. Remote/local access authentication
 - 8.1.2. Bypass authentication.
 - 8.2 Test bed Diagram:



- 8.3 Tools required: null
- 8.4 Test Execution steps:
 - i. The tester shall access the DUT with the configured access modes
 - ii. The tester shall check if there is at least one authentication before DUT is accessed
 - iii. the tester shall also attempt password bypass authentication attack on DUT
9. **Expected Result for pass**
 - i. The DUT should authenticate the user on at least one authentication attribute
 - ii. The DUT shouldn't let authentication bypass
10. **Expected format of evidence:** Screenshot of Terminal
11. **Test Execution:**
 - 11.1 **Test Case Number: 01**
 - 11.1.1.1 **Test case Name:** Test scenario for Remote/local access authentication
 - 11.1.1.2 **Test Case Description:** The Tester shall attempt to access the DUT to identify the authentication for remote and local access

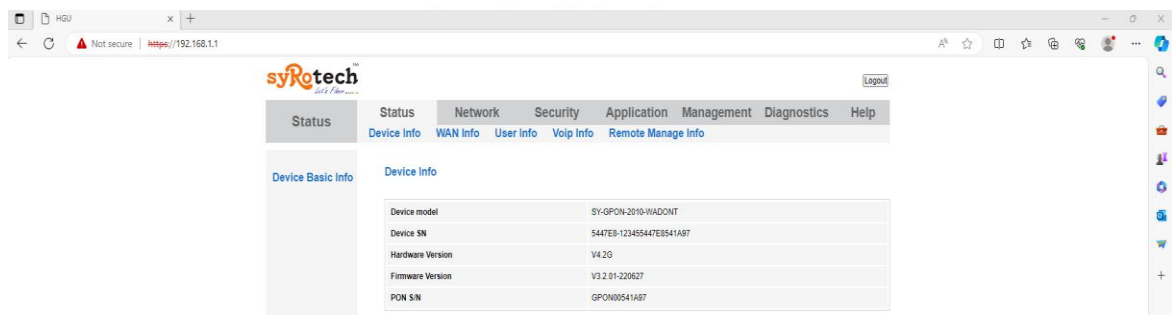
11.1.1.3 Execution Steps:

- i. The Tester opens web browser in test machine (192.168.1.22) to connect DUT (https://192.168.1.1)

```
Pinging 192.168.1.1 with 32 bytes of data:  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64  
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64  
  
Ping statistics for 192.168.1.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 1ms, Average = 1ms  
  
C:\Users\GRL>
```



- ii. After successful authentication with user name and password the tester is able to access the DUT.



11.2 Test Case Number: 02

11.2.1 Test case Name: Bypass authentication attack

11.2.2 Test Case Description: The Tester shall attempt to bypass the authentication system of DUT

11.2.3 Execution Steps:

- i. The Tester shall attempt to perform authentication bypass the web interface of the DUT using the SQL injection

- ii. The tester can use the 'OR '1' = '1 sql injection attack to bypass the authentication
- iii. SQL Map can be used for automated SQL Injection Testing

11.2.4 Test Observations:

- i. **Test case01:** After successful authentication with user name and password the tester is able to access the DUT.
The Tester observed that DUT doesn't have console port. DUT can be configured remotely through web interface <http://192.168.1.1/> only.
- ii. **Test case02:** The test needs to be performed

11.2.5 **Evidence Provided:** Screenshots are attached above

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Remote/local access authentication		
2	Bypass authentication attack		



2.1.5 TSTP for Evaluation of Remote login restrictions for privileged users

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.1.5
---	--------------------------	-----------------

DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

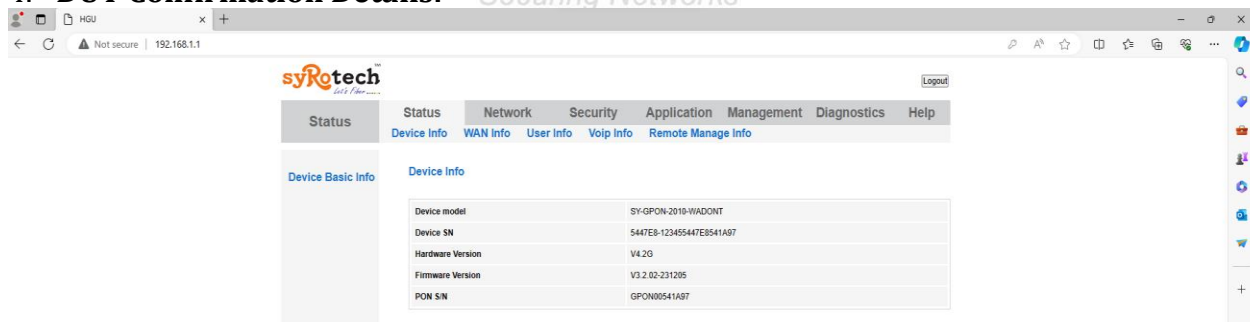
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.1: Access and Authorization
2. **<Security Requirement No & Name >** 2.1.5: Remote login restrictions for privileged users
3. **Requirement Description:** Login to ONU/ONT as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to ONU/ONT remotely i.e. remote login access for root/admin/highest privileged users, by default shall be disabled permanently at the time of first installation.

This remote root user access restriction is also applicable to application software / tools such as TeamViewer, desktop sharing which provide remote access to the ONU/ONT.

[Reference TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.6]

4. DUT Confirmation Details: *Securing Networks*



5. **DUT Configuration:** The DUT should be configured to disallow root login into the DUT
6. **Pre-Condition:** OEM shall provide details remote management standards such as TR-069 and entity mutual authentication, encryption of the management traffic. OEM to provide the credentials of the highest privilege root account

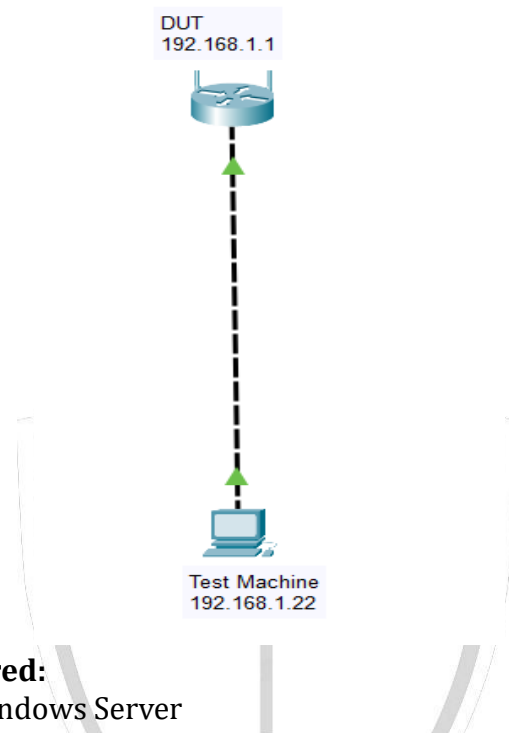
7. **Test Objective:** To verify that DUT restricts direct remote root login

8. **Test Plan**

8.1. No of Test Scenarios:

8.1.1 Test case 01: Verification of remote root login

8.2. Test-bed Diagram:



8.3. **Test tool required:**

- i. TR-069-ACS-Windows Server
- ii. Wireshark

8.4. **Test Execution:**

- i. The tester shall log into the DUT through console to confirm the existence of the root account with its credentials
- ii. The tester shall remotely login into the DUT using the root credentials to check if the DUT permits root login into the DUT

9. **Expected result for pass:** The DUT disallows the remote root login into the DUT

10. **Expected Format of Evidence:** screenshots

11. **Test Execution:**

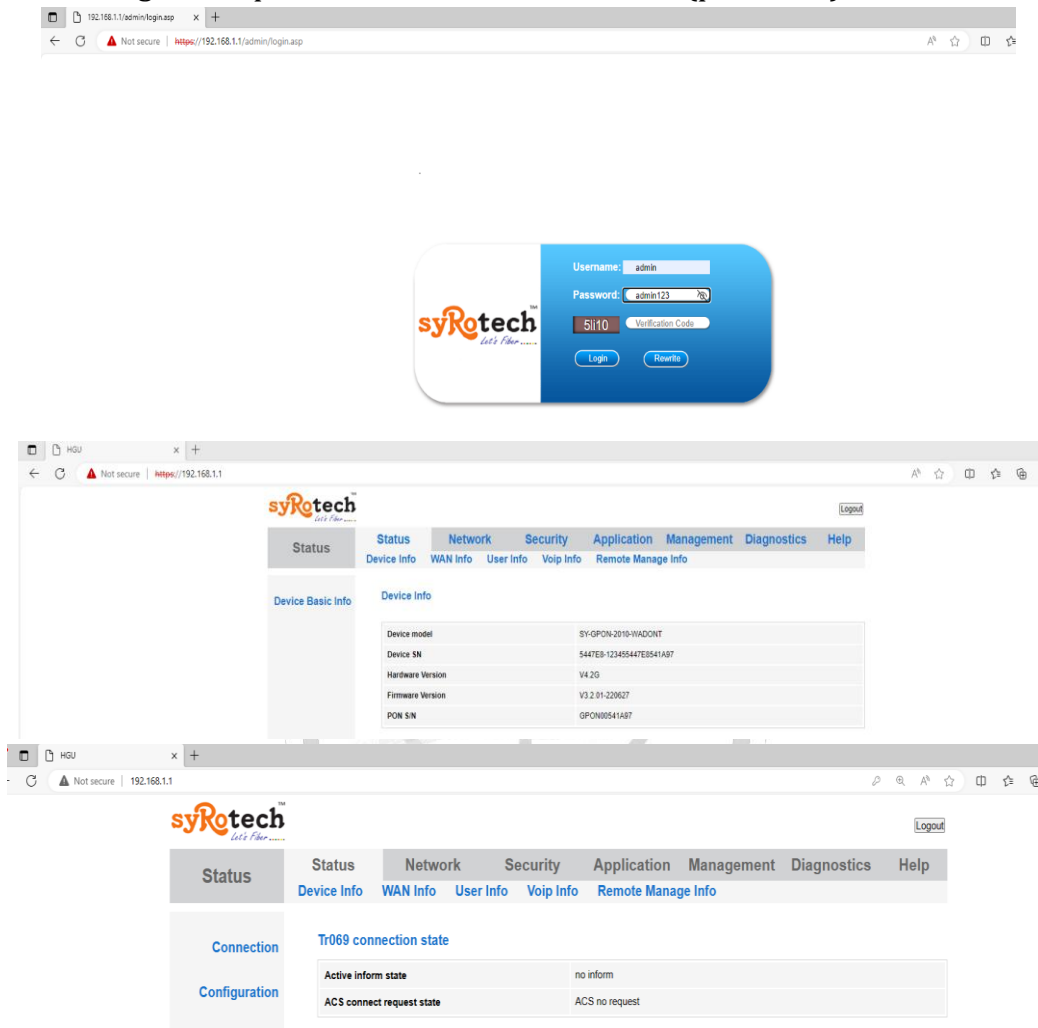
11.1 **Test Case Number: 01**

11.1.1 **Test case Name:** Verification of remote root login

11.1.2 **Test Case Description:** The tester shall try to login to the DUT using the credentials of the root or equivalent highest privileged user from to check whether DUT is restricting the remote login or not.

11.1.3 **Execution Steps:**

- i. The tester login the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) using pre-defined account “admin” with using the respective authentication attribute(password).



11.1.4 Test Observation: The DUT allows remote login of the root/admin account. The Tester observed that it was possible to login with the admin account remotely

11.1.5 Evidence Provided: Screenshots of the DUT remote management.

12 Test Case Results:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Verification of remote root login		

2.1.6 TSTP for Evaluation of Unambiguous identification of the user & group accounts removal

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.1.6
---	--------------------------	-----------------

DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

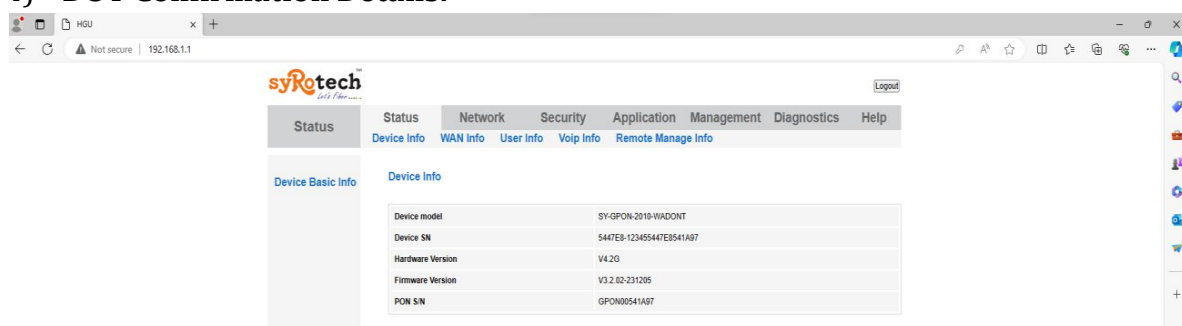
<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

- 1) **<ITSAR Section No & Name> Section 1.1:** Access and Authorization
- 2) **<Security Requirement No & Name> 2.1.6:** Unambiguous identification of the user & group accounts removal
- 3) **Requirement Description:** The ONU/ONT shall identify each login user unambiguously. ONU/ONT shall be able to assign individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. It is a desirable feature to configure user preferred USERID name in configuration menu instead of pre-configured ADMIN User ID. Use of group accounts or group credentials, or sharing of the same account between several users shall not be enabled by ONU/ONT.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 vV.1.0.0. Sections 4.2.3.4.1.2]

4) DUT Confirmation Details:



- 5) **DUT Configuration:** There is no additional configuration required for this test case.

6) Pre-Condition:

- i. OEM shall provide all predefined accounts available on DUT as categorized below–

- a. **Machine Accounts:** These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.
 - b. **Local access:** The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from DUT local hardware interface.
 - c. **Remote access:** The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.
- ii. OEM shall share configuration document to define unique identification (UID) to each user accounts.

7) **Test Objective:** To verify that DUT has unique user identification

8) **Test Plan:**

8.1 Number of Test Scenarios:

- 8.1.1 Test case:01 OEM Documentation review
- 8.1.2 Test case:02 verify unique identification
- 8.1.3 Test case:03 duplicate user id
- 8.1.4 Test case:04 simultaneous logins
- 8.1.5 Test case:05 Unique UID
- 8.1.6 Test case:06 Group account policy verification

8.2 **Test bed Diagram:**

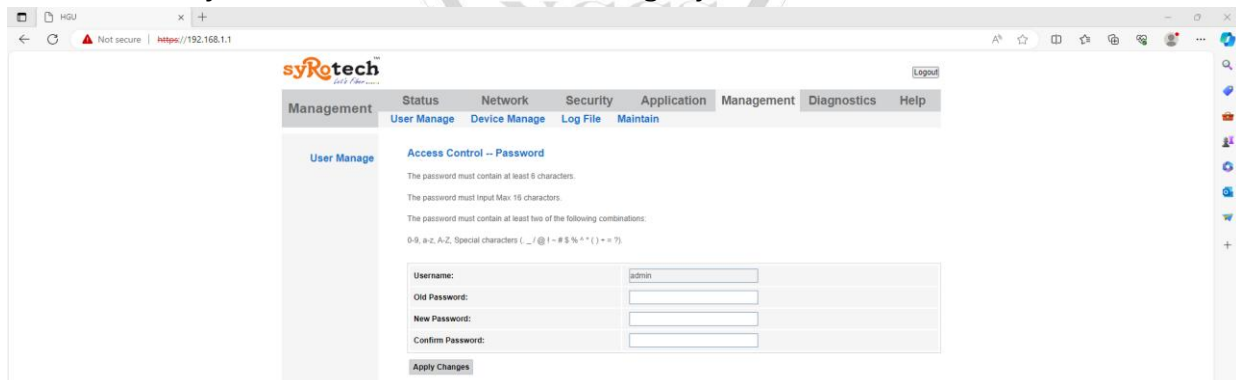


8.3 **Tools required:** Burpe Suite Professional

8.4 **Test Execution:**

- i) The tester shall verify existing individual user accounts user id
- ii) The tester shall verify that every user account has individual/unique user id
- iii) The OEM documentation shall be reviewed for the group account policy supported by the DUT

- iv) The tester shall also verify the disallowance of the concurrent sessions in the DUT
- 9) **Expected Results for Pass:** The DUT shall unambiguously assign individual user accounts and also support group account policy in accordance to the ITSAR
- 10) **Expected Format of Evidence:** screenshots
- 11) **Test Plan:**
 - 11.1 **Test Case Number:** 01
 - 11.1.1 **Test case Name:** OEM documentation review
 - 11.1.2 **Test Case Description:** The Tester reviews the system documentation (in particular operations manual) provided by OEM whether it encourages or requires the use of group accounts, group credentials, or sharing of the same account between several users.
 - 11.1.3 **Execution Steps:** The Tester shall review the user accounts and the group account policy supported by the DUT
 - 11.2 **Test Case Number:** 02
 - 11.2.1 **Test case Name:** verify unique identification
 - 11.2.2 **Test Case Description:** The Tester attempts to create new user in the ONT with existing username that is already available in ONT to verify if the ONT handles ambiguous identification.
 - 11.2.3 **Execution Steps:**
 - i. The tester observed that ONT doesn't support multiple user accounts. It uses only one user account. Hence, ambiguity cannot be verified.



- 11.3 **Test Case Number:** 03
 - 11.3.1 **Test case Name:** duplicate user id
 - 11.3.2 **Test Case Description:** The Tester shall verify that system should not allow creation of duplicate user IDs.
 - 11.3.3 **Execution Steps:**
 - i. The Tester observed that in DUT there is no user creation feature.

syrotech Let's Filter..... [Logout](#)

Management **Status** **Network** **Security** **Application** **Management** **Diagnostics** **Help**

User Manage **Device Manage** **Log File** **Maintain**

User Manage

Access Control -- Password

The password must contain at least 6 characters.
The password must Input Max 32 characters.
The password must contain at least two of the following combinations:
0-9, a-z, A-Z, Special characters (_ / @ ! ~ # \$ % ^ * () + = ?)

Username:

Old Password:

New Password:

Confirm Password:

Apply Changes

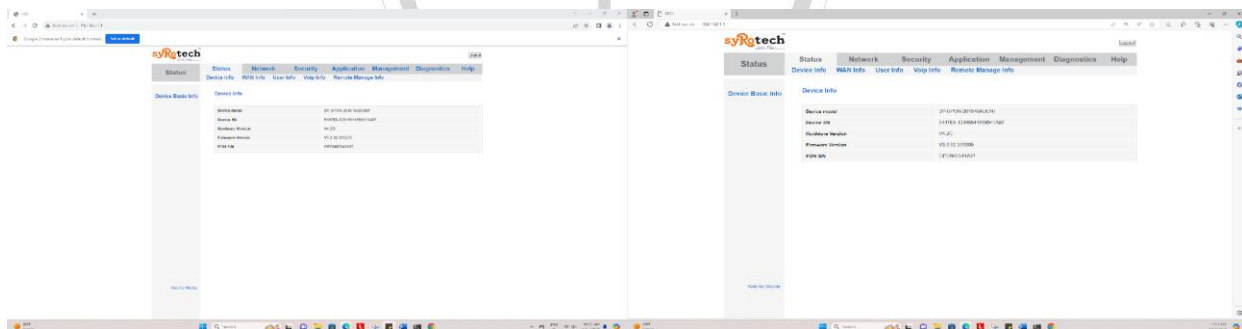
11.4 Test Case Number: 04

11.4.1 Test case Name: simultaneous logins

11.4.2 Test Case Description: The Tester shall verify that simultaneous login is restricted to one session per user ID (concurrent sessions).

11.4.3 Execution Steps:

- The tester attempts to login with the same user's name in the multiple browsers and it should not be allowed to login with the same user at same time.



11.5 Test Case Number: 05

11.5.1 Test case Name: Unique UID

11.5.2 Test Case Description: The Tester shall verify that unique UIDs are assigned for each account.

11.5.3 Execution Steps:

- The tester creates new users and check their user id and they should be unique in the nature to distinguish each user irrespective of their username.

11.6 Test Case Number: 06

11.6.1 Test case Name: Group account policy verification

11.6.2 **Test Case Description:** The Tester shall verify that there should not be any group account password.

11.6.3 Execution Steps:

- i. The tester attempts to create user group account in the DUT and it should not be allowed to create or user group accounts or group credentials.

11.6.4 Test Observations:

- i. **Test case01:** Need to perform the test
- ii. **Test case02:** The tester observed that the DUT comes with a pre-define single user management configuration.
- iii. **Test case 03:** DUT does not allow creation of new user or removal of any pre-defined user.
- iv. **Test case 04:** In the DUT there is not option to check the user id of each user.
- v. **Test case 05:** DUT does not allow group users and group user IDs.
- vi. **Test case 06:** DUT does not allow to create duplicate, as it comes with a pre-defined single user.

11.6.5 **Evidence Provided:** Screenshot of the management >user management and log in tabs of the DUT.

12) **Test Case Results:**

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM documentation review		
2	verify unique identification		
3	Duplicate user id		
4	simultaneous logins		
5	Unique UID		
6	Group account policy verification		



Section 2: Authentication Attribute Management

2.2.1 TSTP for Evaluation of Authentication Policy

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.1
---	--------------------------	-----------------

DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1) **<ITSAR Section No & Name>** Section 2.2: Authentication Attribute Management

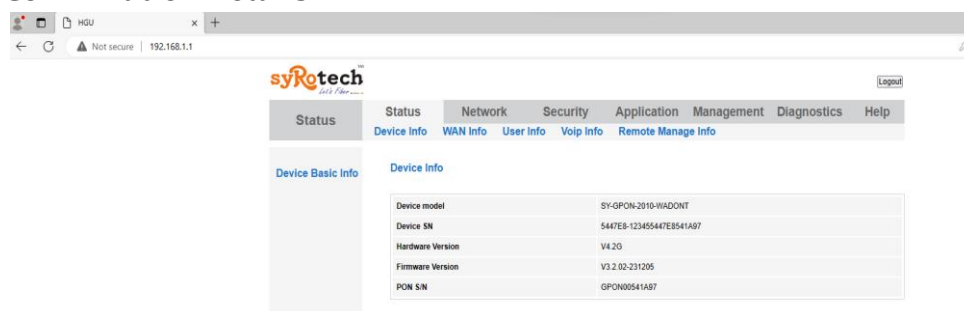
2) **<Security Requirement No & Name >**2.2.1: Authentication Policy

3) **Requirement Description:** The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g. password, certificate, token) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems. This requirement shall also be applied to accounts that are only used for communication between systems.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.1.1]

Securing Networks

4) **DUT Confirmation Details:**



5) **DUT Configuration:** There is no additional configuration required for this test case.

6) **Pre-Conditions:**

- OEM shall supply the list of system functions which include network services, local access via a management console, local usage of operating system and applications

ii. OEM shall supply the list of access entries for system functions.

7) **Test Objective:** To verify that the DUT authenticates the usage of the system function

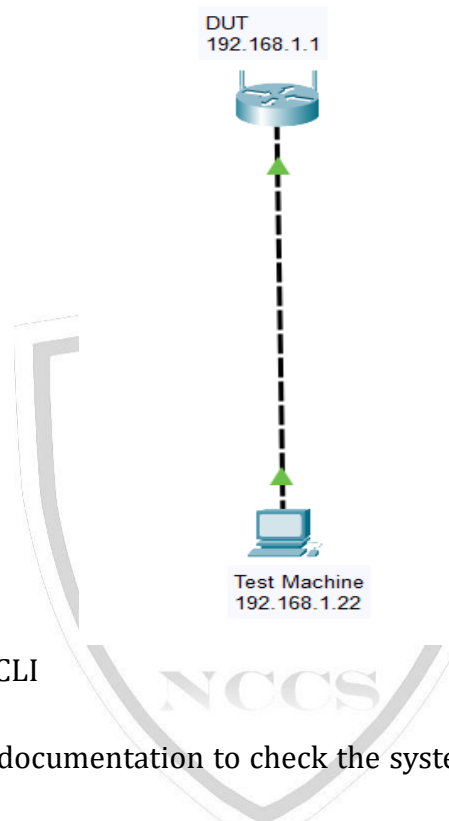
8) **Test Plan:**

8.1 Number of Test Scenarios:

8.1.1 Test case 01: OEM documentation review

8.1.2 Test case 02: Two factor authentication verification

8.2 Test-bed Diagram:



8.3 **Tools required:** CLI

8.4 **Test Execution:**

- i. Verify the OEM documentation to check the system functions supported by the DUT
- ii. Verify that the DUT authenticates the user attempting to access the system functions with at least two authentication attributes

9) **Expected Results for Pass:** DUT should authenticate the user attempting to access the system functions with at least two authentication attributes

10) **Expected Format of Evidence:** screenshots

11) **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test case Name:** OEM documentation review

11.1.2 **Test Case Description:** The tester verifies the list of system functions (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications mentioned in document provided by OEM and on based of his/her own experience, verifies that the list is adequate.

11.1.3 Execution Steps: The Tester reviewed the DUT document available on OEM website and identified that DUT supports Web service, SSH

11.2 Test Case Number: 02

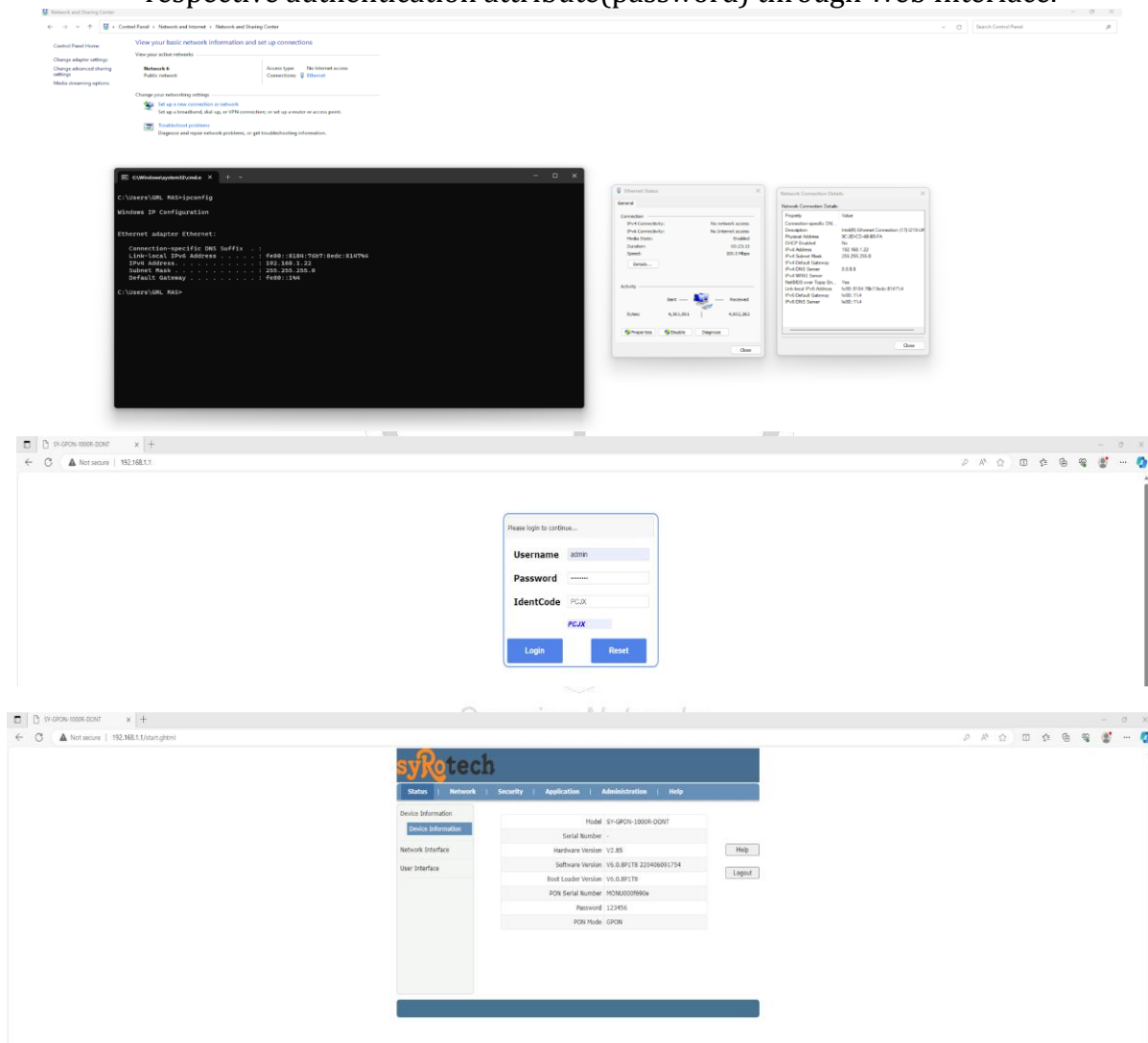
11.2.1 Test case Name: Two factor authentication verification

11.2.2 Test Case Description: The tester verifies that the access entries to use system functions, which are listed by the manufacturer, require successful authentication on the basis of the username and at least two authentication attribute such as “Password / Token / Certificate”.

11.2.3 Execution Steps:

a) LAN Interface: Web GUI

- i. The tester logged into the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.0.22) account “**admin**” with using the respective authentication attribute(password) through Web Interface.



- ii. The Tester is able to login to the DUT successfully with one authentication attribute (password).

b) Telnet

- i. Connect to DUT using telnet

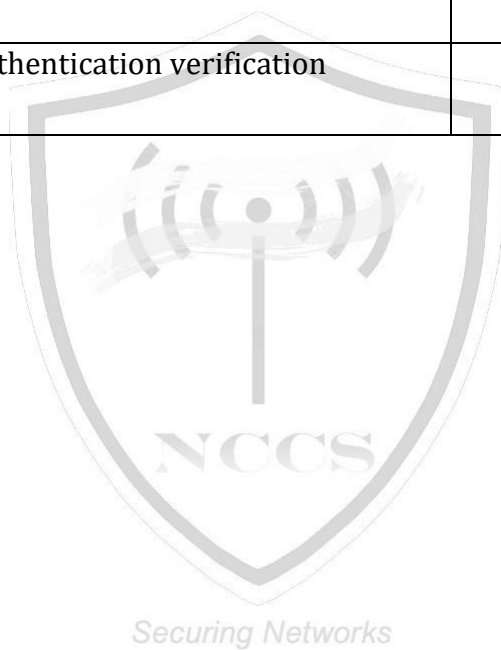
<screenshot>

11.2.4 Test Observations:

- i. **Test case01:** The Tester observed that was only one authentication attribute password while authenticating user. DUT only authenticates user using password authentication attribute
- ii. **Test case02:** DUT does allow to access to any system function provided by the manufacturer with a successful user authentication attribute is password but as per clause authentication on basis of the user identity, at least two authentication attributes (e.g. password, certificate, token) shall be prevented.

12) Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM documentation review		
2	Two factor authentication verification		



2.2.2 TSTP for Evaluation of Authentication support - External

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.2
---	--------------------------	-----------------

<DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

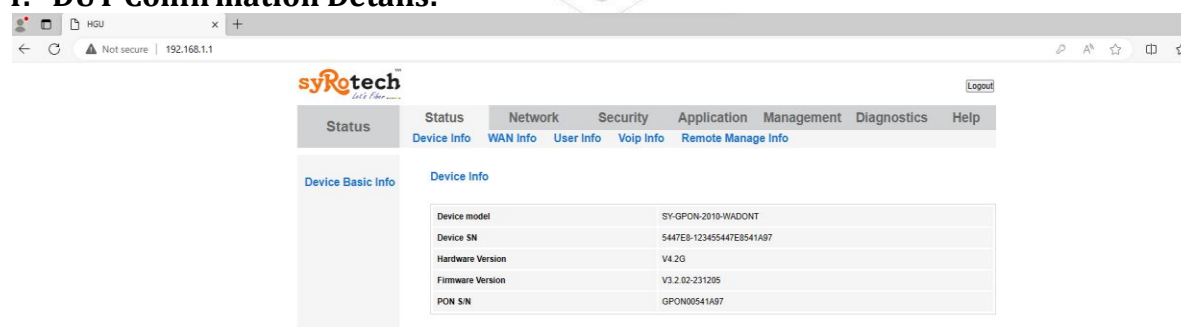
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 1.2: Authentication Attribute Management
2. <Security Requirement No & Name > 2.2.2: Authentication support – External
3. **Requirement Description:** If the ONU/ONT supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services), then the communication between ONU/ONT and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.
OEM/TSP shall disable permanently the supported weaker algorithm other than specified in ITSAR crypto control list document.

4. DUT Confirmation Details:



5. **DUT Configuration:** Configure the DUT connection with the external AAA server

6. Pre-Conditions:

- i. OEM shall provide configuration documentation if DUT supports external authentication mechanism.
- ii. If DUT supports external authentication, then OEM shall provide confirmation that it has protection mechanism and communicate securely.

7. **Test Objective:** To verify that the DUT communicates with the external authentication with secure ciphers

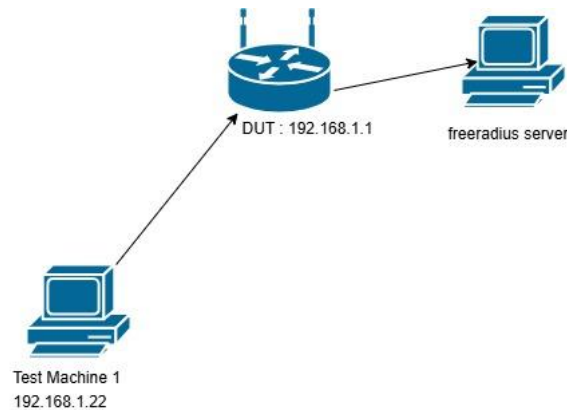
8. Test Plan

8.1. Number of Test Scenarios:

8.1.1 Test case: 01 OEM documentation review

8.1.2 Test case: 02 Communication with external AAA server

8.2. Test-bed Diagram:



8.3. **Tools required:** external authentication server, wireshark

8.4. Test Execution:

- i. Review the OEM documentation to check for the supported external AAA server supported by the DUT
- ii. Post configuration attempt to access the DUT with configured external authentication.
- iii. Simultaneously capture the communication between the DUT and the AAA server and analyze the ciphers used to verify if they are in accordance to the Crypto control ITSAR.

9. **Expected Results for Pass:** DUT uses secure ciphers to communicate with the AAA server for external authentication of the user

10. Expected Format of Evidence: Screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test case Name:** OEM documentation review

11.1.2 **Test Case Description:** The Tester shall review the OEM documentation if DUT supports external authentication mechanism.

11.1.3 **Execution Steps:** Review the OEM documentation for the supported external AAA servers by the DUT

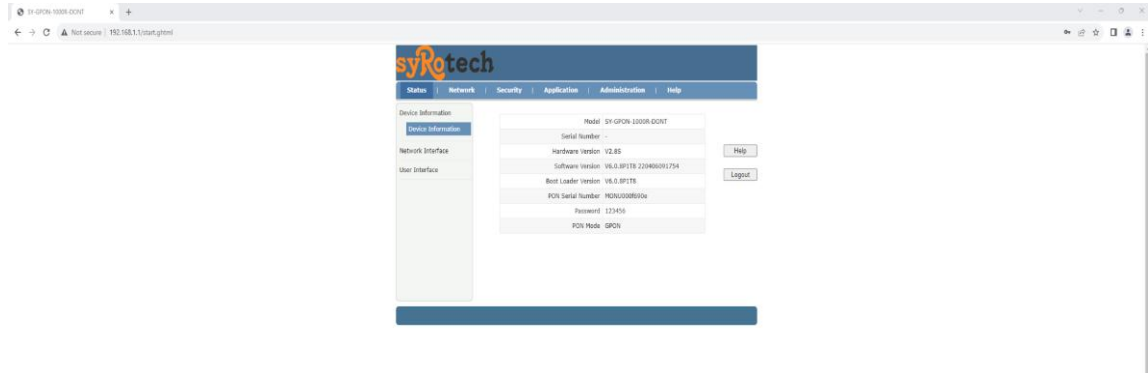
11.2 Test Case Number: 02

11.2.1 **Test case Name:** Communication with external AAA server

11.2.2 Test Case Description: The Tester shall configure the External Authentication Server (AAA) on DUT and established a connection between DUT and AAA server.

11.2.3 Execution Steps:

- i. The Tester observed that DUT doesn't have external authentication mechanism.



11.2.4 Test Observation: Tester observed that DUT doesn't have external authentication mechanism.

Additional Observations

- i. If the DUT supports external authentication (eg: RADIUS), use a tool supporting RADIUS server (eg: free radius) and configure the connection with DUT, by inputting the DUT ip address and credentials at the radius server side.
- ii. Attempt to connect to DUT from the tester machine and capture the whole login session on a packet capturing tool (eg: Wireshark), and inspect for RADIUS packets to check for secure ciphers and leak of sensitive data

11.2.5 Evidence Provided: Screenshots are attached above.

12 Test Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM documentation review		
2	Communication with external AAA server		

2.2.3 TSTP for Evaluation of Protection against brute force and dictionary attacks

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.3
---	--------------------------	-----------------

DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

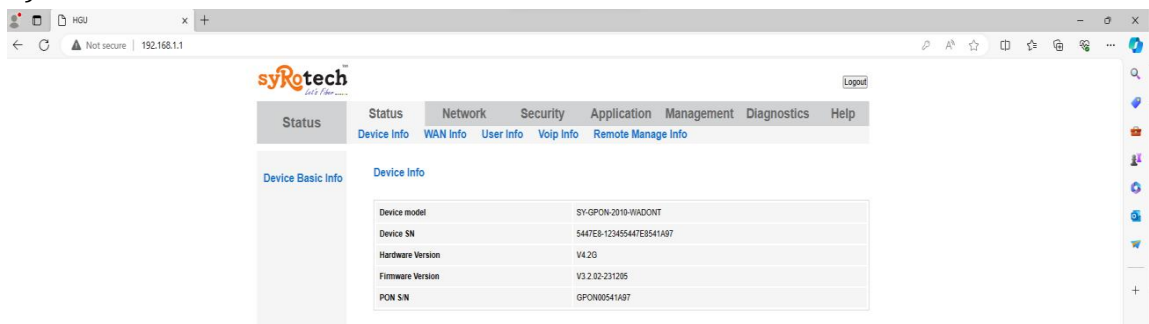
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

- 1) **<ITSAR Section No & Name>** Section 1.2: Authentication Attribute Management
- 2) **<Security Requirement No & Name >** 2.2.3: Protection against Brute force and Dictionary attacks
- 3) **Requirement Description:** ONU/ONT shall have a mechanism that provides a protection against brute force and dictionary attacks which aim to use manual/automated guessing to obtain the passwords for user and machine accounts. ONU/ONT to detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time and it may implement at least one of the following most commonly used protection measures
 - a) Increasing the delay (e.g. doubling) for each newly entered incorrect password.
 - b) Blocking an account after a specified number of incorrect attempts (typically 5) for a certain period of time.
 - c) Using CAPTCHA to prevent automated attempts

This feature to be enabled for login attempts for ONU/ONT and on authentication attempts on ONU/ONT access through SSID with PSK.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.3]

4) DUT Confirmation Details:



5) **DUT Configuration:** There is no additional configuration required for this test case.

6) **Pre-Condition:**

- i. OEM shall provide detail if DUT have mechanism that provides a protection against brute force and dictionary attacks.
- ii. OEM shall provide instruction to configure following most commonly used protection measures -
 - a. Increasing the delay (e.g., doubling) for each newly entered incorrect password.
 - b. blocking an account after a specified number of incorrect attempts (typically 5) for a certain period of time.
 - c. using CAPTCHA to prevent automated attempts.This feature to be enabled for login attempts for ONT and on authentication attempts on ONT access through SSID with PSK.

7) **Test Objective:** To verify that the DUT has protection mechanism against brute force and dictionary attack.

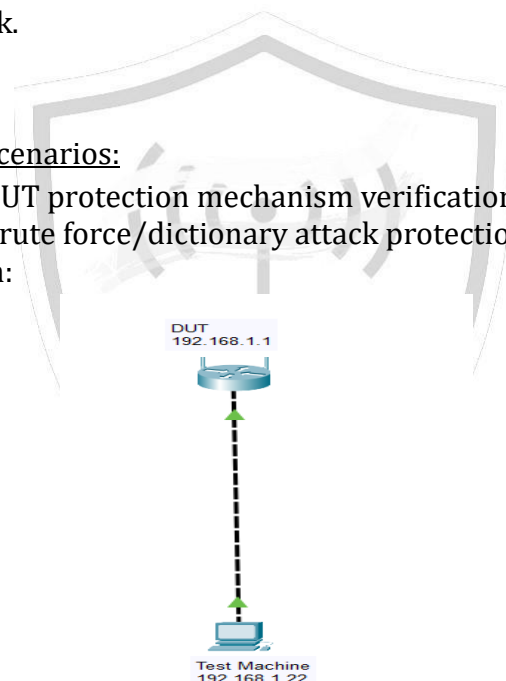
8) **Test Plan:**

8.1 Number of Test Scenarios:

8.1.1 Test case 01: DUT protection mechanism verification

8.1.2 Test case 02: Brute force/dictionary attack protection

8.2 Test-bed Diagram:



8.3 Tools required: Burp Suite Professional

8.4 Execution steps:

- i. The tester shall manually input multiple incorrect attempts to verify the DUT's protection mechanism against repeated attempts
- ii. The tester shall perform brute force and dictionary attack on the DUT using the necessary tools and verify the DUT's response on the same

9) **Expected Results for pass:** The DUT shall have protection mechanism against brute force and dictionary attack

10) **Expected Format of Evidence:** screenshots

11 Test Execution

11.1 Test Case Number: 01

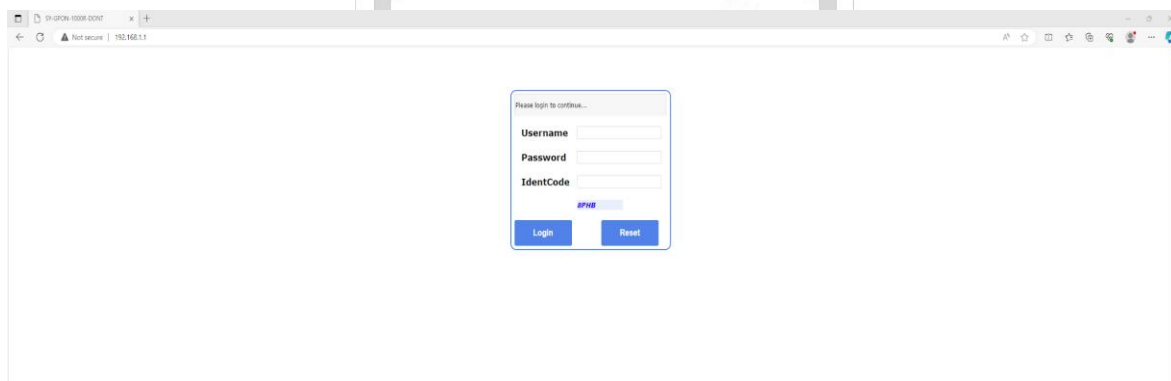
11.1.1 **Test case Name:** DUT protection mechanism verification

11.1.2 **Test Case Description:** Tester shall configure password policy management of the DUT to set -

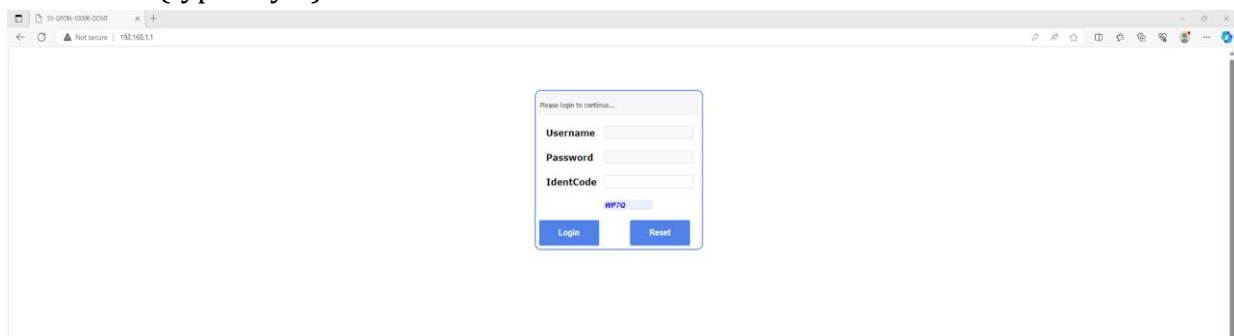
- i. timer delay after each incorrect password input.
- ii. block an account following a specified number of incorrect password attempts (typically 5).
- iii. CAPTCHA feature on web interface to prevent automated attempts

11.1.3 Execution Steps:

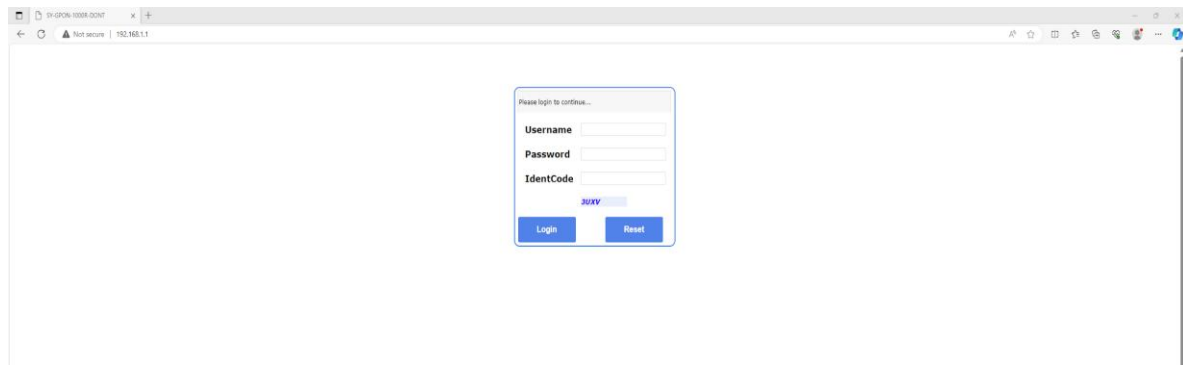
- i. Tester observed that DUT doesn't have password policy management feature on DUT however the Tester attempts to test timer delay feature after each incorrect password input.
- ii. Tester login on DUT (<http://192.168.1.1/>) using test machine 192.168.0.22 with user "admin" and incorrect password multiple times and observed DUT doesn't have any feature for timer delay after each incorrect password input.



- iii. Tester login on DUT (<http://192.168.1.1/>) using test machine 192.168.1.22 with user "admin" and incorrect password and observed have feature for block an account following a specified number of incorrect password attempts (typically 3).



- iv. Tester visits on DUT (<http://192.168.1.1/>) using test machine 192.168.1.22 and observed have CAPTCHA feature on web interface to prevent automated attempts.



- v. Tester observed that DUT doesn't have below mentioned features by default or available to configure timer delay after each incorrect password input.

11.2 Test Case Number: 02

11.2.1 Test case Name: Brute force/dictionary attack protection

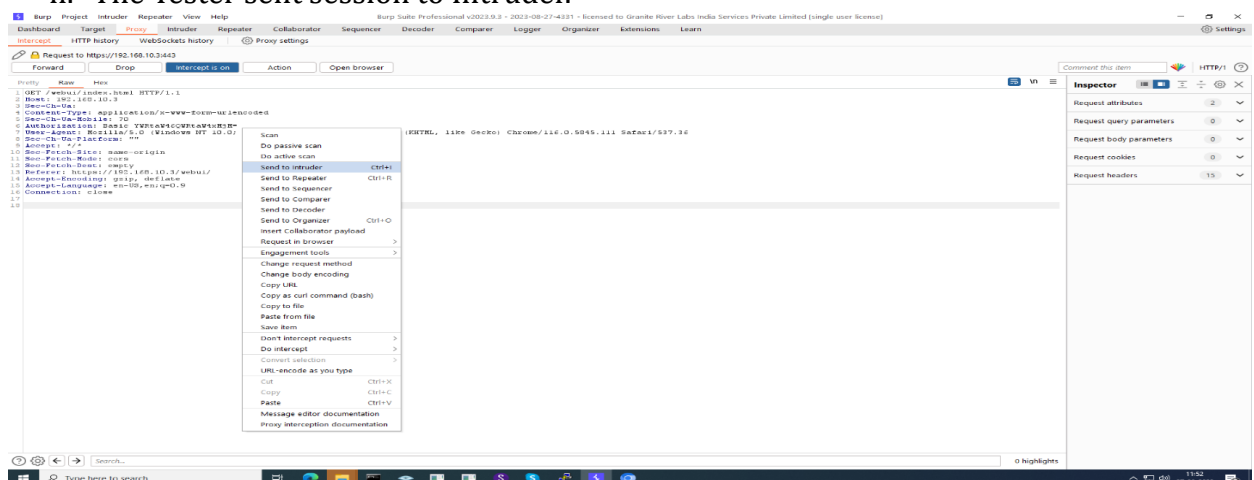
11.2.2 Test Case Description: The Tester shall perform Brute force and dictionary attacks on both CLI or GUI interfaces and supporting evidences needs to be attached in the report.

11.2.3 Execution Steps:

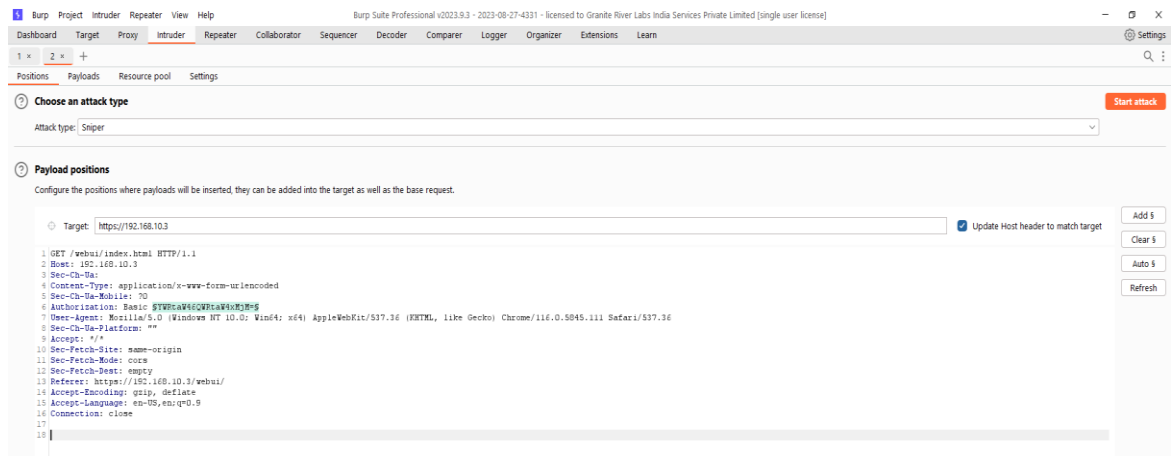
- i. The Tester login into DUT's Web GUI with used id "admin" and captured the sessions in Burp suite.



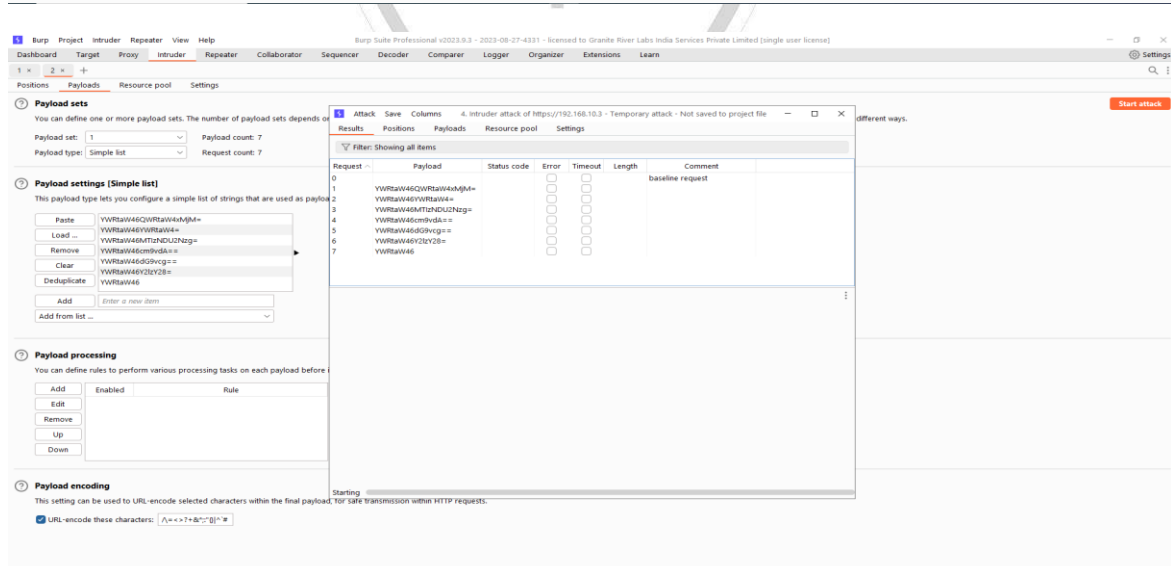
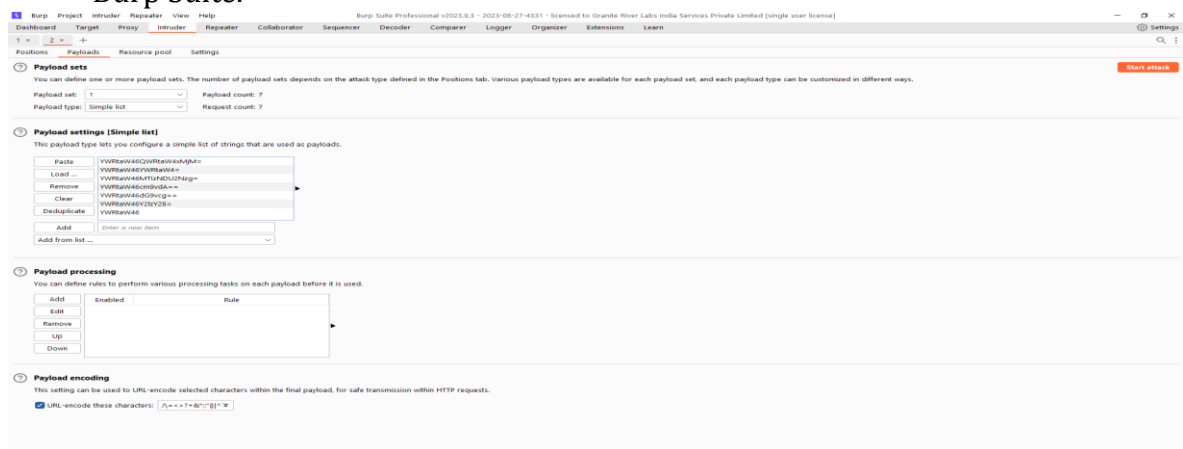
- ii. The Tester sent session to Intruder.

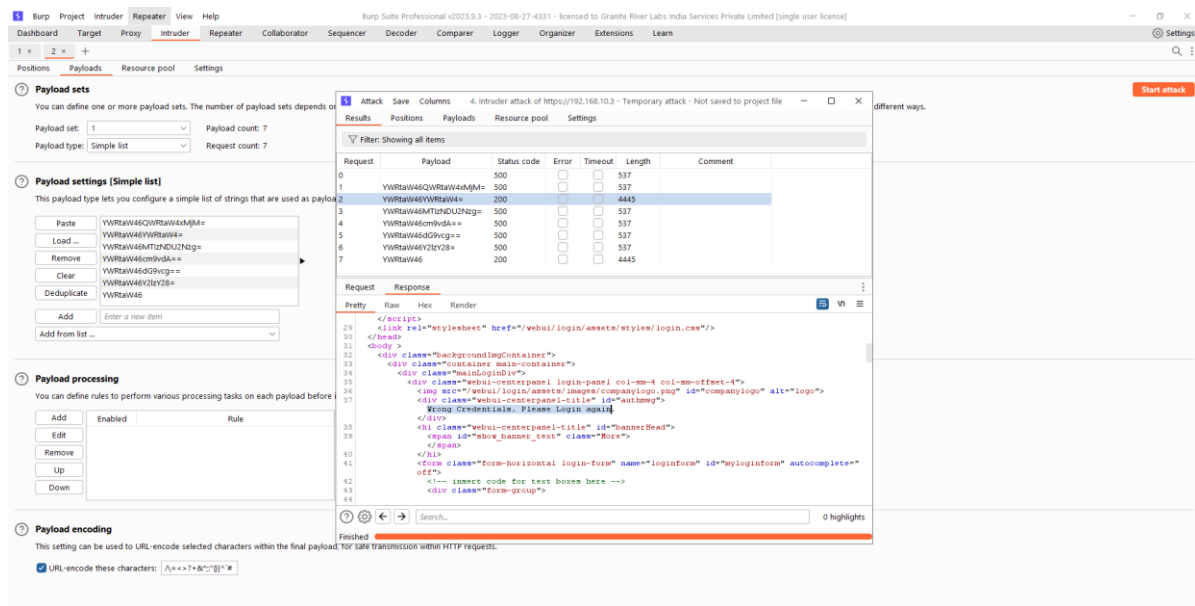


- iii. The Tester selects the Authorization value (Password of admin user ID) to apply a payload for Brute force Attack.



iv. Below screenshots showing the process of applying Brute force attack through Burp Suite.





- v. The Tester observed that DUT didn't compromise due to Brute Force attack. (similarly dictionary attack can also be performed on DUT)
- vi. The tester performed using pre-defined default user as "admin".



11.2.4 Test Observation:

- i. **Test case 01:** DUT doesn't have feature for Timer delay after each incorrect password input is configured and tested. DUT have feature for Block an account following a specified number of incorrect attempts is configured and tested. DUT have feature for pre-configuring CAPTCHA on web interface.
- ii. **Test case 02:** DUT didn't compromise on Brute Force attack. DUT doesn't have feature to be enabled for login attempts for ONU/ONT and on authentication attempts on ONU/ONT access through SSID with PSK. The Tester observed that DUT has limited protection features and doesn't get exposed to brute force attack

11.2.5 Evidence Provided: Screenshots are attached above

12 Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	DUT protection mechanism verification		
2	Brute force/dictionary attack protection		



2.2.4 TSTP for Evaluation of Enforce Strong Password

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.4
---	--------------------------	-----------------

<DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1) **<ITSAR Section No & Name>** Section 1.2: Authentication Attribute Management

2) **<Security Requirement No & Name >** 2.2.4: Enforce Strong Password

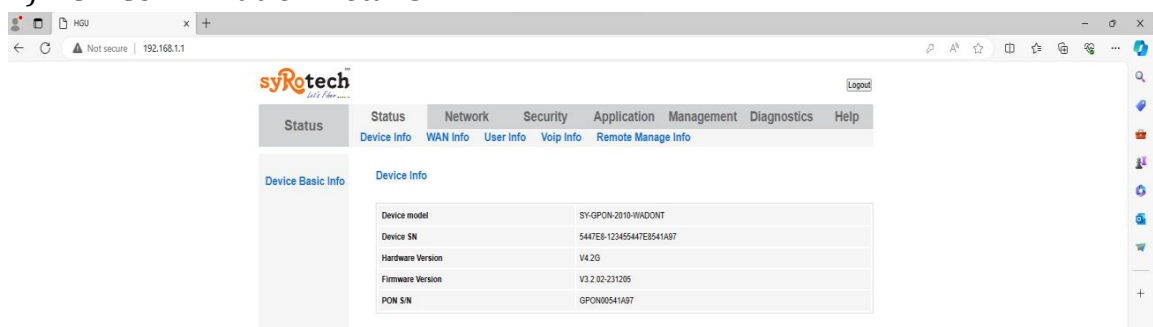
3) **Requirement Description:** ONU/ONT shall only accept passwords that comply with the following complexity criteria:

- Password containing a minimum length of 8 characters are only permitted by default. shorter lengths shall be rejected by the ONU/ONT.
- Minimum password length - the default minimum value of 8 characters.
- Password comprises at least three of the following categories:
 - at least 1 uppercase character (A-Z)
 - at least 1 lowercase character (a-z)
 - at least 1 digit (0-9)
 - at least 1 special character (e.g. @; \$.)

ONU/ONT shall support password field length of minimum 64 characters. This Feature to be enabled for ONU/ONT. Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0 Section 4.2.3.4.3]

4) DUT Confirmation Details:



5) **DUT Configuration:** There is no additional configuration required for this test case.

6) Pre-Condition:

- i. OEM shall provide OEM documentation that describes the password complexity criteria supported by DUT.
- ii. If DUT supports password complexity criteria, then it must support following criteria
 - a. Password containing a minimum length of 8 characters are only permitted by default. shorter lengths shall be rejected by the DUT
 - b. Minimum password length - the default minimum value of 8 characters.
 - c. Password comprises at least three of the following categories:
 - at least 1 uppercase character (A-Z)
 - at least 1 lowercase character (a-z)
 - at least 1 digit (0-9)
 - at least 1 special character (e.g. @;!\$.)
- iii. Tester has rights to create user account.

7) **Test Objective:** To verify the DUT's password policy is in accordance with the ITSAR

8) Test Plan

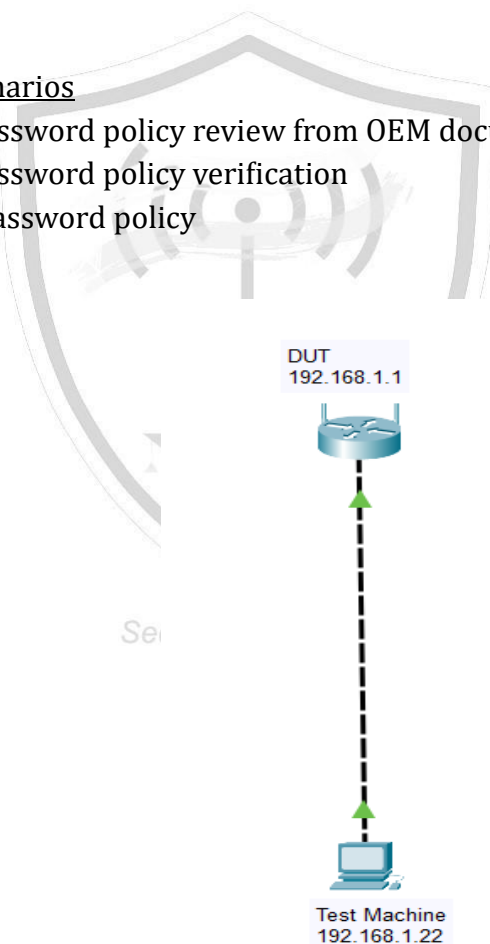
8.1 Number of Test Scenarios

8.1.1 Test case 01: Password policy review from OEM documentation or in the DUT

8.1.2 Test case 02: Password policy verification

8.1.3 ONT Login ID password policy

8.2 Test-bed Diagram:



8.3 Tools required: NA

8.4 Test Execution:

- i. Verify the user's password length if it's below the configured length
- ii. Verify the password policy by attempting negative test cases
- iii. Verify the same for PSK at the ONT access users

9) **Expected Results for pass:**

- i. DUT should follow the configured password policy as well as the min length of the password
- ii. The password should also be followed for the PSK for Wi-Fi access users

10) **Expected Format of Evidence:** Screenshots

11) **Test Execution**

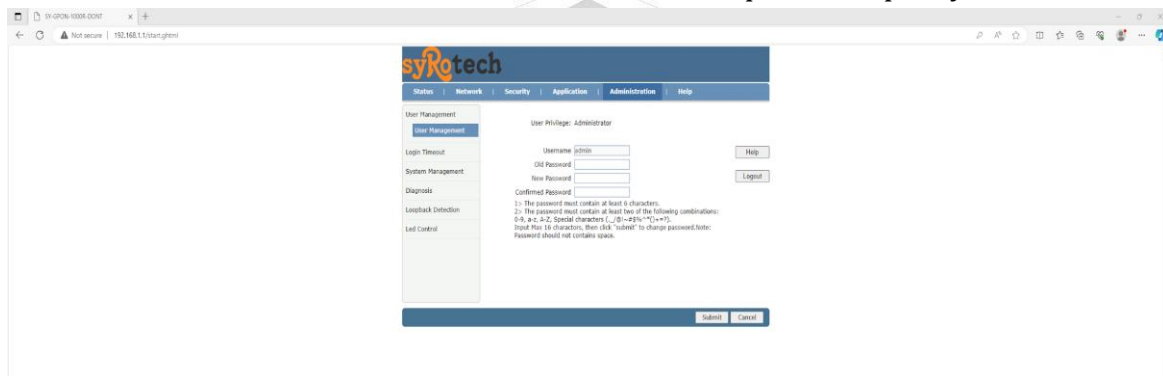
11.1 **Test Case Number:** 01

11.1.1 **Test case Name:** Password policy review from OEM documentation or in the DUT

11.1.2 **Test Case Description:** The Tester shall configure password policy on the DUT as per criteria mentioned in ITSAR.

11.1.3 **Execution Steps:**

- i. The Tester observed that in DUT there is no password policy feature.



11.2 **Test Case Number:** 02

11.2.1 **Test case Name:** Password policy verification

11.2.2 **Test Case Description:** The Tester creates a USER A following the password complexity criteria. (Positive Test).

11.2.3 **Execution Steps:**

- i. The Tester observed that in DUT there is no user creation and password complexity criteria feature.

11.3 **Test Case Number:**03

11.3.1 **Test case Name:** ONT login ID password policy

11.3.2 **Test Case Description** This feature to be enabled for ONT Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

11.3.3 **Execution Steps:** The Tester should observe if the DUT doesn't have feature to enforcing strong password.

11.3.4 **Test observation:**

- i. **Test case01:** Tester observed that in DUT there is no password policy feature.
- ii. **Test case02:** Tester observed that in DUT there is no user creation and password complexity criteria feature.

- iii. **Test case03:** Tester observed that DUT doesn't have feature to enforcing strong password for CPE Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

11.3.5 **Evidence provided:** NA

12) **Test Case Results:**

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Password policy review from OEM documentation or in the DUT		
2	Password policy verification		
3	CPE Login ID password policy		



2.2.5 TSTP for Evaluation of Inactive Session Timeout

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.5
---	--------------------------	-----------------

<DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

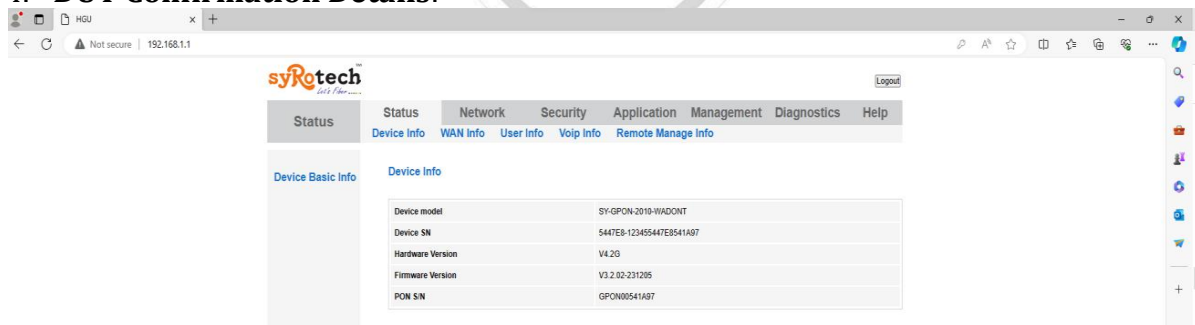
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed

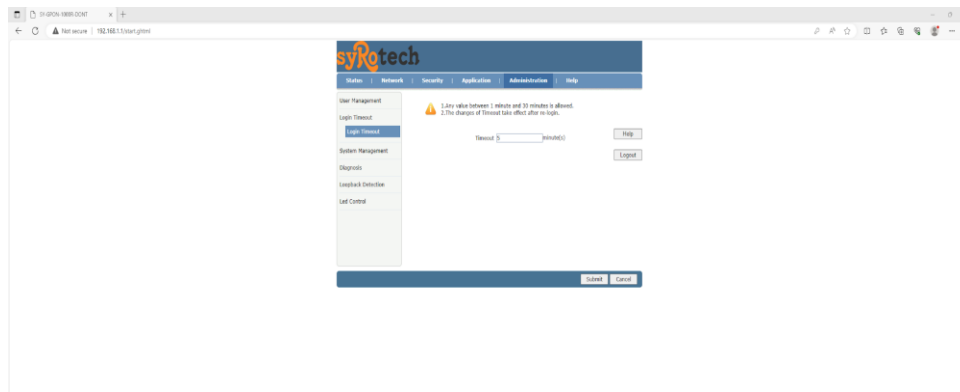
1. **<ITSAR Section No & Name>** Section 1.2: Authentication Attribute Management
2. **<Security Requirement No & Name >** 2.2.5: Inactive Session Timeout
3. **Requirement Description:** ONU/ONT shall monitor inactive sessions of administrative login users, Data users either on LAN or Wi-Fi and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement. When the time out occurs, the same screen must be cleared of all displayed information.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.5.2]

4. DUT Confirmation Details:



5. DUT Configuration:

- i. Configure the DUT to set inactive session timeout
- ii. The Tester observed that DUT have configuration feature of Inactive Session timeout setting.



6. Pre-Condition:

- i. OEM shall provide details on by default Inactive Session Timeout duration configured on DUT.
- ii. OEM shall share instructions to configure inactive session timeout on DUT for each user.

7. Test Objective: To verify that DUT supports inactive session timeout upon being idle

8. Test Plan

8.1. Number of Test Scenarios:

- 8.1.1 Test case 01: Session timeout verification
- 8.1.2 Test case 02: Log analysis

8.2. Test-bed Diagram:

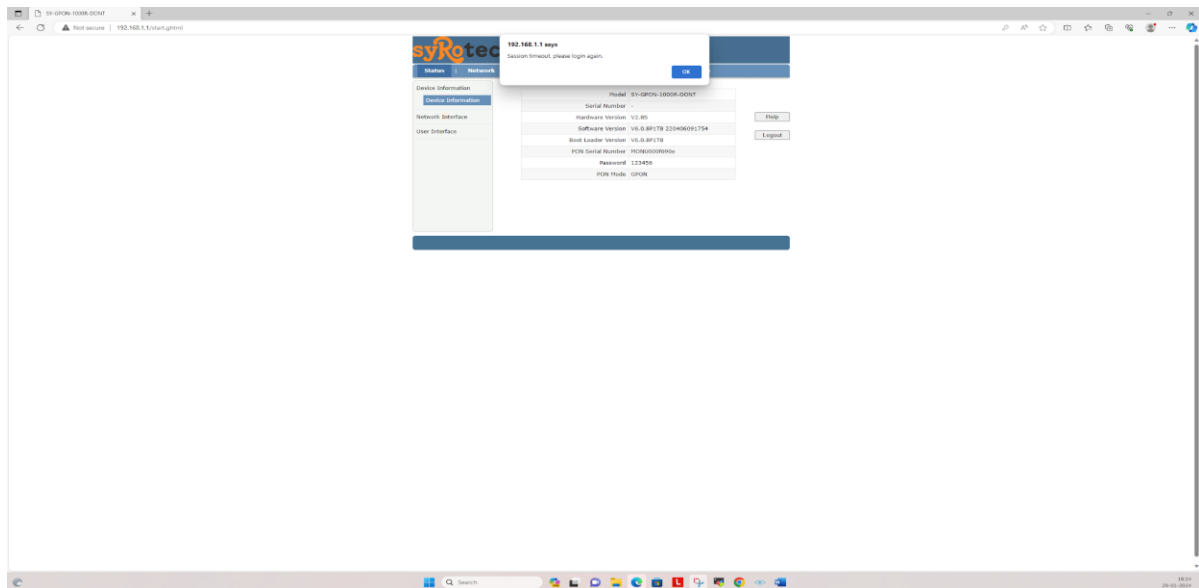


8.3. Tools required: NA

8.4. Test Execution

- i. Post configuration access the DUT
- ii. Stay idle for the configured time
- iii. Check if session timeout is initiated by the DUT and the user gets logged out
- iv. Analyze the logs for timestamps of log in and log out

9. Expected Results for pass: DUT should log out the user upon exceeding the configured session timeout



11.2. Test Case Number: 02

11.2.1 Test case Name: Log analysis

11.2.2 Test Case Description: The Tester analyses the inactive timeout setting in log file also to verify login and logout time.

11.2.3 Execution Steps: The Tester looked for DUT system log to verify login and logout time but DUT doesn't have feature recorded login/logout.

11.2.4 Test Observations:

- i. **Test case01:** The tester observed that after 5 minutes DUT's Session was timeout asked for authentication again. The tester observed that DUT have feature to configure inactive session timeout. Operationally, the Tester verified that DUT have by default configuration of inactivity time-out period for 5 minutes.
- ii. **Test case02:** The Tester looked for DUT system log to verify login and logout time but DUT doesn't have feature recorded login/logout.

12. Test Case Results:

Securing Networks

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Session timeout verification		
2	Log analysis		

2.2.6 TSTP for Evaluation of Password Changes

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.6
---	--------------------------	-----------------

<DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

- 1) **<ITSAR Section No & Name>** Section 1.2: Authentication Attribute Management
- 2) **<Security Requirement No & Name >** 2.2.6: Password Changes
- 3) **Requirement Description:** If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it is possible to redirect or implement this function on this system.
Password change shall be enforced after initial login.
The system shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. ONU/ONT shall support a configurable period for expiry of passwords. Previously used passwords shall not be allowed up to a certain number (password history).
The number of disallowed previously used passwords shall be:
 - Configurable;
 - Greater than 0;
 - And its minimum value shall be 3. This means that the ONU/ONT shall store at least the three previously set passwords. The maximum number of passwords that the ONU/ONT can store for each user is up to the manufacturer.

When a password is about to expire, a password expiry notification shall be provided to the user.

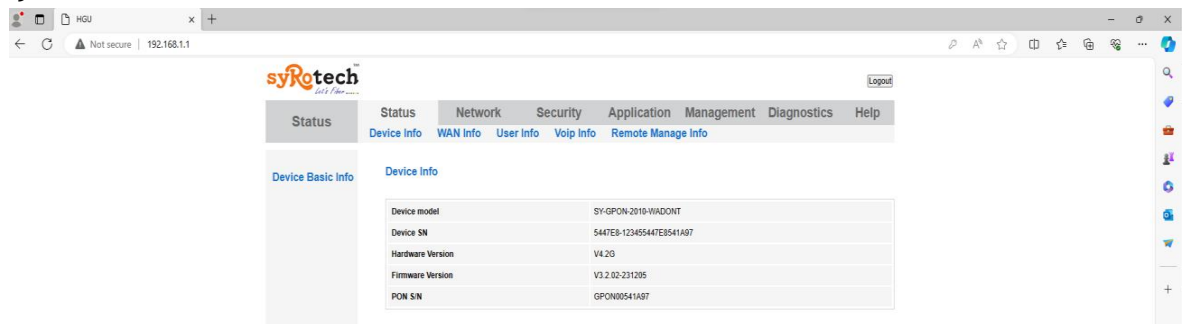
Above requirements shall be applicable for all passwords used (e.g. application-level, OS level, etc.). An exception to this requirement is machine accounts.

ONU/ONT to have in-built mechanism to support this requirement. If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.

And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the ONU/ONT.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.2]

4) DUT Confirmation Details:



5) **DUT Configuration:** There is no additional configuration required for this test case.

6) Pre-Condition:

- i. OEM shall provide documentation which describes that DUT enforce password change on 1st installation.
- ii. OEM shall provide documentation which describes that DUT provide a function that facilitates the user to change his password at any time.
- iii. OEM shall provide confirmation that DUT shall not allow the previously used passwords up to a certain number (Password History).

7) **Test Objective:** To verify that DUT supports password changes in accordance to the ITSAR

8) Test Plan

8.1 Number of Test Scenarios:

- 8.1.1 Test case01: Password change anytime
- 8.1.2 Test case02: Password change anytime (external authentication)
- 8.1.3 Test case 03: Password change after initial login
- 8.1.4 Test case 04: The Tester verify that DUT enforce password change based on password management policy. (if central system used then the management policy should be reflected there)
- 8.1.5 Test case05: Password History.
- 8.1.6 Test case 06: The Tester verify that limit of previously used password is working or not. (Positive and Negative scenarios)

8.2 Test-bed Diagram:



8.3 Tools required: Burp Suite Professional

8.4 Test Execution:

- i. The tester shall verify password change anytime and also after initial login
- ii. The tester shall verify the password management policy and test the same
- iii. The tester shall verify the password history feature supported by the DUT

9) **Expected Results for pass:** DUT follows the password change policy in accordance to the ITSAR

10) **Expected Format of Evidence:** Screenshots

11) **Test Execution**

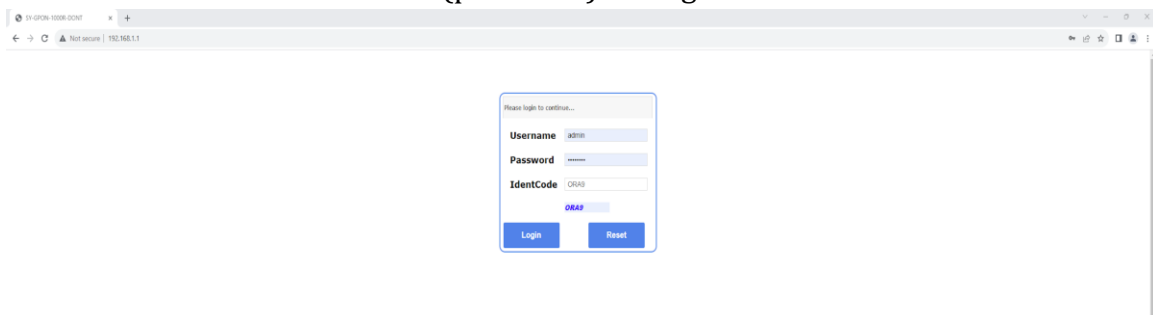
11.1 **Test Case Number:** 01

11.1.1 **Test case Name:** Password change anytime

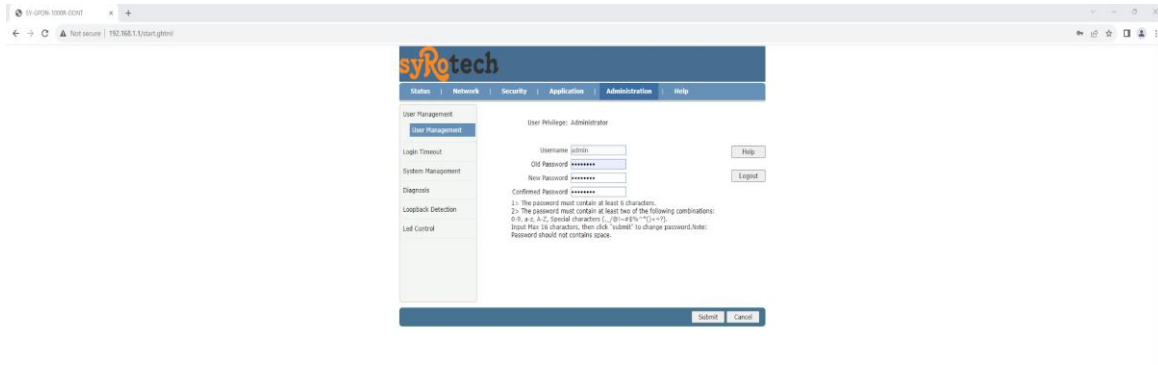
11.1.2 **Test Case Description:** The Tester verify that the DUT allow user to change his password at any time.

11.1.3 **Execution Steps:**

- i. The tester login the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) account "admin" with using the respective authentication attribute(password) through Web Interface.



- ii. The tester clicks on Administration > User Management.
- iii. The Tester observed DUT can allow to User can change password.

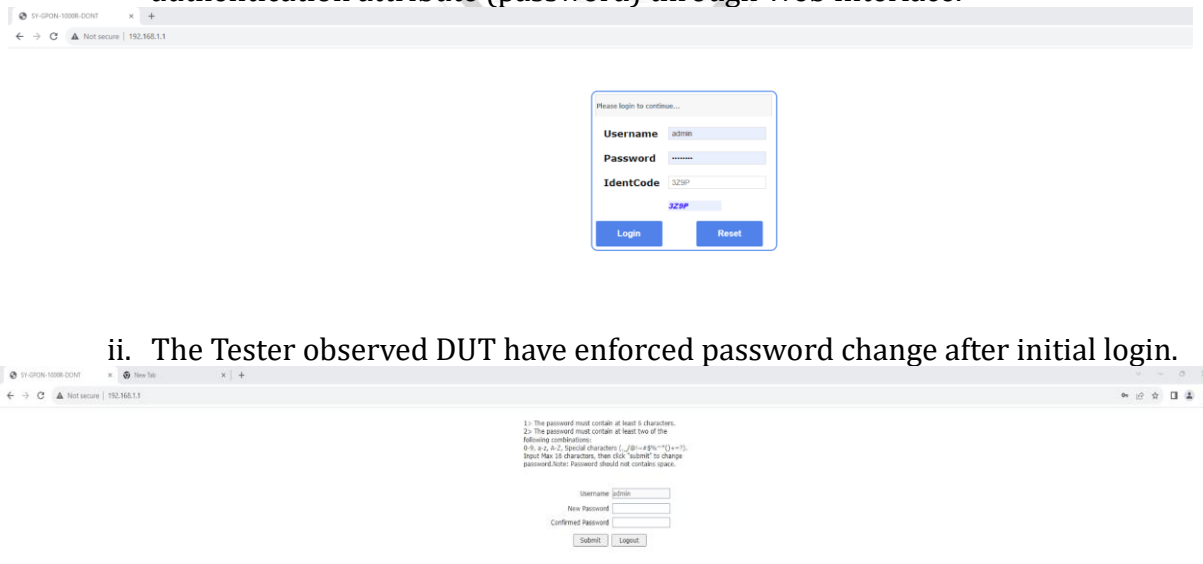


11.2 Test Case Number: 02

- 11.2.1 **Test case Name:** Password change anytime (external authentication)
- 11.2.2 **Test Case Description:** If external Authentication System is in used, then the Tester verify that it allows user to change his password at any time.
- 11.2.3 **Execution Steps:** The Tester observed that DUT doesn't have external authentication mechanism.

11.3 Test Case Number:03

- 11.3.1 **Test case Name:** Password change after initial login
- 11.3.2 **Test Case Description:** The Tester verify that DUT enforce password change after initial login.
- 11.3.3 **Execution Steps:**
- The tester login the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) account "admin" with using the respective authentication attribute (password) through Web Interface.



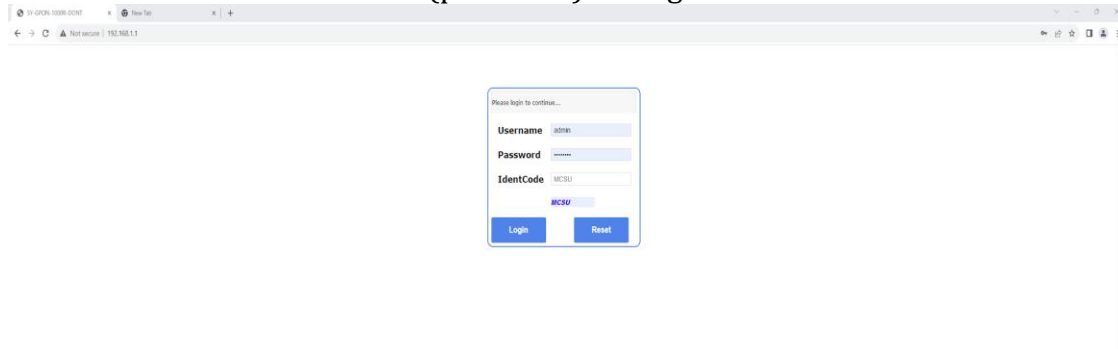
11.4 Test Case Number: 04

- 11.4.1 **Test case Name:** The Tester verify that DUT enforce password change based on password management policy.

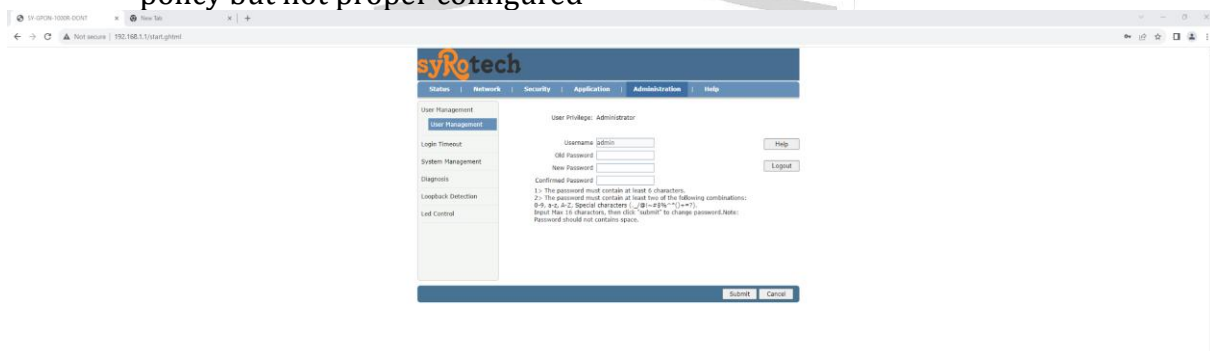
11.4.2 Test Case Description: The Tester verify that DUT enforce password change based on password management policy.

11.4.3 Execution Steps:

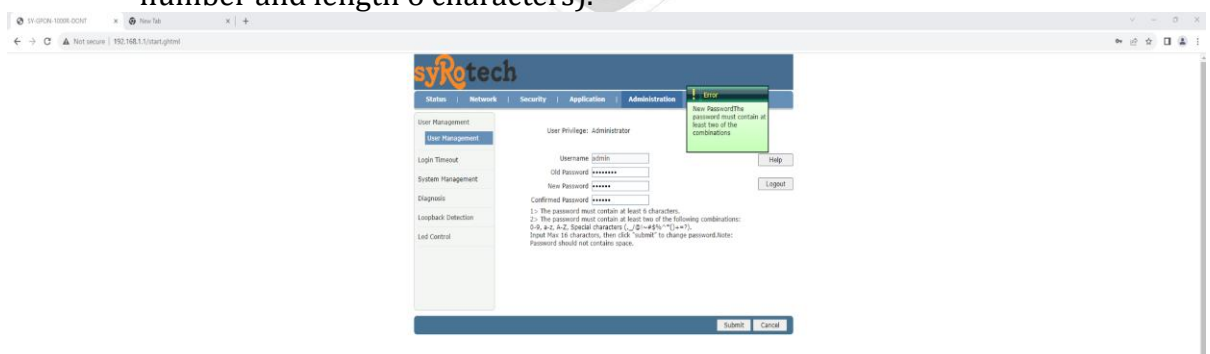
- i. The tester login the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) account "admin" with using the respective authentication attribute(password) through Web Interface.



- ii. The Tester observed DUT can allow to user change password.
- iii. The Tester observed that DUT have enforce feature password management policy but not proper configured



- iv. The Tester observed that DUT support two combinations (lower case and number and length 6 characters).



- v. (if central system used for authentication, then password management policy should be enforced there as well)

11.5 Test Case Number: 05

11.5.1 Test case Name: The Tester verify that limit of previously used password is working or not. (Positive and Negative scenarios).

11.5.2 Test Case Description: The Tester verify that limit of previously used password is working or not. (Positive and Negative scenarios).

11.5.3 **Execution Steps:** The Tester observed during password change that DUT doesn't have feature to configure the limit of previously used passwords (Password History).

11.6 Test Case number: 06.

11.6.1 **Test Case Name:** Password Expiry Notification

11.6.2 **Test Case Description:** To check if DUT sends notification upon password expiry

11.6.3 **Execution Steps:** -<>

11.6.4 **Test observations:**

- i. **Test case01:** The Tester observed DUT can allow to User can change password.
- ii. **Test case02:** The Tester observed that DUT doesn't have external authentication mechanism.
- iii. **Test case 03:** The Tester observed DUT have enforced password change after initial login.
- iv. **Test case04:** The Tester observed that DUT has enforced feature password management policy but not proper configured.
- v. **Test case05:** Tester observed during password change that DUT doesn't have feature to configure the limit of previously used passwords (Password History).
- vi. **Test case 06:** Tester verified enforce password change after initial login.

12) Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1			

2.2.7 TSTP for Evaluation of Protected Authentication feedback

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.7
--	--------------------------	-----------------

<DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

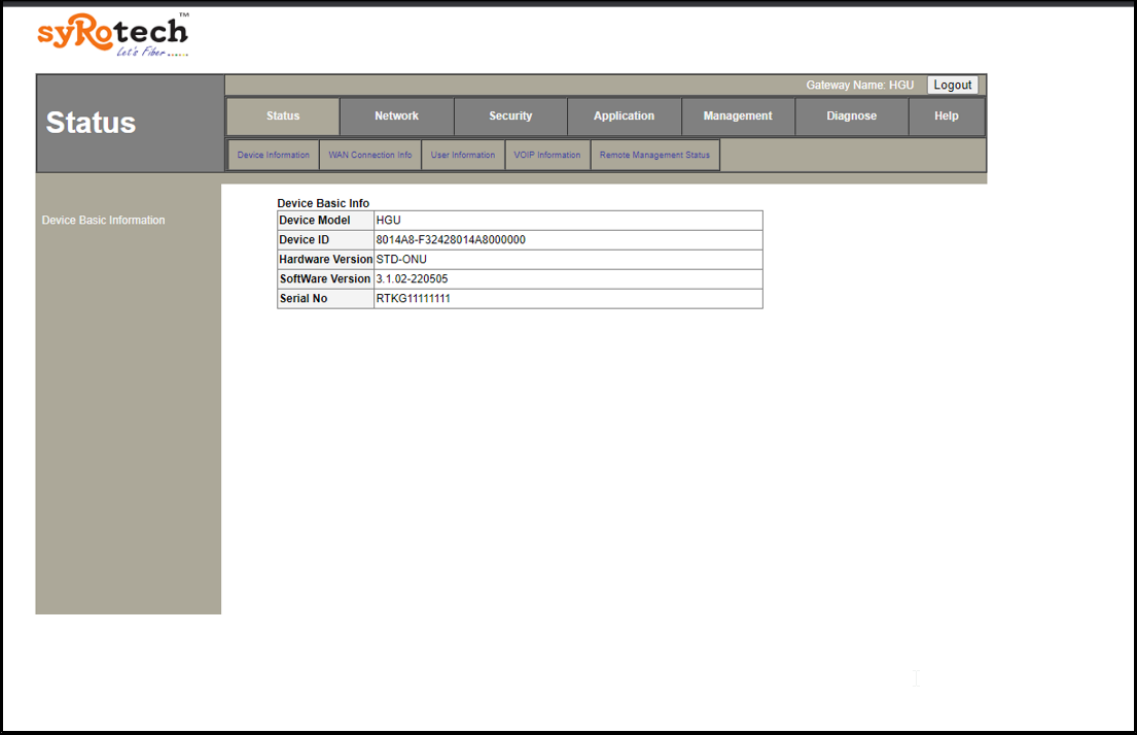
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

- 1) <ITSAR Section No & Name> **Section No: 1.2 Authentication Attribute Management**
- 2) <Security Requirement No & Name > **2.2.7 Protected Authentication feedback**
- 3) **Requirement Description:** The Authentication attribute shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "*".

4) DUT Confirmation Details:



The screenshot displays the syrotech web interface. At the top, the logo 'syrotech' is visible with the tagline 'Let's Fiber.....'. The main navigation bar includes 'Status', 'Network', 'Security', 'Application', 'Management', 'Diagnose', and 'Help'. A 'Gateway Name: HGU' and a 'Logout' button are also present. Below the navigation bar, there are tabs for 'Device Information', 'WAN Connection Info', 'User Information', 'VOIP Information', and 'Remote Management Status'. The 'Device Information' tab is selected, showing a table of device details:

Device Basic Info	
Device Model	HGU
Device ID	8014A8-F32428014A8000000
Hardware Version	STD-ONU
Software Version	3.1.02-220505
Serial No	RTKG11111111



Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
FXS	1 Port(s)	Physical	FXS
GUI	-	Man-Machine	Syrotech

5) DUT Configuration: No configuration needed

6) Pre-Condition: One DUT Documentation that lists each of the password access methods of DUT

7) Test Objective: to verify that DUT's authentication attribute shouldn't be visible

8) Test Plan

8.1 Test Cases:

8.1.1 Test case01: Password text during login

8.1.2 Test case02: Password text during Wi-Fi connection

8.1.3 Test case03: Password text during password change

8.2 Test-bed Diagram:

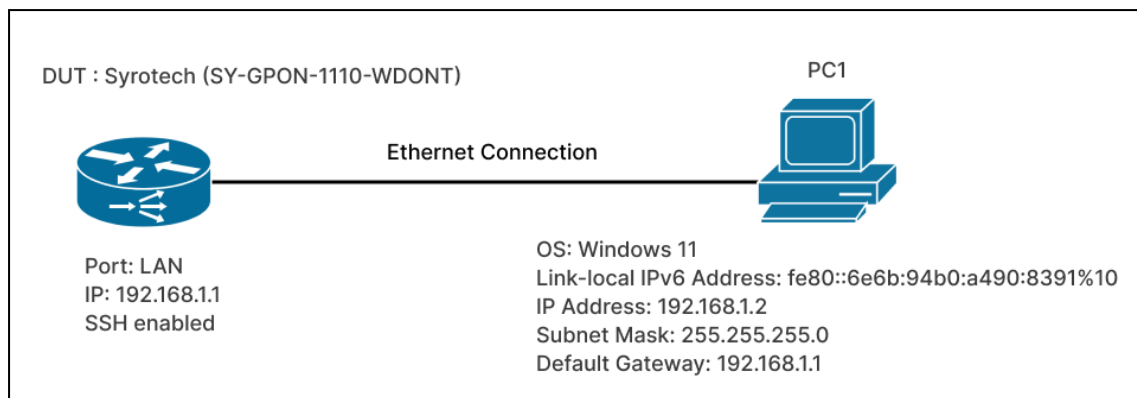
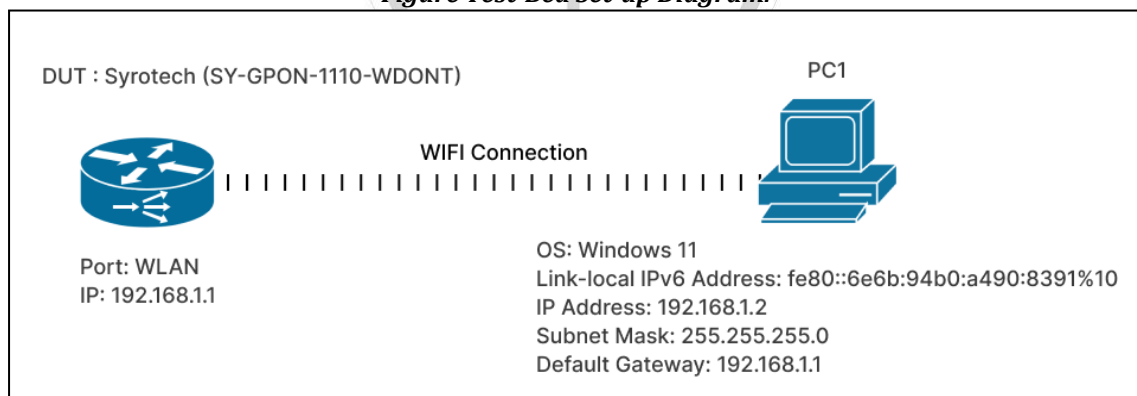


Figure Test-Bed Set-up Diagram.



8.3 Test tool required per scenario/test case:

8.4 Test Execution steps

- Open a web browser and enter the default gateway address (192.168.1.1), Therefore, enter the username "admin" and password "admin123" in the login dialog box to check
- In PuTTY, enter the ONT's IP address (192.168.1.1) in the "Host Name" field and set the port to your desired number (e.g., 22 for SSH). Then click "Open" and user is prompt to enter username "admin" and password "admin123" for login into the ONT.
- On the Wi-Fi quick setting, select Manage Wi-Fi connections.
 - Choose the Wi-Fi network, here it is SSID FTTH-210F, then select Connect.

- b. Verify whether the password is displayed in an encrypted format or in plain text, after entering the network password 12345678.
- iv. Open a web browser and enter the default gateway address (192.168.1.1), Therefore, enter the username "admin" and password "admin123" in the login dialog box to login.
 - a. In the Management setting section, navigate to the user management tab. Change the password.
 - b. Verify that password is encrypted format while changing via web access.
- v. In PuTTY, enter the ONT's IP address (192.168.1.1) in the "Host Name" field and set the port to your desired number (e.g., 22 for SSH). Then click "Open" and user is prompt to enter username "admin" and password "admin123" for login into the ONT.
 - a. To change the password of user "admin", execute the below command.
 - b. config account password user "admin" oldpasswd "admin123" newpasswd "admin@123".
 - c. Verify that password is encrypted format while changing via CLI access.

9) Expected Results for Pass: - The DUT and the operator shall mutually authenticate each other for every management protocol supported by the DUT

10) Expected format of evidence: screenshots

11) Test Execution:

11.1 Test Case Number: 01

11.1.1 Test case Name: Password text during login

11.1.2 Test Case Description: The tester verifies if the password is displayed in an encrypted format while logging.

11.1.3 Execution Steps:

a) Web Access

- i. Open a web browser and enter the default gateway address (192.168.1.1), Therefore, enter the username "admin" and password "admin123" in the login dialog box to check - as show in figure

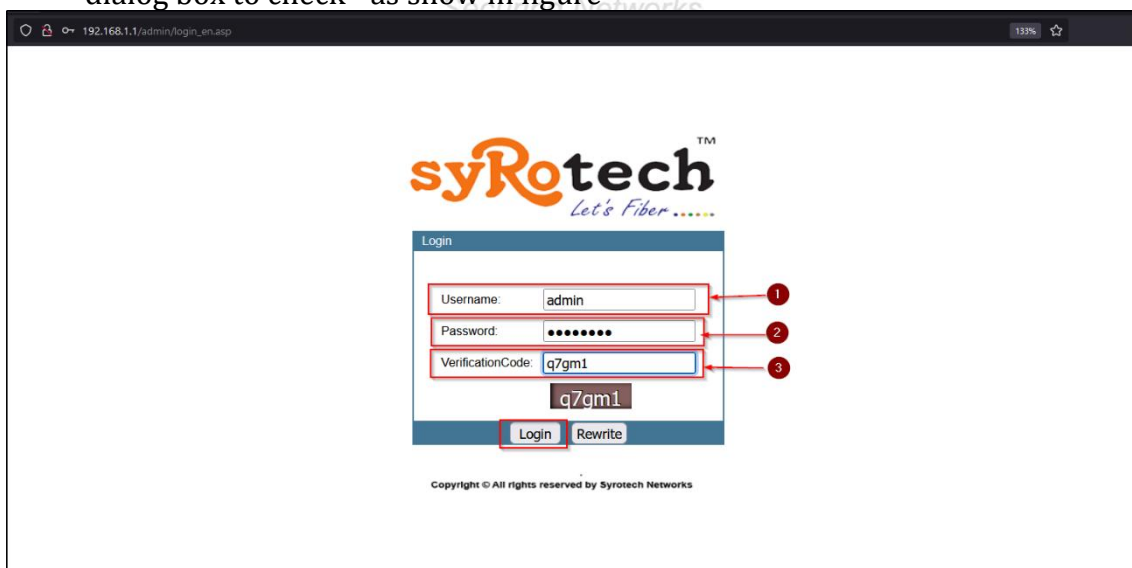


Figure: Login page of DUT

b) CLI Access.

- i. In PuTTY, enter the ONT's IP address (192.168.1.1) in the "Host Name" field and set the port to your desired number (e.g., 22 for SSH). Then click "Open" and the user is prompt to enter username "admin" and password "admin123" for login into the ONT - as show in figure

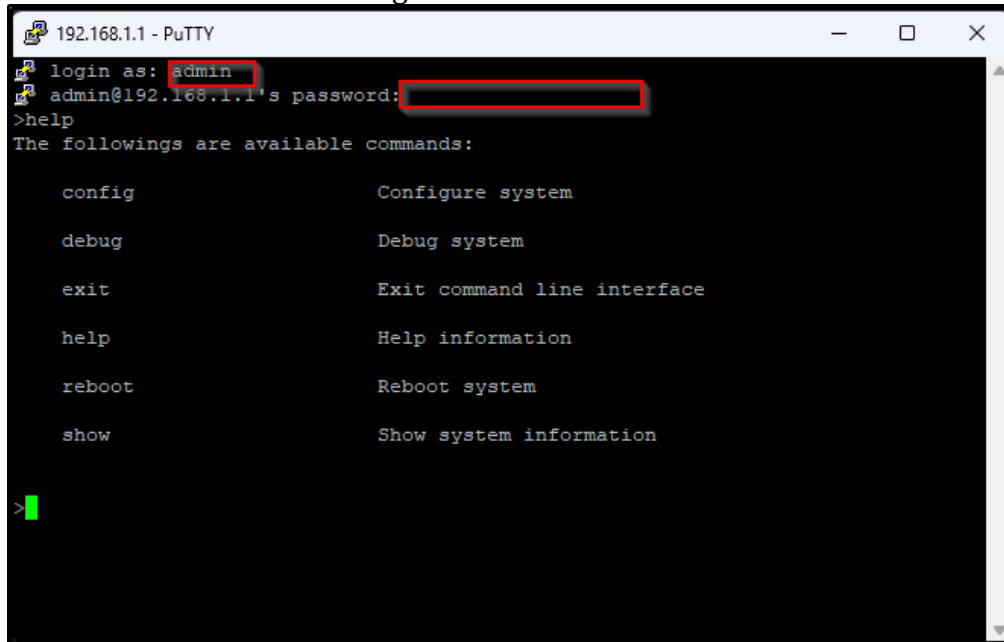


Figure Login page of DUT via CLI access.

11.1.4 Evidence Provided: The password is obfuscated while login over the web interface.



- No password is displayed while login through SSH.

```
192.168.1.1 - PuTTY
login as: admin
admin@192.168.1.1's password:
>help
The followings are available commands:

config          Configure system
debug           Debug system
exit            Exit command line interface
help            Help information
reboot          Reboot system
show            Show system information

>
```

11.2 Test Case Number: 02

11.2.1 Test case Name: Password text during Wi-Fi connection

11.2.2 **Test Case Description:** The tester verifies if the password is displayed in an encrypted format during Wi-Fi connection

11.2.3 Execution Steps:

- i. On the Wi-Fi quick setting, select **Manage Wi-Fi connections**.

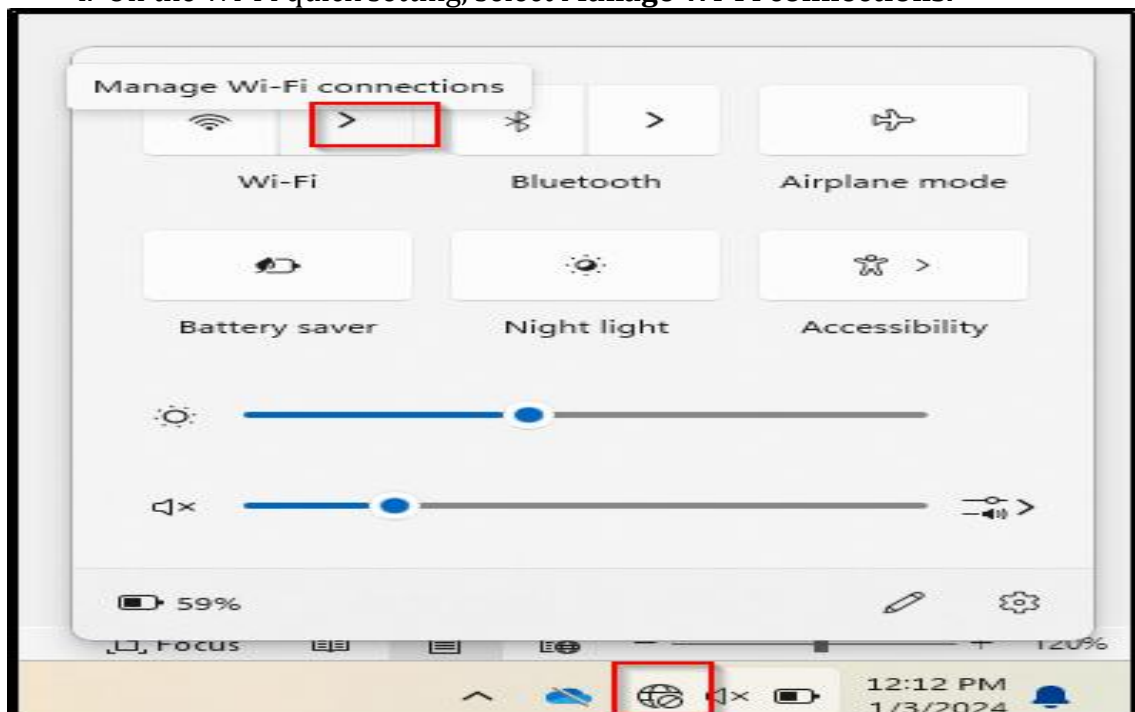


Figure Select Manage Wi-Fi Connection

- ii. Choose the Wi-Fi network, here it is SSID **FTTH-210F**, then select **Connect**.

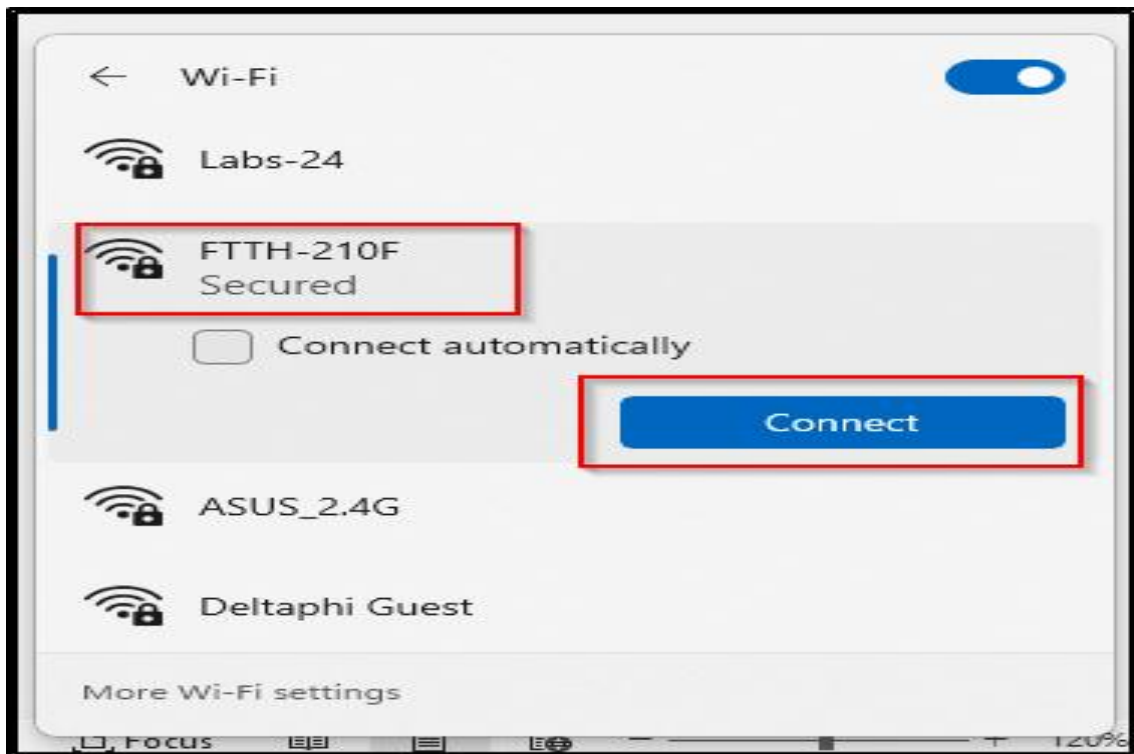


Figure Connect to FTTH-210F Wi-Fi Connection

iii. Verify whether the password is displayed in an encrypted format or in plain text, after entering the network password **12345678**.

11.2.4 Evidence Provided: No password was displayed during Wi-Fi connection.



11.3 Test Case Number: 8.3

11.3.1 **Test case Name:** Password text during password change

11.3.2 **Test Case Description:** The tester verifies if the password is displayed in an encrypted format during password change.

11.3.3 **Execution Steps**

a) **Web Access.**

- i. Open a web browser and enter the default gateway address (192.168.1.1), Therefore, enter the username "admin" and password "admin123" in the login dialog box to check - as show in figure



Figure Login page of DUT

- ii. In the Management setting section, navigate to the user management tab. Change the current user password - as shown in figure

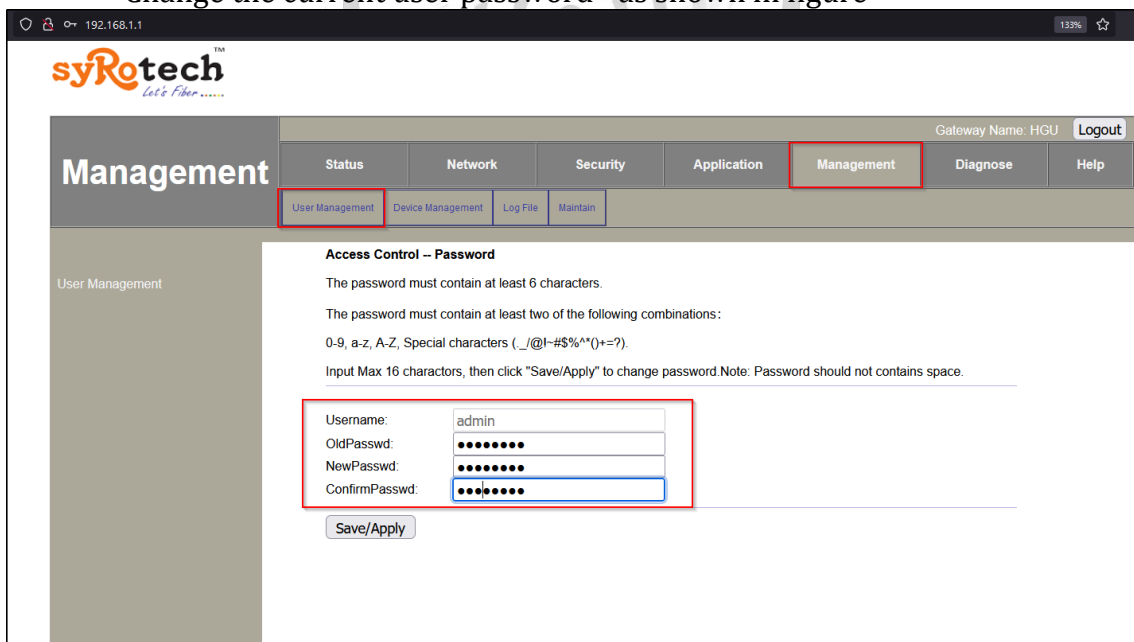


Figure Password Change

- iii. Verify that password is encrypted format while changing via web access.

b) CLI Access.

- i. In PuTTY, enter the ONT's IP address (192.168.1.1) in the "Host Name" field and set the port to your desired number (e.g., 22 for SSH). Then click "Open" and user is prompt to enter username "admin" and password "admin123" for login into the ONT.
- ii. To change the password of user "admin", execute the below command.
- iii. config account password user "admin" oldpasswd "admin123" newpasswd "admin@123"


```
>config account password user "admin" oldpasswd "admin123" newpasswd "admin@123"
arg_name:user
arg_value: admin
arg_name:oldpasswd
arg_value: admin123
arg_name:newpasswd
arg_value: admin@123
>
```

Figure Password Change via CLI access.

iv. Verify that password is encrypted format while changing via CLI access.

11.3.4 Evidence Provided: Password is not visible during password change over web interface.

The screenshot shows the syRotech web management interface. The 'Management' tab is active, and the 'User Management' sub-tab is selected. The 'Access Control - Password' section is displayed, showing password requirements and a form for changing the password. The form fields are masked with dots, indicating that the password is not visible during the change process.

- Password is visible during password change for SSH session.

```
>config account password user "admin" oldpasswd "admin123" newpasswd "admin@123"
arg_name:user
arg_value: admin
arg_name:oldpasswd
arg_value: admin123
arg_name:newpasswd
arg_value: admin@123
>
```

11.3.5 Test Observations

i. Test Case :01

- The tester verified that the password is not displayed in plain text format while login over the web interface.
- The tester verified that the password is not displayed in plain text while logging in through CLI. Hence, the test scenario is passed.

ii. Test Case:02

- The tester verified that the password is not displayed in plain text in Wi-Fi access. Hence, the test scenario is passed.

iii. Test Case:03

- The tester verified password security by confirming that passwords were not displayed in plain text during the web-based change process.
- The tester verified that the password is displayed in plain text while password change through CLI access. Hence, the test scenario is failed.

12 Test Results:

Sl. No	Test name	Actual Result
1.	Password text during login	
2.	Password text during Wi-Fi connection	
3.	Password text during password change	



2.2.8 TSTP for Evaluation of Removal of predefined or default authentication attributes

Optical Network Terminal (ONT) - PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.2.8
---	--------------------------	-----------------

<DUT Details: > GPON-ONT

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> **1.2 Authentication** Attribute Management
2. <Security Requirement No & Name: - 2.2.8: Removal of predefined or default authentication attributes
3. **Requirement Description:** ONU/ONT may come with predefined (by the vendor, developer or producer) authentication attributes such as password or cryptographic keys. ONU/ONT shall remove the predefined / default authentication attributes from its run-time configuration. Such predefined authentication attributes can be restored only through factory reset, preferably through operating a physical button.

4. DUT Confirmation Details:

The screenshot displays the syrotech web interface. At the top, the syrotech logo is visible. The main navigation bar includes tabs for Status, Network, Security, Application, Management, Diagnose, and Help. The 'Status' tab is active, showing a 'Gateway Name: HGU' and a 'Logout' button. Below the navigation bar, there are sub-tabs for Device Information, WAN Connection Info, User Information, VOIP Information, and Remote Management Status. The 'Device Basic Info' section is expanded, showing the following details:

Device Model	HGU
Device ID	8014A8-F32428014A8000000
Hardware Version	STD-ONU
Software Version	3.1.02-220505
Serial No	RTKG11111111



Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
FXS	1 Port(s)	Physical	FXS
GUI	-	Man-Machine	Syrotech

5. DUT Configuration: Factory reset the DUT

6. Pre-Condition: Documentation that lists each of the default accounts and also the path to access the run time configuration

7. Test objective: To verify DUT's predefined authentication attributed can be disabled or removed.

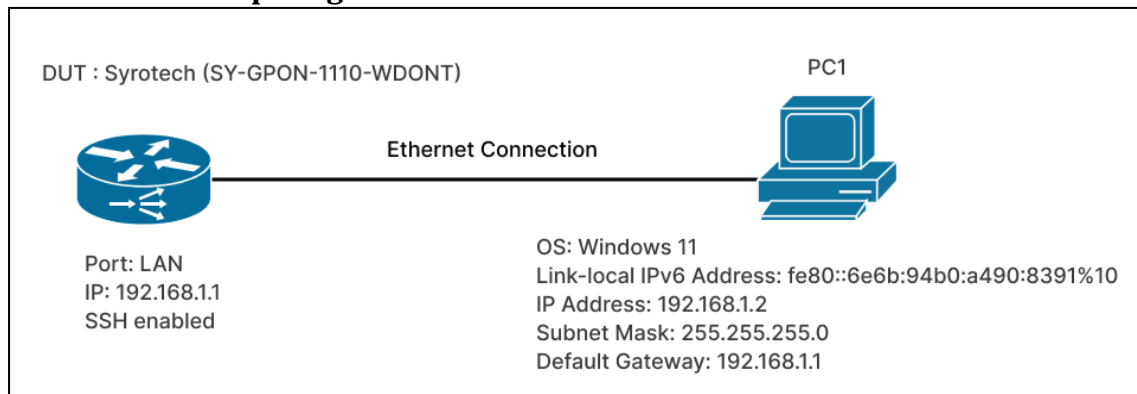
8. Test Plan

8.1 Test Cases:

8.1.1 Test case01: removal of predefined account or default authentication attributes

8.1.2 Test case02: Factory reset restoring

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: Nil

8.4 Test Execution steps

8.4.1 Test Case 1

- i. Initially, Reset the ONT by pressing a physical button.
- ii. Access the DUT
- iii. Now it will prompt to change the password for current logged in user (admin).
- iv. The system requires a new password to be set, this indicates that the system enforces automatic password changes as expected.
- v. Now set the new password and access the DUT
- vi. Also check the run time configuration to check the presence of the DUT default credentials

8.4.2 Test Case 2

- i. Reset the DUT
- ii. Post reset attempt to access the DUT with default credentials

9. Expected Results for Pass

- i. DUT should let the user change the default credentials of the user
- ii. Upon reset the default credentials should be restored

10. Expected Format of evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test case Name:** removal of predefined account or default authentication attributes

11.1.2 Test Case Description: The tester checks that the removal of predefined or default authentication attributes.

11.1.3 Execution Steps:

- i. Initially, Reset the ONT by pressing a physical button.
- ii. Now starting the ONT for the first time, to log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **admin** and password **Syro@43210\$** in the login dialog box.
- iii. Now it will prompt to change the password for current logged in user (admin) – as shown in figure 4.1.6.1.

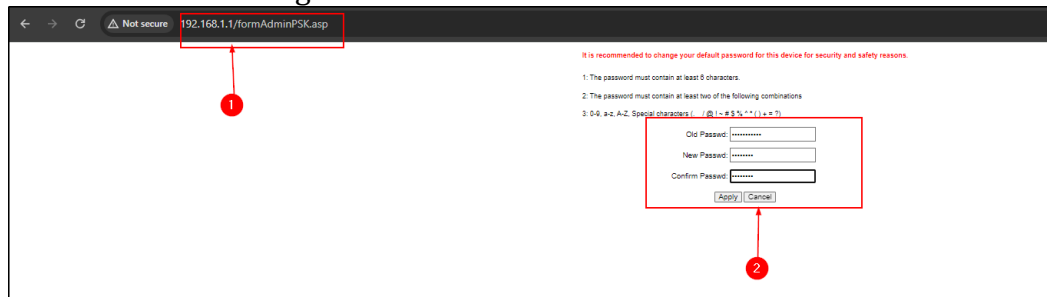


Figure No Default password change.

- iv. The system requires a new password to be set, this indicates that the system enforces automatic password changes as expected.
- v. Now set the new password as admin123 and confirm the password then logout. Login with newly set password – as shown in figure

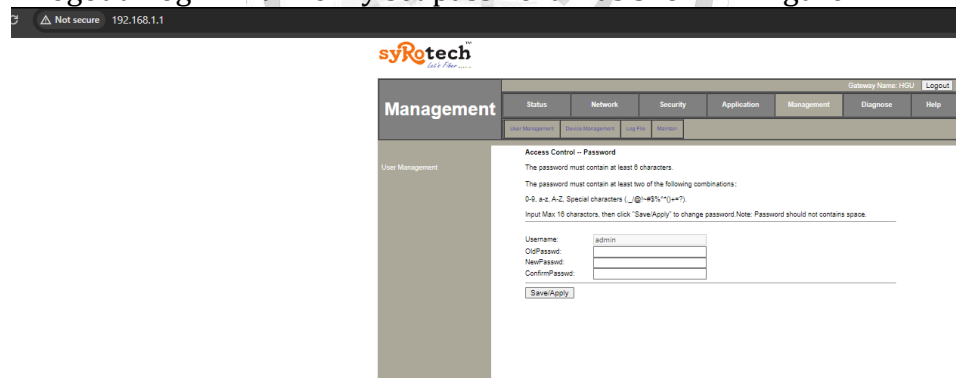
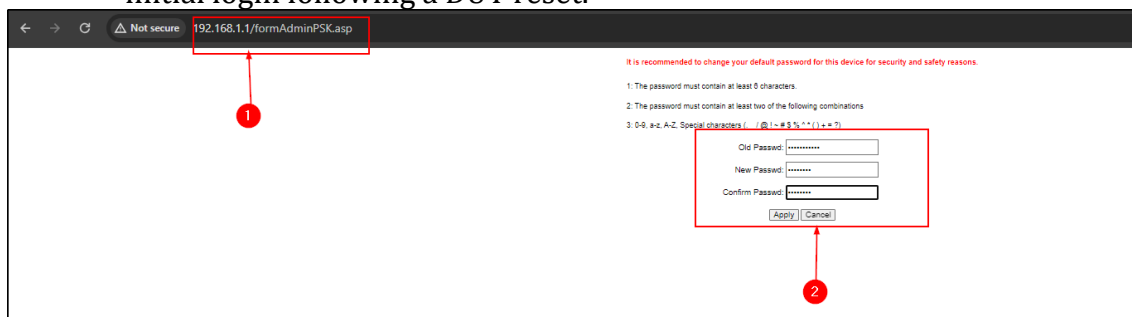


Figure No Check login post password change

11.1.4 Evidence Provided: The DUT prompts for a password change after the initial login following a DUT reset.



11.2 Test Case Number: 8.2

11.2.1 Test case Name: Factory reset restoring

11.2.2 Test Case Description: The tester verifies that predefined authentication attributes can be restored only through factory reset.

11.2.3 Execution Steps:

- i. To verify if the DUT accepts default attributes (like default password), navigate to Management > User management. Provide the old password as **admin123** and try to change the password to default password "**Syro@43210\$**" – as shown in figure

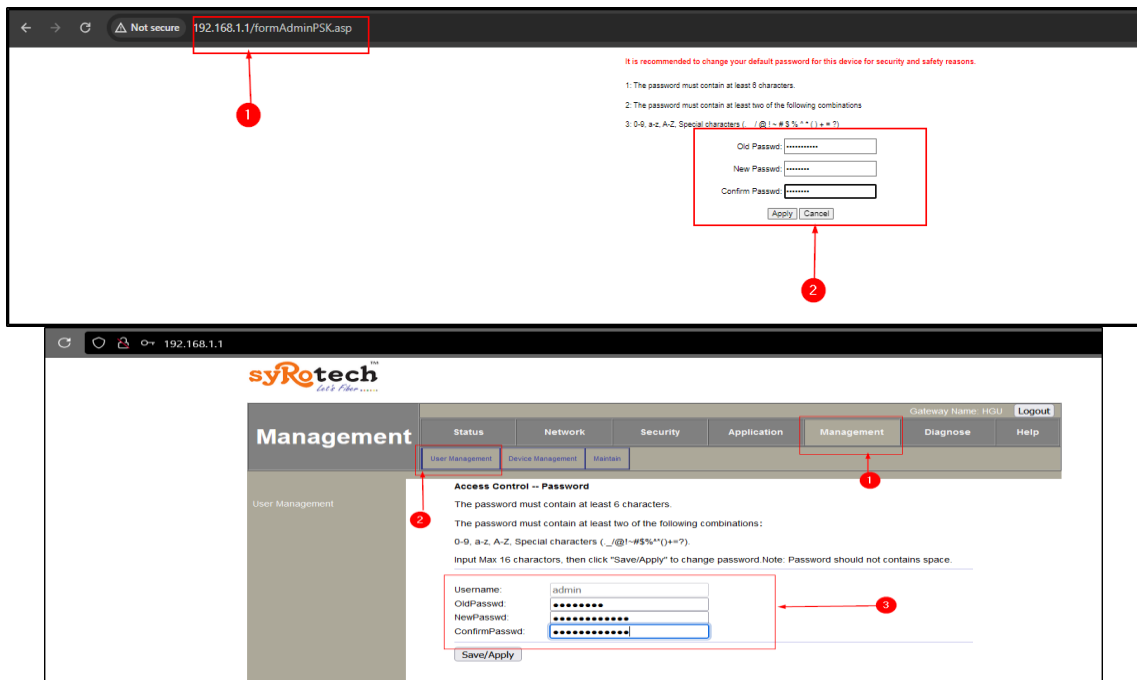


Figure – Change password from admin123 to Syro@3210\$

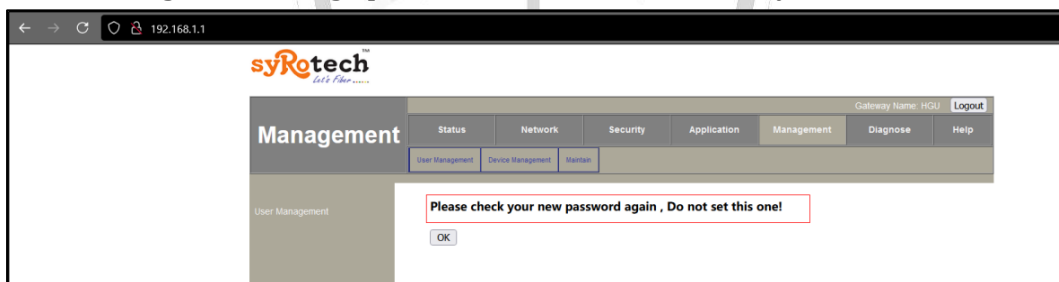
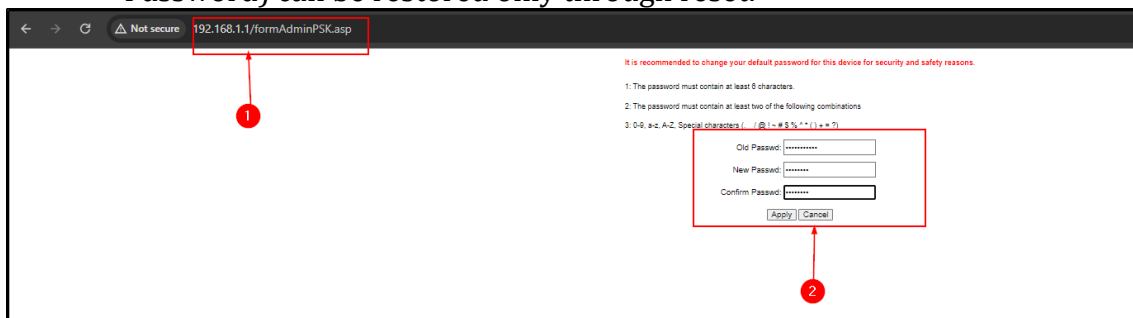


Figure DUT does not allow to set default password.

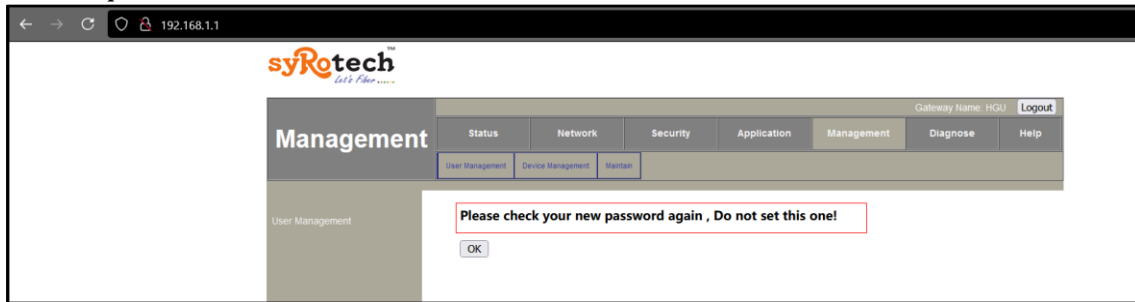
- ii. To check that the ONT authentication attributes can be restored through factory reset, Reset the ONT by pressing a physical button.
- iii. Post reset, log back into the admin account using predefined authentication attributes by entering the username as **admin** and password **Syro@43210\$** .– as shown in figure

Figure– Check default password is recovered/ asked after reset.

11.2.4 Evidence Provided: The predefined authentication attribute (i.e: Default Password) can be restored only through reset.



- i. The DUT does not accept default password when trying to change the password.

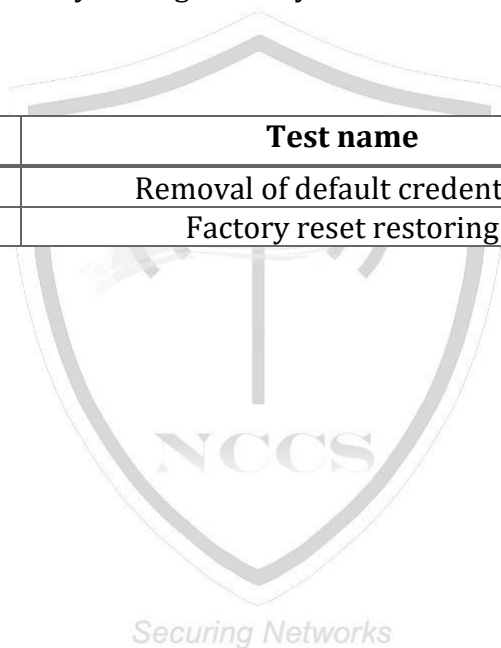


11.2.5 Test Observations

- i. **Test Case 01:** The DUT enforces a password change post reset on initial login. Hence the default credentials get changed
- ii. **Test Case 02:** The tester verified that predefined authentication attributes can be restored only through factory reset.

12. Test Result

ITSAR ONU-ONT No.	Test name	Actual Result
1.	Removal of default credentials	
2.	Factory reset restoring	



Section 3: Software Security

2.3.1 TSTP for Evaluation of Secure Update

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.1
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
DOCA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3: Software Security

2. **<Security Requirement No & Name >** 2. 3.1 Secure Update

3. **<Requirement Description: >** ONU's/ONT's system software updates shall be carried out strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only. ONU/ONT shall allow updates only if code signing certificate is valid and not time expired. Software update integrity shall be verified strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

4. **DUT Confirmation Details:**

- Use the command line/GUI interface to get details of the machine on which test is conducted.
- Use GUI to get Application No/Version No & hardware Info
- The below screenshot shows the firmware version of the DUT

5. DUT Configuration:

- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.

The screenshot shows the DIGISOL web interface at the URL <https://192.168.1.1>. The main menu includes Status, Network, Security, Application, Management, Diagnostics, and Help. Under the Status menu, there are links for Device Info, WAN Info, User Info, Voip Info, and Remote Manage Info. The left sidebar has links for WLAN Info and LAN Info. The main content area displays the following information:

- Device Info:** IP Address: 192.168.1.1, MAC Address: 00177caa069e.
- LAN Port Status:** A table showing the status of LAN ports. Port_2 is highlighted with a red box.
- Send and Recv:** A table showing network statistics for Port_1 and Port_2.
- Active DHCP Clients:** A table with columns for Device Type, MAC Address, IP Address, and Lease Time.

Interface	State	Speed	Mode
Port_1	down	--	--
Port_2	up	1000 M	Full duplex

Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
Port_1	2079	467487	0	0	2204	636909	0	0
Port_2	784	171280	0	0	608	204454	0	0

- ii. HTTPS is enabled.

The screenshot shows the DIGISOL web interface at the URL <https://192.168.1.1>. The main menu includes Status, Network, Security, Application, Management, Diagnostics, and Help. Under the Security menu, there are links for WAN Access, Firewall, MAC Filtering, and IP/Port Filtering. The left sidebar has links for IP/Port Filtering and Common Filtering. The main content area displays the following information:

- IP/Port Filtering:** A table showing the configuration for common ports. The HTTPS row is highlighted with a red box.
- Submit:** A button to save the configuration.

Service-Name	LAN	WAN	Port	Remote Host
Telnet	☐	☐	23	
Flp	☐	☐	21	
Http	☒	☒	80	
HTTPS	☒	☒	443	
Ping	☒	☐		

- iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~
aravind@Aravind_V:~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN

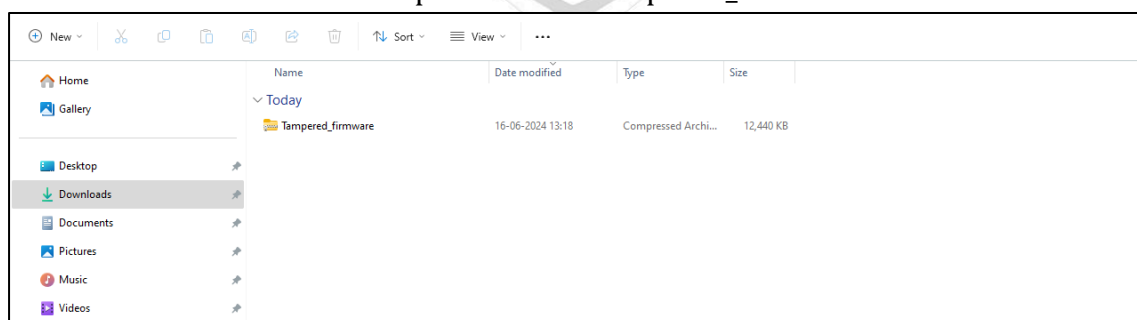
aravind@Aravind_V:~$

```

6. **Precondition:** OEM should provide document regarding how many modes the DUT firmware/software can be updated. OEM should provide the firmware/software file for software update. For negative testcase, tester should have Tampered firmware image file in the tester machine for software update. To create a tampered firmware file, open the firmware file in HxD. Replace random values from the hexa-decimal file, and then save it as a new file (Tampered_firmware.tar). This will tamper with the integrity of the file.



Save the tampered file as Tampered_firmware.tar



7. **Test Objective:** To verify that DUT have mechanism that validates the software package integrity based on digital signature during installation/update stage

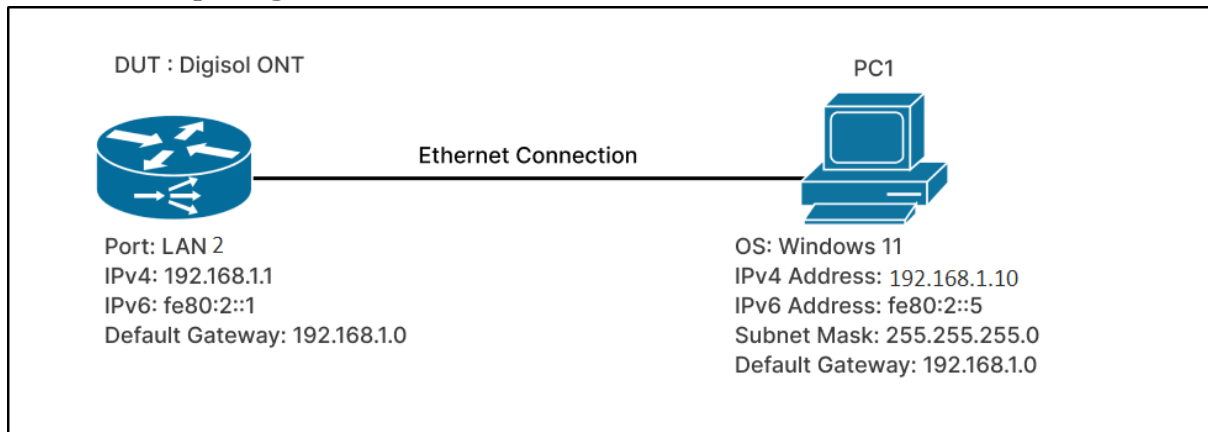
8. Test Plan:

8.1 Number of Test Case Scenarios: 4

8.1.1 Test case01: Verify that the network product enforces secure software updates based on signed certificates and code integrity verification for correct firmware.

- 8.1.2 Test case02: Verify that the code signing certificate associated with the update package is valid and not expired.
- 8.1.3 Test case03: Verify that the network product enforces secure software updates based on signed certificates and code integrity verification for tampered software.
- 8.1.4 Test case04: Verify that a low-privilege user cannot perform update/upgrade actions.

8.2 Test Setup Diagram



8.3 Tools Used: HxD, Web browser (For access GUI of DUT)

8.4 Test Execution Steps

- 8.4.1 **Test case01:** Verify that the network product enforces secure software updates based on signed certificates and code integrity verification for correct firmware.
- To log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username as admin and password is admin123 in the login dialog box.
 - Navigate to Management > Device Manage > Update Image.
 - To browse the firmware image to Update, click on the "Browse" button and select the firmware to Update and click on "Update".
 - The Update process will start, and the DUT will be automatically rebooted post Update.
- Note: Before initiating the software update process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required to explain the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by the DUT.
- 8.4.2 **Test case02:** Verify that the code signing certificate associated with the update package is valid and not expired.
- Note: The ONT does not provide access to viewing the code signing certificate associated with the update package. Hence, OEM documentation is required explaining the code signing certificate used for the specific DUT and its firmware.

- Access the ONT Management Interface:

i. Connect to the ONT:

- Ensure your computer is connected to the ONT via Ethernet or Wi-Fi.

ii. Open a Web Browser:

- Open a web browser and enter the ONT's management IP address (e.g., <http://192.168.1.1>).

iii. Log In:

- Enter the login credentials. The default username and password are often provided in the ONT's manual or on the device itself.

b) Navigate to the Firmware or Software Update Section:

i. Locate the Firmware Section:

- Once logged in, navigate to the section related to firmware updates. This is often found under "System", "Administration", "Maintenance", or a similar menu.

ii. View Current Firmware:

- In the firmware section, you should see the currently installed firmware version and details about its digital signature.

c) View the Code Signing Certificate:

i. View Digital Signature Details:

- Look for options like "Signature", "Certificate", "Details", or "Verify" related to the firmware. These options will display the digital signature and certificate information.

ii. Check Certificate Information:

- Click on the details to view the issuer, subject, validity period, and other relevant details of the code signing certificate.

8.4.3 Test Case02: Verify that the network product enforces secure software updates based on signed certificates and code integrity verification for tampered software.

- To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username admin, password admin@123 and verification code in the login dialog box.
 - Checking the hash of the tampered firmware (Tampered firmware) using PowerShell by executing the following command.
 - Get-FileHash LoadDef_HG323DACv2_all_V2.1.08-240403_Digisolver.tar
 - Get-FileHash Tampered_firmware.tar
 - To enable maintain mode, navigate to management > maintain and click End maintain.
 - Then navigate to Update image > browser > upload the tampered file (Tampered_firmware.tar) and click Update.
 - Wait until the ONT reboots.
- Note: Before initiating the software update process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required to explain the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by the DUT.

8.4.4 Verify that a low-privilege user cannot perform update/upgrade actions.

- i. To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username user, password user@123 and verification code in the login dialog box.
- ii. Navigate to management > device manage.
- iii. Verify that the low-privilege user cannot perform update or upgrade actions.

9. **Expected Results for Pass:** Software package integrity shall be validated using cryptographic means, e.g. Digital certificate (digital signature) in the installation/upgrade stage. Tampered software shall not be executed or installed if integrity check fails. Only authorized person, can able to do software update.

10. **Expected Format of Evidence:** Screenshots of terminal

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test Case Description:** The tester verifies that the secure software updates based on signed certificates and code integrity verification for correct firmware.

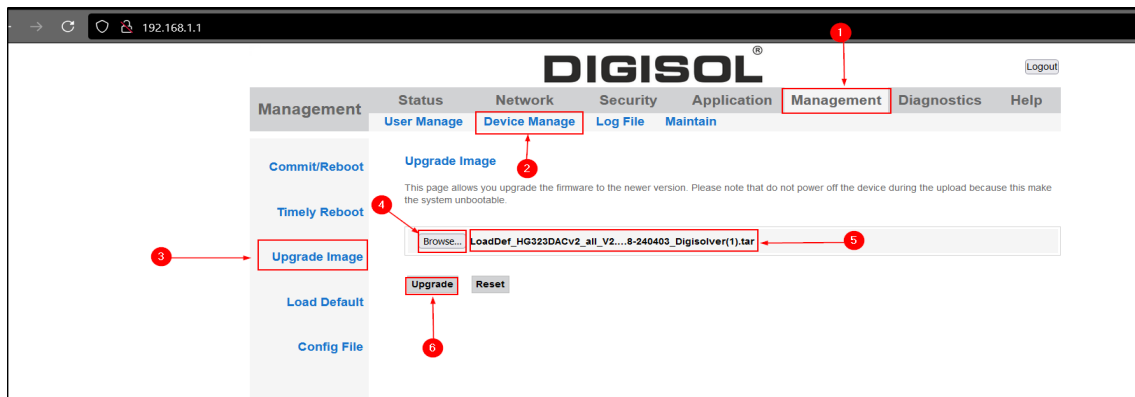
11.1.2 Execution Steps:

- i. To log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username as admin and password is admin123 in the login dialog box.
- ii. Navigate to Status and check the software version



iii. Navigate to Management-> Device Manage -> Upgrade Image.

iv. To browse the firmware image to Update, click on the "Browse" button and select the firmware to Update and click on "Update".



Firmware update initiation.'

- v. The Update process will start, and the DUT will be automatically rebooted post Update.
- vi. Navigate to Status and check the software version for whether software update is done or not.
 - o Note: Before initiating the software update process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required explaining the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by DUT.

11.2 Test Case Number: 02

11.2.1 **Test Case Description:** Verify that the code signing certificate associated with the update package is valid and not expired.

11.2.2 Execution Steps:

- o **Note:** The ONT does not provide access to viewing the code signing certificate associated with the update package. Hence, OEM documentation is required explaining the code signing certificate used for the specific DUT and its firmware.
- a) Access the ONT Management Interface:
 - i. Connect to the ONT:
 - o Ensure your computer is connected to the ONT via Ethernet or Wi-Fi.
 - ii. Open a Web Browser:
 - o Open a web browser and enter the ONT's management IP address (e.g., http://192.168.1.1).
 - iii. Log In:
 - o Enter the login credentials. The default username and password are often provided in the ONT's manual or on the device itself.
- b) Navigate to the Firmware or Software Update Section:
 - i. Locate the Firmware Section:
 - o Once logged in, navigate to the section related to firmware updates. This is often found under "System", "Administration", "Maintenance", or a similar menu.
 - ii. View Current Firmware:
 - o In the firmware section, you should see the currently installed firmware version and details about its digital signature.

c) View the Code Signing Certificate:

i. View Digital Signature Details:

- o Look for options like "Signature", "Certificate", "Details", or "Verify" related to the firmware. These options will display the digital signature and certificate information.

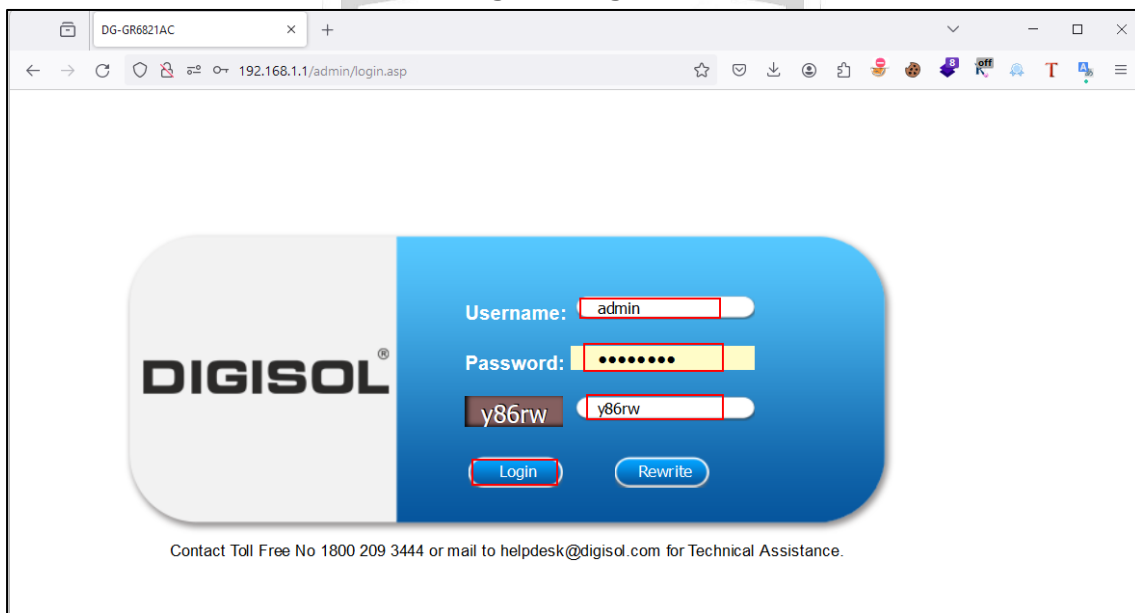
ii. Check Certificate Information:

- o Click on the details to view the issuer, subject, validity period, and other relevant details of the code signing certificate.

11.3 Test Case Number: 03

11.3.1 Test Case Description: The tester checks that the network product enforces secure software updates based on signed certificates and code integrity verification for tampered software.

11.3.2 Execution Steps: To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **admin**, password **admin@123** and **verification code** in the login dialog box.



Given username, password and verification code on login page.

- Checking the hash of the tampered firmware (Tampered_firmware) using PowerShell by executing the following command
- Get-FileHash LoadDef_HG323DACv2_all_V2.1.08-240403_Digisolver.tar
- Get-FileHash Tampered_firmware.tar

```
Windows PowerShell
PS C:\Users\AravindV\Downloads\12.3> Get-FileHash LoadDef_HG323DACv2_all_V2.1.08-240403_Digisolver.tar

Algorithm      Hash
-----
SHA256         DC5E1F822E3B838B7546D77DE8116648AAF0DCA4F823AEAE417EA1F8D6114B8E
Path           C:\Users\AravindV\Downloads\1...

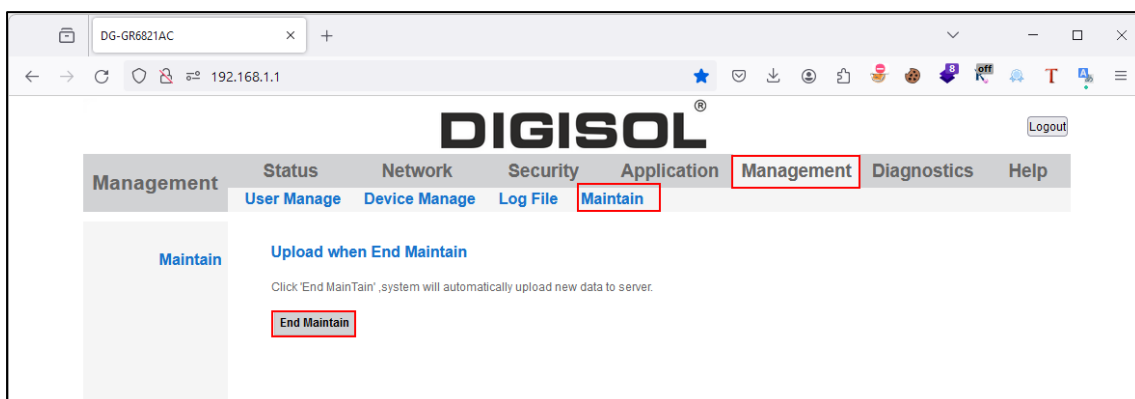
PS C:\Users\AravindV\Downloads\12.3> Get-FileHash Tampered_firmware.tar

Algorithm      Hash
-----
SHA256         40859EB7123A63447AA0A074E145F0A09053CE336FA510ACC7E39AE1DBED83F5
Path           C:\Users\AravindV\Downloads\1...

PS C:\Users\AravindV\Downloads\12.3> |
```

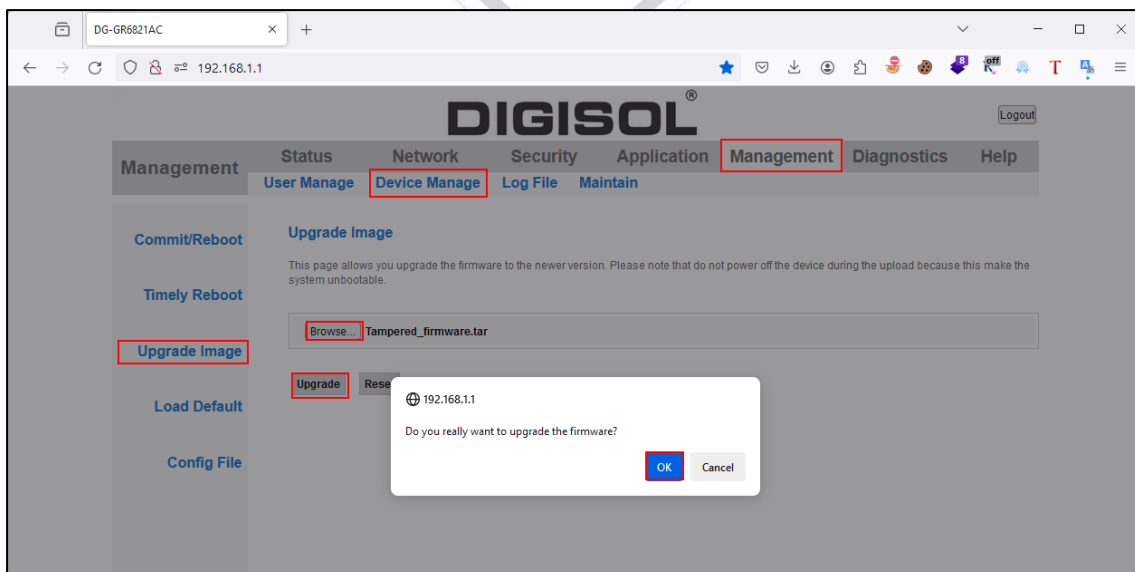
Compare tampered hash value with download option.

- iv. To enable maintain mode, navigate to management > maintain and click End maintain.

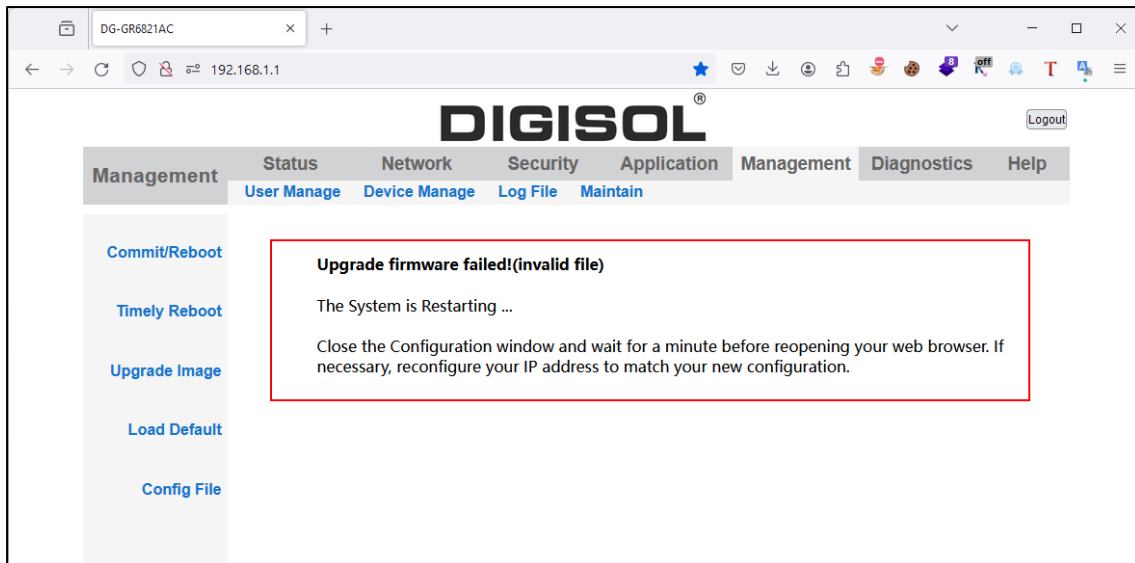


Enable maintain mode before update firmware.

- v. Then navigate to Update image > browser > upload the tampered file (Tampered_firmware.tar) and click Update - as shown in figure Wait until the ONT reboots.



Upload the tampered firmware file.



Reboot the ONT.

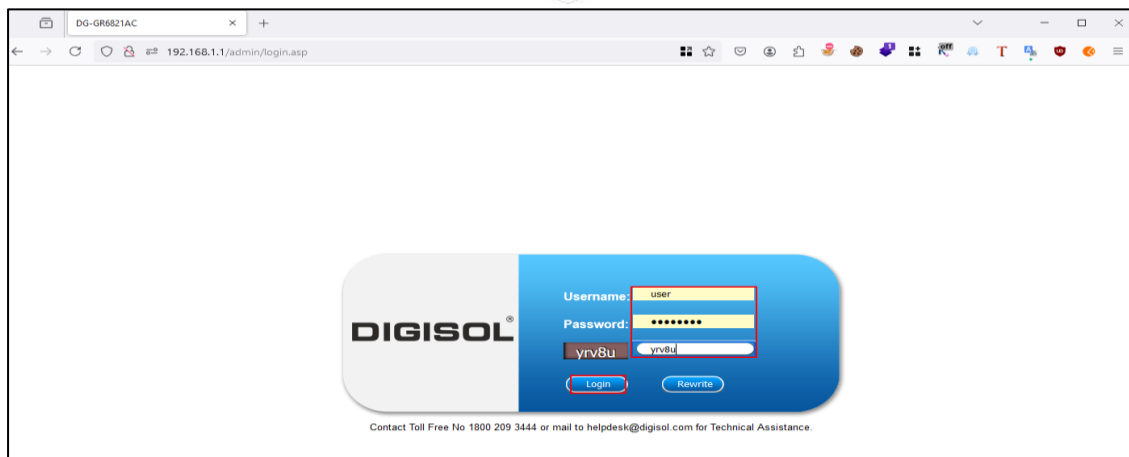
- **Note:** Before initiating the software update process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required to explain the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by the DUT

11.4 Test Case Number: 04

11.4.1 Test Case Description: The tester should add a test case to verify that an low-privilege user cannot perform update/upgrade actions.

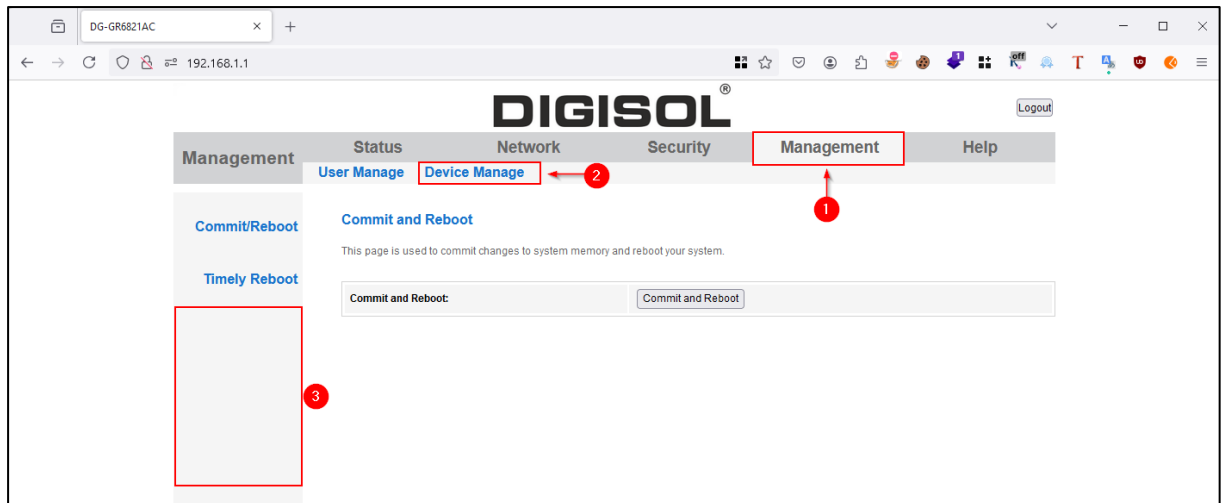
11.4.2 Execution Steps:

- i. To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **user**, password **user@123** and verification code in the login dialog box.



low privilege user login

- ii. Navigate to management > device manage



- iii. verify low privilege cannot perform update/upgrade.
- iv. Verify that the low-privilege user cannot perform update or upgrade actions.

11.4.3 Test Observation:

i. Test case01:

- The DUT successfully does checks and updates the DUT firmware but the integrity check, hashing mechanism and digital certificates are not visible to check the security controls of the mechanisms used.
- For this OEM documentation is required. Hence the testcase is "Not Tested."

ii. Test case02: Hence the testcase is "Not Tested."

iii. Test case03: The DUT successfully does checks and rejects the tampered DUT firmware but the integrity check, hashing mechanism and digital certificates are not visible to verify the security controls of the mechanisms used. For this OEM documentation is required. Hence the testcase is "Not Tested"

iv. Test case04: A low-privilege user does not have the option to perform updates or upgrades. Hence the testcase is Pass.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	01		
2	02		
3	03		
4	04		

2.3.2 TSTP for Evaluation of Secure Upgrade

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.2
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 3: Software Security

2. <Security Requirement No & Name > 2.3.2 Secure Upgrade

3. <Requirement Description: >

- (i) ONU/ONT Software package integrity shall be validated in the installation and upgrade stages strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.
- (ii) ONU/ONT shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the ONU/ONT shall have a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software upgrade is originated from only these sources.
- (iii) Tampered software shall not be executed or installed if integrity check fails.
- (iv) ONU's/ONT's software upgrades shall be carried out strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.
- (v) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5]

4. DUT Confirmation Details:

- i. Use the command line/GUI interface to get details of the machine on which test is conducted.
- ii. Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT

5. DUT Configuration:

- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.

DIGISOL Logout

Status | Network | Security | Application | Management | Diagnostics | Help

Device Info | WAN Info | User Info | Voip Info | Remote Manage Info

WLAN Info

LAN Info

Device Info

IP Address	192.168.1.1
MAC Address	00177caa069e

LAN Port Status

Interface	State	Speed	Mode
Port_1	down	--	--
Port_2	up	1000 M	Full duplex

Send and Recv

Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
Port_1	2079	467487	0	0	2204	636909	0	0
Port_2	784	171280	0	0	608	204454	0	0

Active DHCP Clients

Device Type	MAC Address	IP Address	Lease Time
-------------	-------------	------------	------------

- ii. HTTPS is enabled.

DIGISOL Logout

Security | Status | Network | Security | Application | Management | Diagnostics | Help

WAN Access | Firewall | MAC Filtering | IP/Port Filtering

IP/Port Filtering

Common Filtering

This page configures the access control of common ports on the upstream and downstream directions; if you need to control other ports, please configure on the page of port filter.

Service-Name	LAN	WAN	Port	Remote Host
Telnet	☐	☐	23	
Ftp	☐	☐	21	
Http	☒	☒	80	
HTTPS	☒	☒	443	
Ping	☒	☐		

Submit

Web for Mobile

- iii. DUT is pre-configured with **BOA** as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~
aravind@Aravind_V:~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN

aravind@Aravind_V:~$

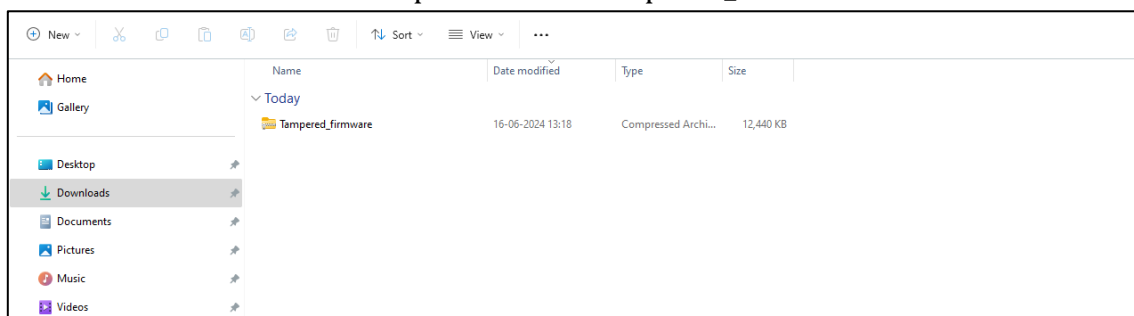
```

6. Precondition:

- OEM should provide document regarding how many modes the DUT firmware/software can be upgraded.
- OEM should provide the firmware/software file for software upgrade
- For negative testcase, tester should have Tampered firmware image file in the tester machine for software upgrade
- To create a tampered firmware file, open the firmware file in HxD. Replace random values from the hexa-decimal file, and then save it as a new file (Tampered_firmware.tar). This will tamper with the integrity of the file.



Save the tampered file as Tampered_firmware.tar



7. Test Objective: To verify that DUT have mechanism that validates the software package integrity based on digital signature during installation/upgrade stage

8. Test Plan:

8.1 Number of Test Case Scenarios: 4

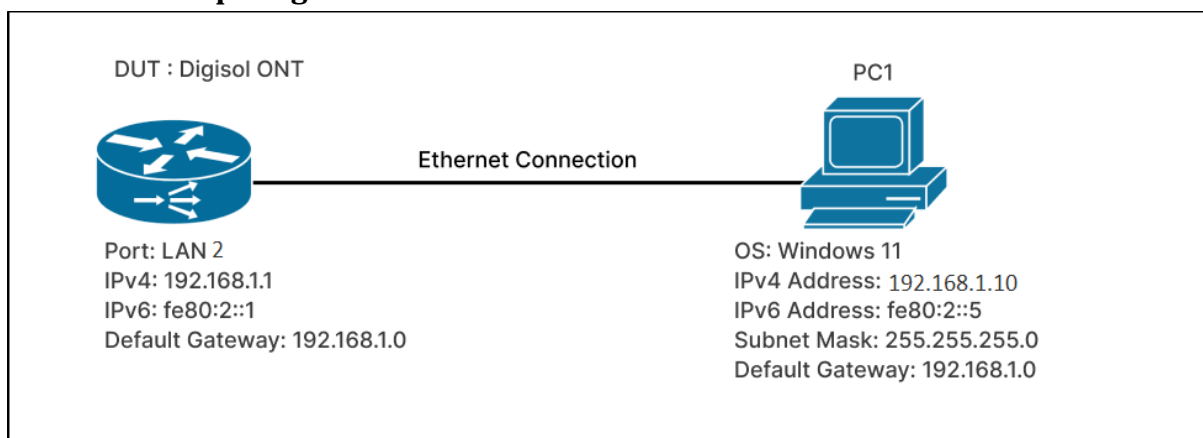
8.1.1 Test case01: Verify that the network product enforces secure software upgrades based on signed certificates and code integrity verification for correct firmware.

8.1.2 Test case02: Verify that the code signing certificate associated with the upgrade package is valid and not expired.

8.1.3 Test case03: Verify that the network product enforces secure software upgrades based on signed certificates and code integrity verification for tampered software.

8.1.4 Test case04: Verify that a low-privilege user cannot perform upgrade/upgrade actions.

8.2 Test Setup Diagram



8.3 Tools Used: HxD, Web browser (For access GUI of DUT)

8.4 Test Execution Steps

8.4.1 Test case:01 Verify that the network product enforces secure software upgrades based on signed certificates and code integrity verification for correct firmware.

- i. To log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username as admin and password is admin123 in the login dialog box.
- ii. Navigate to Management > Device Manage > Upgrade Image.
- iii. To browse the firmware image to Upgrade, click on the "Browse" button and select the firmware to Upgrade and click on "Upgrade".
- iv. The Upgrade process will start, and the DUT will be automatically rebooted post Upgrade.

➤ Note: Before initiating the software upgrade process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required to explain the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by the DUT.

8.4.2 **Test case 02:** Verify that the code signing certificate associated with the upgrade package is valid and not expired.

➤ Note: The ONT does not provide access to viewing the code signing certificate associated with the upgrade package. Hence, OEM documentation is required explaining the code signing certificate used for the specific DUT and its firmware.

➤ Sample steps

(A) Access the ONT Management Interface:

1. Connect to the ONT:
 - Ensure your computer is connected to the ONT via Ethernet or Wi-Fi.
2. Open a Web Browser:
 - Open a web browser and enter the ONT's management IP address (e.g., <http://192.168.1.1>).
3. Log In:
 - Enter the login credentials. The default username and password are often provided in the ONT's manual or on the device itself.

(B) Navigate to the Firmware or Software Upgrade Section:

1. Locate the Firmware Section:
 - Once logged in, navigate to the section related to firmware upgrades. This is often found under "System", "Administration", "Maintenance", or a similar menu.
2. View Current Firmware:
 - In the firmware section, you should see the currently installed firmware version and details about its digital signature.

(C) View the Code Signing Certificate:

1. View Digital Signature Details:
 - Look for options like "Signature", "Certificate", "Details", or "Verify" related to the firmware. These options will display the digital signature and certificate information.
2. Check Certificate Information:
 - Click on the details to view the issuer, subject, validity period, and other relevant details of the code signing certificate.

8.4.3 Test case03: Verify that the network product enforces secure software upgrades based on signed certificates and code integrity verification for tampered software.

Securing Networks

- i. To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username admin, password admin@123 and verification code in the login dialog box.
- ii. Checking the hash of the tampered firmware (Tampered firmware) using PowerShell by executing the following command.
 - a. `Get-File Hash LoadDef_HG323DACv2_all_V2.1.08-240403_Digisolver.tar`
 - b. `Get-FileHash Tampered_firmware.tar`
- iii. To enable maintain mode, navigate to management > maintain and click End maintain.
- iv. Then navigate to Upgrade image > browser > upload the tampered file (Tampered_firmware.tar) and click Upgrade.
- v. Wait until the ONT reboots.

- Note: Before initiating the software upgrade process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required to explain the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by the DUT.

8.4.4 Test case04: verify that a low-privilege user cannot perform upgrade/upgrade actions.

- i. To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username user, password user@123 and verification code in the login dialog box.
- ii. Navigate to management > device manage.
- iii. Verify that the low-privilege user cannot perform upgrade or upgrade actions.

9. Expected Results for Pass: Software package integrity shall be validated using cryptographic means, e.g. Digital certificate (digital signature) in the installation/upgrade stage. Tampered software shall not be executed or installed if integrity check fails. Only authorized person, can able to do software upgrade.

10. Expected Format of Evidence: Screenshots of GUI, log

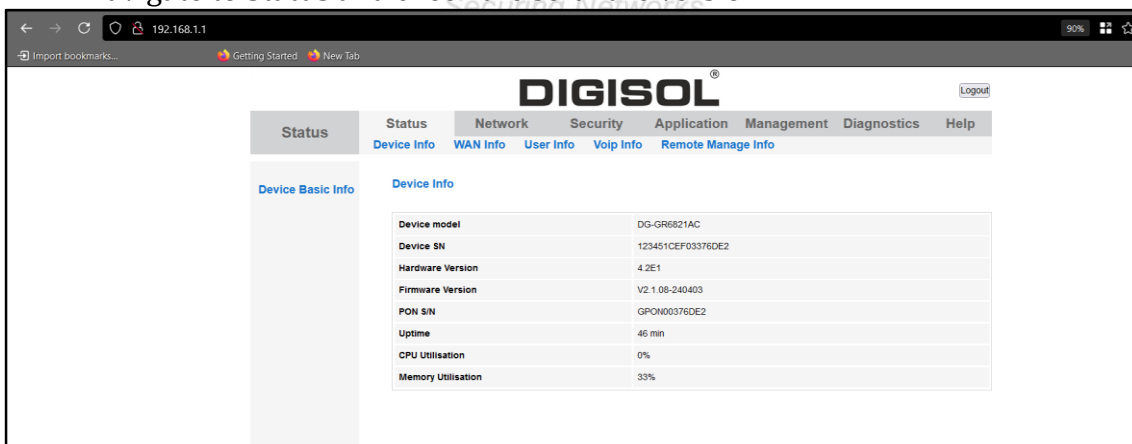
11. Test Execution:

11.1 Test Case Number: 01

11.1.1 Test Case Description: The tester verifies that the secure software upgrades based on signed certificates and code integrity verification for correct firmware.

11.1.2 Execution Steps:

- i. To log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username as **admin** and password is **admin123** in the login dialog box.
- ii. Navigate to Status and check the software version



- iii. Navigate to Management-> Device Manage -> Upgrade Image.
- iv. To browse the firmware image to Upgrade, click on the "Browse" button and select the firmware to Upgrade and click on "Upgrade" – as shown in figure



Firmware upgrade initiation.'

- v. The Upgrade process will start, and the DUT will be automatically rebooted post Upgrade.
- vi. Navigate to Status and check the software version for whether software upgrade is done or not
- **Note:** Before initiating the software upgrade process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required explaining the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by DUT.

11.2 Test Case Number: 02

11.2.1 **Test Case Description:** Verify that the code signing certificate associated with the upgrade package is valid and not expired.

11.2.2 Execution Steps:

- **Note:** The ONT does not provide access to viewing the code signing certificate associated with the upgrade package. Hence, OEM documentation is required explaining the code signing certificate used for the specific DUT and its firmware.

1. Access the ONT Management Interface:

- a) Connect to the ONT:
 - Ensure your computer is connected to the ONT via Ethernet or Wi-Fi.
- b) Open a Web Browser:
 - Open a web browser and enter the ONT's management IP address (e.g., http://192.168.1.1).
- c) Log In:
 - Enter the login credentials. The default username and password are often provided in the ONT's manual or on the device itself.

2. Navigate to the Firmware or Software Upgrade Section:

- a) Locate the Firmware Section:
 - Once logged in, navigate to the section related to firmware upgrades. This is often found under "System", "Administration", "Maintenance", or a similar menu.
- b) View Current Firmware:

- In the firmware section, you should see the currently installed firmware version and details about its digital signature.

3. View the Code Signing Certificate:

- a) View Digital Signature Details:
 - Look for options like "Signature", "Certificate", "Details", or "Verify" related to the firmware. These options will display the digital signature and certificate information.
- b) Check Certificate Information:
 - Click on the details to view the issuer, subject, validity period, and other relevant details of the code signing certificate.

11.3 Test Case Number: 03

11.3.1 **Test Case Description:** The tester checks that the network product enforces secure software upgrades based on signed certificates and code integrity verification for tampered software.

11.3.2 **Execution Steps:** To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **admin**, password **admin@123** and **verification code** in the login dialog box as shown in figure

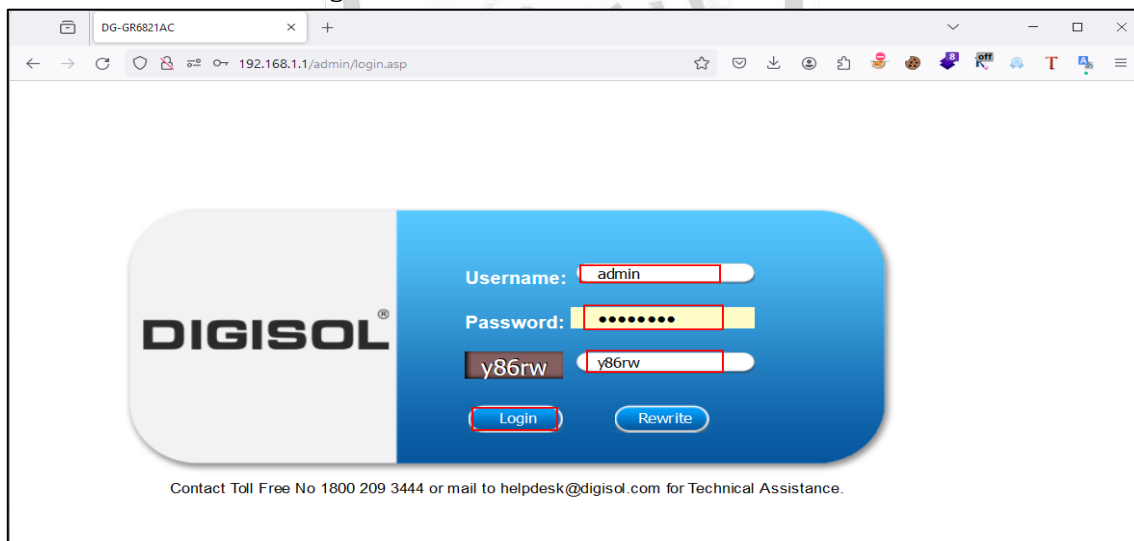


Figure: given username, password and verification code on login page.

- i. Checking the hash of the tampered firmware (Tampered firmware) using PowerShell by executing the following command- as shown in the figure
- ii. `Get-FileHash LoadDef_HG323DACv2_all_V2.1.08-240403_Digisolver.tar`
- iii. `Get-FileHash Tampered_firmware.tar`

```

Windows PowerShell
PS C:\Users\AravindV\Downloads\12.3> Get-FileHash LoadDef_HG323DACv2_all_V2.1.08-240403_Digisolver.tar

Algorithm      Hash
-----
SHA256         DC5E1F822E3B838B7546D77DE8116648AAFD9CA4F823AEAE417EA1F8D6114B8E
Path
C:\Users\AravindV\Downloads\1...

PS C:\Users\AravindV\Downloads\12.3> Get-FileHash Tampered_firmware.tar

Algorithm      Hash
-----
SHA256         40859EB7123A63447AA0A074E145F0A09053CE336FA510ACC7E39AE1DBED83F5
Path
C:\Users\AravindV\Downloads\1...

PS C:\Users\AravindV\Downloads\12.3> |

```

Figure - Compare tampered hash value with download option

- iv. To enable maintain mode, navigate to management > maintain and click End maintain as shown in the figure

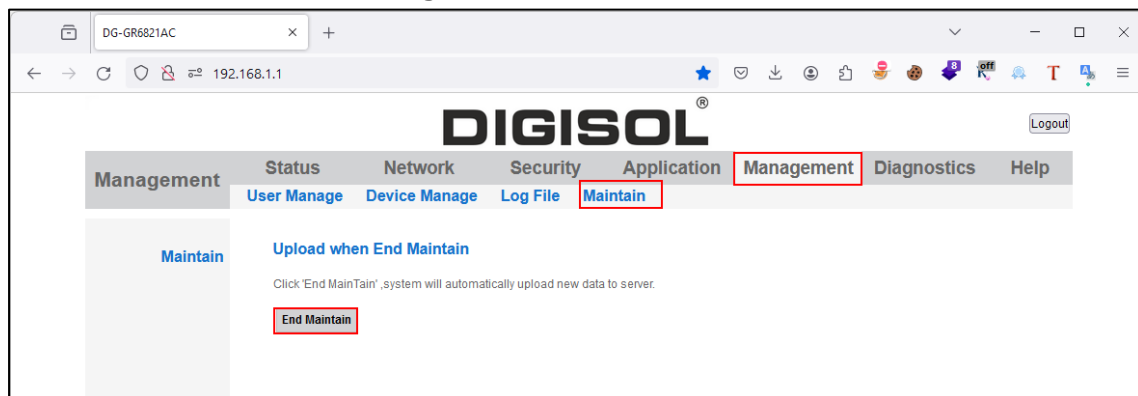


Figure: Enable maintain mode before upgrade firmware.

- v. Then navigate to Upgrade image > browser > upload the tampered file (Tampered_firmware.tar) and click Upgrade - as shown in figure

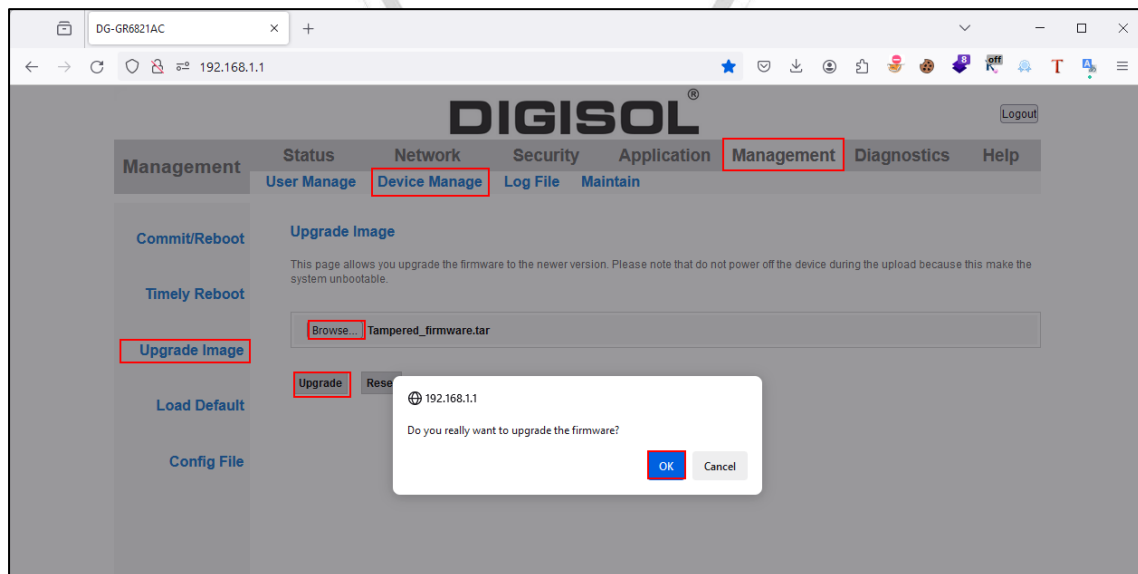


Figure- Upload the tampered firmware file.

- vi. Wait until the ONT reboots - as shown in figure

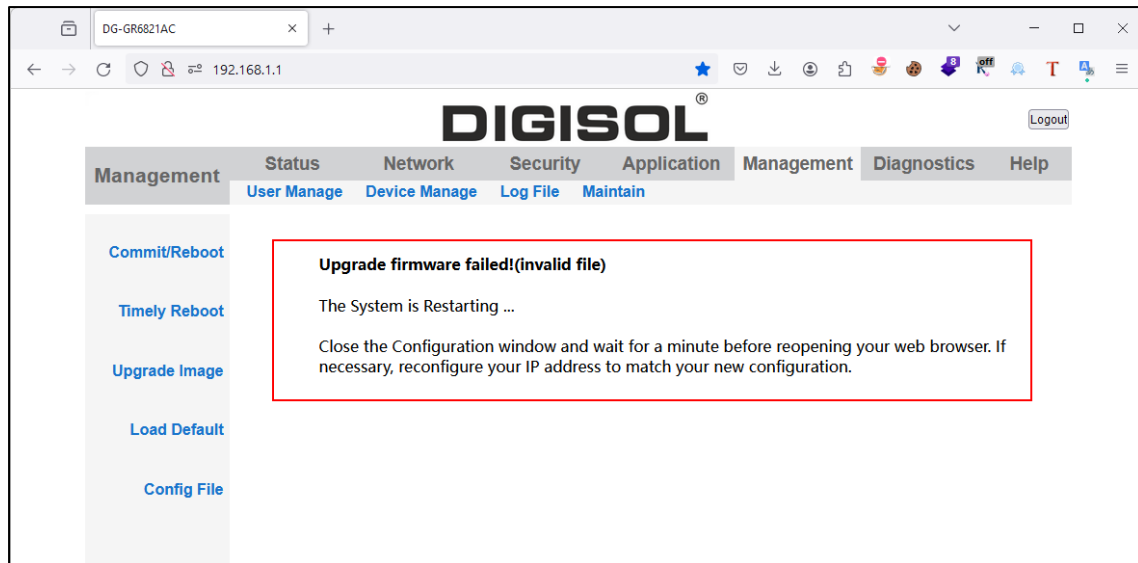


Figure - Reboot the ONT.

- **Note:** Before initiating the software upgrade process, the DUT performs integrity check, but the same is not visible and hence cannot be verified by the tester. Hence, OEM documentation is required to explain the details clarifying the Digital Certificate used for authenticity and hashing mechanism used for integrity verification by the DUT.

11.4 Test Case Number: 04

11.4.1 **Test Case Description:** The tester should add a test case to verify that an low-privilege user cannot perform upgrade/upgrade actions.

11.4.2 Execution Steps:

- i. To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **user**, password **user@123** and verification code in the login dialog box - as shown in figure

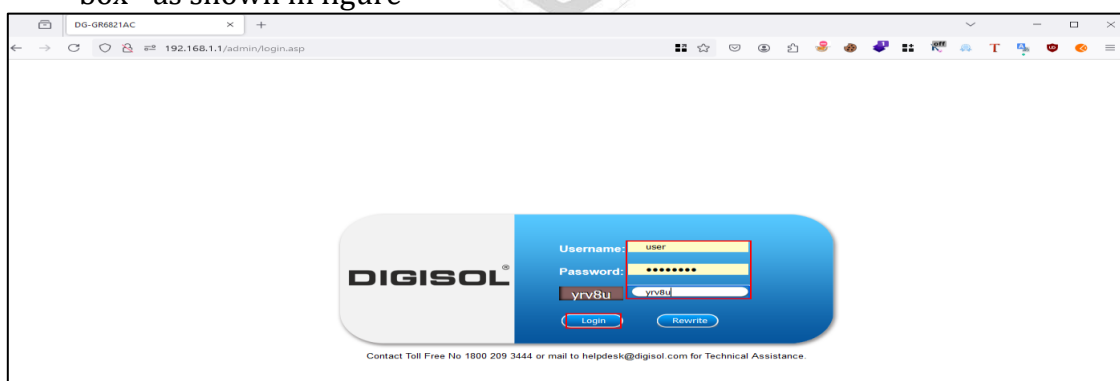


figure -low privilege user login

- ii. Navigate to management > device manage – as shown in figure

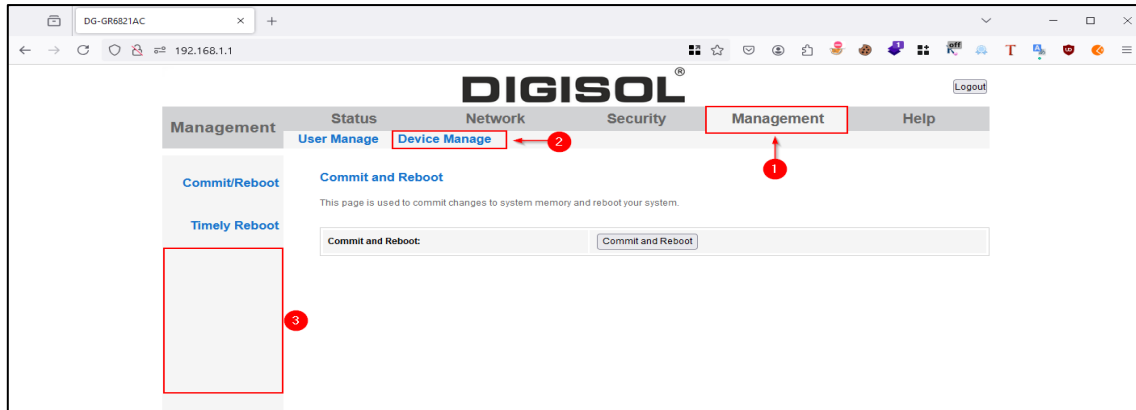


figure -verify low privilege cannot perform upgrade/upgrade.

iii. Verify that the low-privilege user cannot perform upgrade or upgrade actions.

11.4.3 Test Observation:

- i. Test case03: The DUT successfully does checks and rejects the tampered DUT firmware but the integrity check, hashing mechanism and digital certificates are not visible to verify the security controls of the mechanisms used. For this OEM documentation is required. Hence the testcase is "Not Tested"
- ii. Test case04: A low-privilege user does not have the option to perform upgrades or upgrades. Hence the testcase is Pass.

13Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1			
2			
3			
4			

Securing Networks

2.3.3 TSTP for Evaluation of Source code security assurance

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.3
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1) <ITSAR Section No & Name> Section 3: Software Security

2) <Security Requirement No & Name > 2.3.3 Source code security assurance

3) <Requirement Description: >

- a) Vendor should follow best security practices including secure coding for software development. Source code shall be offered to designated TSTP for source code review. It may be supported by furnishing the Software Test Document (STD).
- b) Also, Vendor shall submit the undertaking as below: (i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the ONT/ONU software, which includes vendor developed code, third party software and open-source code libraries used/embedded in the ONT/ONU. (ii) The ONT/ONU software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of ONT/ONU to designated TSTP for testing. For other security weaknesses, OEM shall give mitigation plan. (iii) The binaries for ONT/ONU and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

4) **DUT Confirmation Details:**

- i. Use the command line/GUI interface to get details of the machine on which test is conducted.
- ii. Use GUI to get Application No/Version No & hardware Info
- iii. The below screenshot shows the firmware version of the DUT

192.168.1.1

Getting StartedNew Tab

Import bookmarks...

DIGISOL®

Logout

Status

StatusNetworkSecurityApplicationManagementDiagnosticsHelp

Device InfoWAN InfoUser InfoVoip InfoRemote Manage Info

Device Basic Info

Device Info

Device model	DG-GR6821AC
Device SN	1234510EF03376DE2
Hardware Version	4.2E1
Firmware Version	V2.1.08-240403
PON S/N	GPON00376DE2
Uptime	46 min
CPU Utilisation	0%
Memory Utilisation	33%



Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

- 5) **DUT Configuration:** Load the source code into tester's machine for source code analysis.
- 6) **Precondition:**
- i. OEM should provide undertaking as per the ITSAR requirement.
 - ii. OEM should provide source code of DUT software along with STD (Software Test Document) document.
- 7) **Test Objective:** To verify that the DUT software is free from recently published CWE top 25(SANS) & OWASP top 10 security weaknesses and very high CWE technical impacts (CWSS) related weaknesses.
- 8) **Test Plan:**
- 8.1 Number of Test Case Scenarios: 2
- 8.1.1 Test case01: Verify that the OEM undertaking provided for DUT software is as per the ITSAR requirement.
 - 8.1.2 Test case 02: Verify that DUT software doesn't have any OWASP top 10(latest), SANS top 25(latest) and very high CWE technical impacts (CWSS) related weaknesses with the support of STD
- 8.2 **Test Setup Diagram:** - NA
- 8.3 **Tools** Used A suitable source code analysis tool having support for the programming language of the source code & having capabilities to detect vulnerabilities as per the requirement clause.
- 8.4 **Test Execution Steps**
- 8.4.1 **Test case01:** Verify that the OEM undertaking provided for DUT software is as per the ITSAR requirement. Verify that the OEM given undertaking, as per the following paragraph
 - (i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the ONT/ONU software, which includes vendor developed code, third party software and open-source code libraries used/embedded in the ONT/ONU. (ii) The ONT/ONU software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of ONT/ONU to designated TSTP for testing. For other security weaknesses, OEM shall give mitigation plan. (iii) The binaries for ONT/ONU and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.
 - 8.4.2 **Test case02:** Verify that DUT software doesn't have any OWASP top 10(latest), SANS top 25(latest) and very high CWE technical impacts (CWSS) related weaknesses with the support of STD
 - i. Configure the source code analysis tool as per DUT software code bases.
 - ii. Perform source code analysis on source code of DUT software
 - iii. Generate report as per the ITSAR standard (OWASP top 10, SANS Top 25 and very high CWE)

9) Expected Results for Pass:

- i. The OEM undertaking as per the ITSAR requirement
- ii. The Source code analysis report shows the DUT software free from **OWASP top 10, SANS Top 25 and very high CWE**

10) Expected Format of Evidence: Screenshots of Tool configuration, STD report

11) Test Execution:

11.1 Test Case Number: 01

11.1.1 Test Case Description: The tester verifies that the OEM submitted undertaking as per ITSAR requirement.

11.1.2 Execution Steps: Verify that the OEM given undertaking, as per the following paragraph

- (i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the ONT/ONU software, which includes vendor developed code, third party software and open-source code libraries used/embedded in the ONT/ONU.
- (ii) The ONT/ONU software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of ONT/ONU to designated TSTP for testing. For other security weaknesses, OEM shall give mitigation plan.
- (iii) The binaries for ONT/ONU and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

11.2 Test Case Number: 02

11.2.1 Test Case Description: Verify that DUT software doesn't have any OWASP top 10(latest), SANS top 25(latest) and very high CWE technical impacts (CWSS) related weaknesses with the support of STD.

11.2.2 Execution Steps:

- i. Configure the source code analysis tool as per DUT software code bases.
- ii. Perform source code analysis on source code of DUT software
- iii. Generate report as per the ITSAR standard (OWASP top 10, SANS Top 25 and very high CWE)
- iv. Compare TSTP report with OEM STD document.

11.2.3 Test Observation: Not Tested

12) Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1			Not Tested
2			Not Tested

2.3.4 TSTP for Evaluation of Known Malware and backdoor Check

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR ITSAR403012311	No:	Clause no:2.3.4
---	-------------------------	-----	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

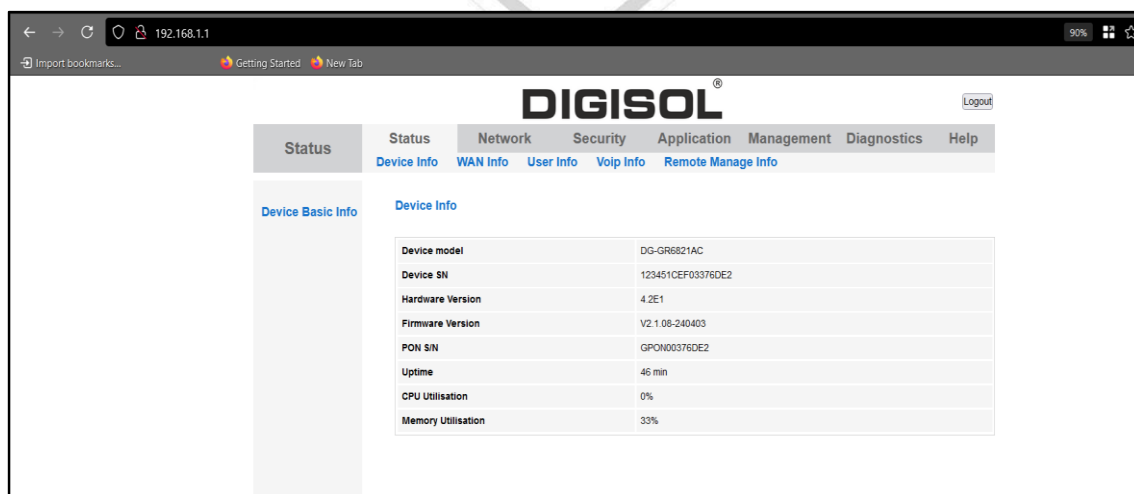
<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

- 1) **<ITSAR Section No & Name>** Section 3: Software Security
- 2) **<Security Requirement No & Name >** 3.4 Known Malware and backdoor Check
- 3) **<Requirement Description: >** Vendor shall submit an undertaking stating that ONU/ONT is free from all known malware and backdoors as on the date of offer to the TSTP for testing and shall submit Malware test document (MTD).
- 4) **DUT Confirmation Details:**
 - i. Use the command line/GUI interface to get details of the machine on which test is conducted.
 - ii. Use GUI to get Application No/Version No & hardware Info
 - iii. The below screenshot shows the firmware version of the DUT





Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5) **DUT Configuration: NA**

6) **Precondition:**

- OEM should provide undertaking as per the ITSAR requirement.
- OEM should provide malware test document (MTD) of DUT software.

7) **Test Objective:** To verify that there is no malware present on the DUT from date of testing

8) **Test Plan:**

8.1 Number of Test Case Scenarios: 2

8.1.1 Test case 01: Verify that the OEM undertaking provided for DUT software is as per the ITSAR requirement.

8.1.2 Test case 02: Verify that DUT software doesn't have any known malware based on MTD

8.2 Test Setup Diagram: - Based on OEM MTD testing

8.3 Tools **Used:** A suitable tool with malware database updated regularly

8.4 Test Execution Steps

8.4.1 Test case01:

- i. Verify that the OEM undertaking provided for DUT software is as per the ITSAR requirement.
- ii. Verify that the OEM given undertaking, as per the following para,
- iii. We are undertaking that ONU/ONT (DUT name with software version) is free from all known malware and backdoors as on the date.

8.4.2 **Test case 02:** Verify that DUT software doesn't have any known malware based on MTD

- i. Check the malware database updated date and malware scan date will be same or not (based on MTD)
- ii. Check malware scan directory coverage (what are the directories covered inside in the DUT software).
- iii. Check there is no known malware present on the DUT based on MTD

9) Expected Results for Pass:

- i. The OEM undertaking as per the ITSAR requirement
- ii. The MTD report showing there is no malware present on the DUT.

10) Expected Format of Evidence: Screenshots of Tool configuration, MTD Report

11) Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

11.1.2. Test Case Description: The tester verifies that the OEM submitted undertaking as per ITSAR requirement.

11.1.3. Execution Steps: Verify that the OEM given undertaking, as per the following paragraph, We are undertaking that ONU/ONT (DUT name with software version) is free from all known malware and backdoors as on the date.

11.2 Test Case Number: 02

11.2.1. Test Case Name: 8.1.2

11.2.2. Test Case Description: Verify that DUT software doesn't have any known malware based on MTD

11.2.3. Execution Steps:

- i. Check the malware database updated date and malware scan date will be same or not (based on MTD)
- ii. Check malware scan directory coverage (what are the directories covered inside in the DUT software).
- iii. Check there is no known malware present on the DUT based on MTD

11.2.4. **Test Observation:** Not Tested

12) **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not Tested
2	8.1.2		Not Tested



2.3.5 TSTP for Evaluation of No Unused software

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.5
---	--------------------------	-----------------

<DUT Details: > Syrotech SY-GPON-1110-WDONT (HGU)

<DUT Software Version:> 1.0.38-230104

<Digest Hash of OS> xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 3: Software Security

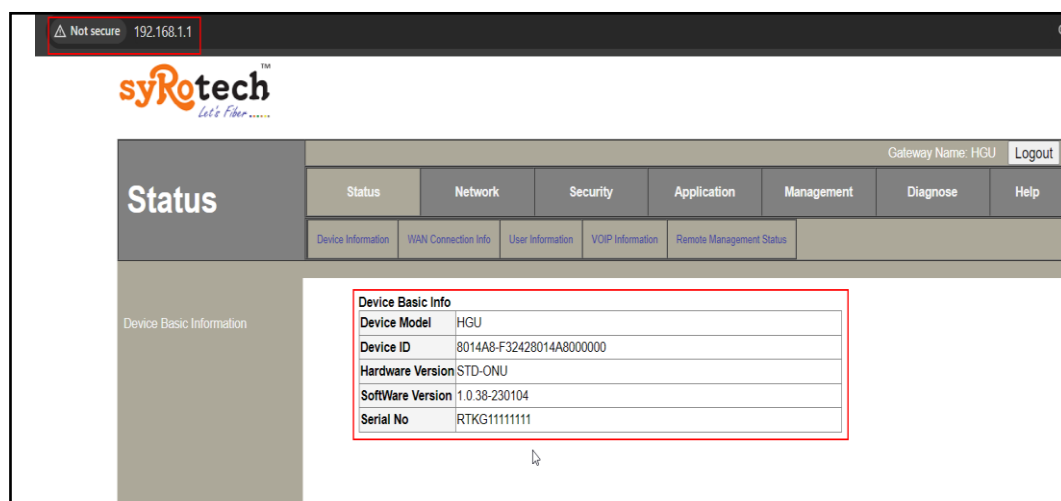
2. <Security Requirement No & Name > 2.3.5 No unused software

3. <Requirement Description: > Software components or parts of software which are not needed for operation or functionality of the ONT/ONU shall not be present. Orphaned software components /packages shall not be present in ONT/ONU. OEM shall provide the list of software that are necessary for its operation. OEM shall furnish an undertaking as "ONT/ONU does not contain Software that is not used in the functionality of ONT/ONU"

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.3]

4. DUT Confirmation Details:

- Use the command line/GUI interface to get details of the machine on which test is conducted.
- Use GUI to get Application No/Version No & hardware Info
- The below screenshot shows the firmware version of the DUT





Securing Networks

Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
FXS	1 Port(s)	Physical	FXS
GUI	-	Man-Machine	Syrotech

5. DUT Configuration:

- i. The DUT (IP:192.168.1.1) is connected with Lab's Testing Machine (IP:192.168.1.2) via LAN2.

Gateway Name: HGU Logout

Status

WLAN Interface Information

LAN Interface Information

Gateway Info:

IP Address: 192.168.1.1

MAC Address: 8014a8000000

Receive/Send Info:

Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
PORT_1	43	7002	0	0	136	13196	0	0
PORT_2	1411	199188	0	0	1298	435765	0	0

LAN Detect Status:

PORT	STATUS
LAN1	FAIL
LAN2	PASS

- ii. DUT is pre-configured with **SSID (FTTH-210F)** having Key "12345678".

syrotech
Let's Fiber.....

Gateway Name: HGU Logout

Network

WLAN Basic

WLAN Advanced

WLAN Security

WPS Configuration

WLAN Security Settings

SSID Type: FTTH-210F

Encryption: WPA2 Mixed

Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite: ☒ TKIP ☐ AES

WPA2 Cipher Suite: ☐ TKIP ☒ AES

Group Key Update Timer: 86400

Pre-Shared Key Format: Passphrase

Pre-Shared Key: *****

Apply Changes

- iii. DUT is pre-configured with **Boa** as a webserver having 0.93.15 version.

← ↻ ⚠ Not secure | 192.168.1.1

syrotech
Let's Fiber.....

Gateway Name: HGU Logout

Status

Device Basic Information

Device Basic Info

Device Model: HGU

Device ID: 8014A8-F32428014A800000

Hardware: STD-ONU

Version: 1.0.38-230104

Software Version: 1.0.38-230104

Serial No: RTKG11111111

12 requests: 18.0 kB transferred 18

192.168.1.1

commonjs

left_en.html

commonjs

UI_04.gif

top_en.asp

commonjs

background_top_en.gif

bar_top.gif

UI_05.gif

status_device_basic_info_en.asp

commonjs

General

Request URL: http://192.168.1.1/

Request Method: GET

Status Code: 200 OK

Remote Address: 192.168.1.1:80

Referrer Policy: strict-origin-when-cross-origin

Response Headers

Connection: close

Content-Length: 1462

Content-Type: text/html

Date: Thu, 01 Jan 1970 03:31:38 GMT

Last-Modified: Wed, 04 Jan 2023 08:56:13 GMT

Server: Boa/0.93.15

Request Headers

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

6. Precondition:

- 1.1.1. A list of all available software and libraries and associated components containing at least the following information shall be included in the OEM documentation accompanying the DUT(SBOM):
- 1.1.2. name of the software / library;
- 1.1.3. version of the software / library installed;

- 1.1.4. list of dependencies and versions;
- 1.1.5. any add-ons and functions;
- 1.1.6. any special hardware/debugging ports;
- 1.1.7. software support type;
- 1.1.8. licensing information;
- 1.1.9. brief description of their purpose.

1.1.10. OS level access is required

- 1.1.11. OEM should provide the list of software that are necessary for its operation
- 1.1.12. OEM should provide an undertaking as “ONT/ONU does not contain Software that is not used in the functionality of ONT/ONU”

7. Test Objective: To ensure that there is no unused software or associated components that might be installed in the network product which are not required for its operation or functionality.

8. Test Plan:

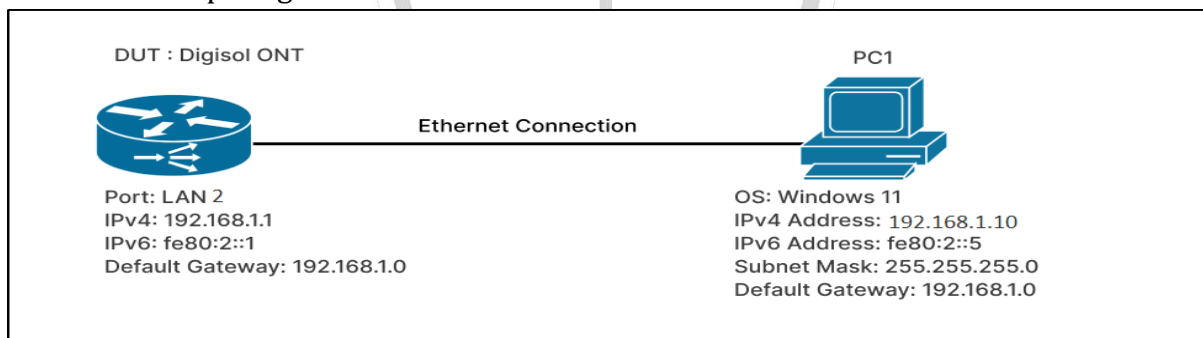
8.1 Number of Test Case Scenarios: 2

8.1.1 Test case01: Verify that the OEM undertaking provided for DUT software is as per the ITSAR requirement.

8.1.2 Test case02: No Unnecessary software

8.1.3 Test case 03: No orphaned (EoL) software/packages

8.2 Test Setup Diagram



8.3 Tools Used: - CLI(OS) of DUT, XEOL

8.4 Test Execution Steps

8.4.1 Test case 01: Verify that the OEM undertaking provided for DUT software is as per the ITSAR requirement.

- i. “ONT/ONU does not contain Software that is not used in the functionality of ONT/ONU”

8.4.2 Test case02: No Unnecessary software

- i. Find the list of installed software in the DUT
- ii. Compare the list of installed software with OEM declared necessary software

8.4.3 Test case03:No orphaned software/packages

- i. Find the EoL for opensource/third-party/proprietary software installed in the DUT

9. Expected Results for Pass:

- i. The OEM undertaking as per the ITSAR requirement
- ii. No unused software present in the system
- iii. No EoL software present in the system

10. Expected Format of Evidence: Screenshots of CLI, Tool report

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. **Test Case Description:** The tester verifies that the OEM submitted undertaking as per ITSAR requirement.

11.1.2. **Execution Steps:** Verify that the OEM undertaking provided for DUT software is as per the ITSAR requirement.

“ONT/ONU does not contain Software that is not used in the functionality of ONT/ONU”

11.2 Test Case Number: 02

11.2.1. **Test Case Description:** verify there is No Unnecessary software present in the DUT

11.2.2. Execution Steps:

- i. Login to the shell (OS) of DUT
- ii. Find the list of installed software in the DUT
 - NOTE 1: The identification of software could be done by, e.g. consulting the package manager of the OS/distribution (e.g. apt, dpkg, rpm, pacman, flatpack, snap...) and package managers of available runtimes (e.g. pip (Python), npm (JavaScript), composer (PHP)...), scanning for executables (global or focused on PATH variable of all available users), scanning for script files related to the available interpreters or listing images and their dependencies when virtualization or containerization is used.
- iii. Compare the list of installed software with OEM declared necessary software

Securing Networks

11.3 Test Case Number: 03

11.3.1. **Test Case Description:** No orphaned software/packages present in the DUT

11.3.2. Execution Steps:

- i. Upload SBOM to XEOL tool for finding the EoL for opensource/third party software
- ii. For proprietary software check with OEM

11.3.3. **Test Observation:** Not Tested

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1			Not Tested
2			Not Tested
3			Not Tested

2.3.6 TSTP for Evaluation of Insecure Services/protocol Removal

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.6
---	--------------------------	-----------------

<DUT Details: > Alphon AONT100C

<DUT Software Version:> R2.0.9.6

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 3: Software Security

2. <Security Requirement No & Name > Insecure Services/protocol Removal

3. <Requirement Description: > The OEM to provide list of essential services and the related ports required for functioning of ONU/ONT, list of optimal services supported by ONU/ONT and their related ports. The ONU/ONT shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services and their ports shall be initially configured to be disabled on the ONU/ONT by the vendor.

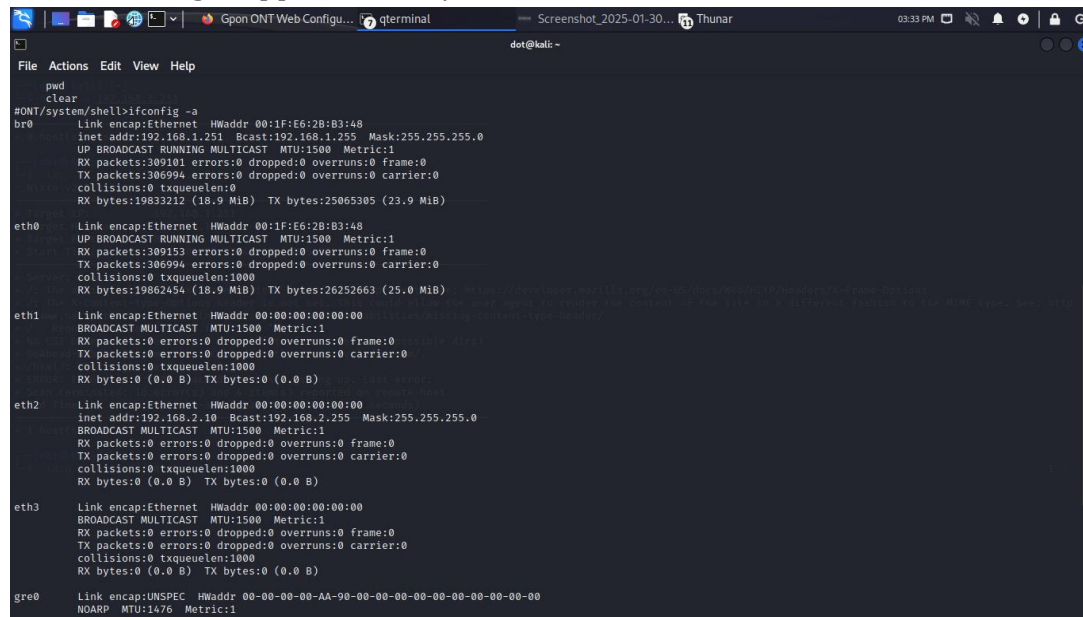
- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP - SNMPv1 and v2
- SSHv1, HNAP
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service
- PAD
- MOP

Full documentation of required protocols and services (Communication matrix) of the Network product and their purpose needs to be provided by the OEM as prerequisite for the test case.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. Section 4.3.2.1]

4. **DUT Confirmation Details:** Use the command line/GUI interface to get details of the machine on which test is conducted.

i. Use GUI to get Application No/Version No & hardware Info



```
pad
clear
#ONT/system>showconfig -a
br0
Link encap:Ethernet HWaddr 00:1F:E6:28:B3:48
inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)

eth0
Link encap:Ethernet HWaddr 00:1F:E6:28:B3:48
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)

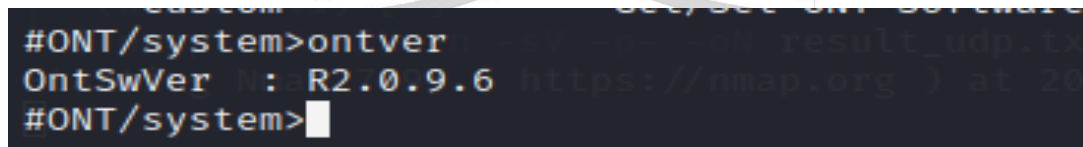
eth1
Link encap:Ethernet HWaddr 00:00:00:00:00:00
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth2
Link encap:Ethernet HWaddr 00:00:00:00:00:00
inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth3
Link encap:Ethernet HWaddr 00:00:00:00:00:00
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

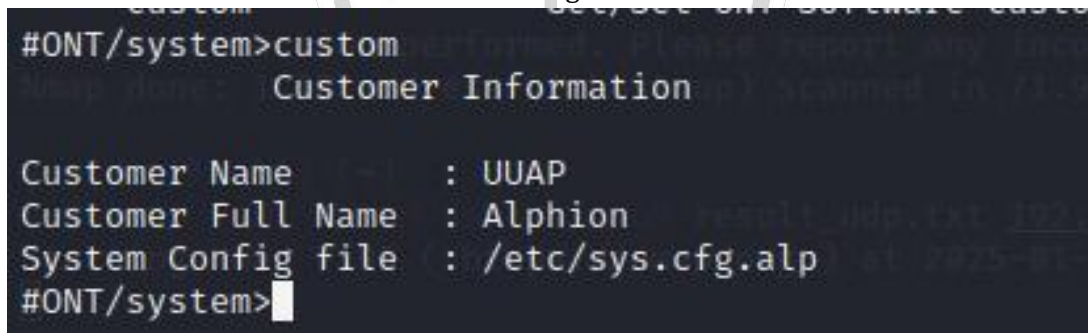
gre0
Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
NOARP MTU:1476 Metric:1
```

ii. The below screenshot shows the firmware version of the DUT



```
#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>
```

iii. The below screenshot shows the DUT configuration file

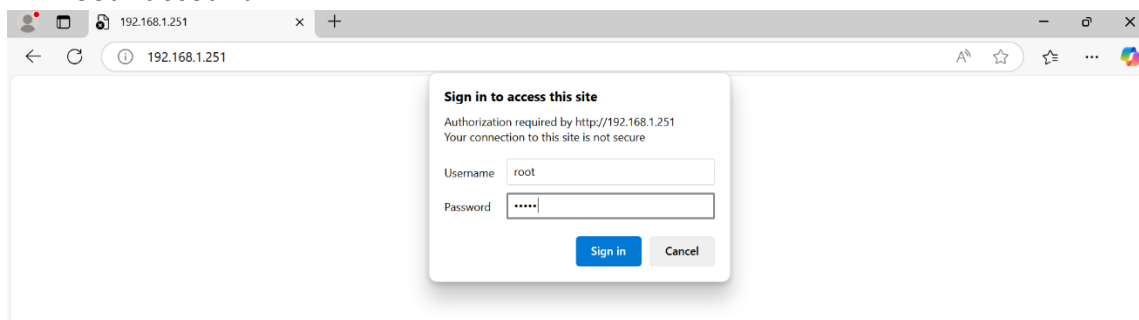


```
#ONT/system>custom
Customer Information

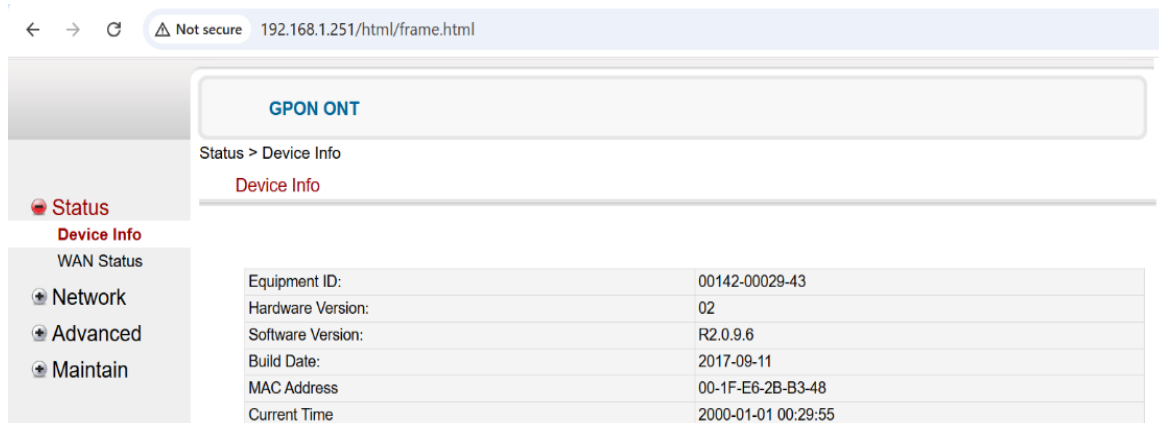
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration:

- i. The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- ii. The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



iii. Verify the DUT information through device info



6. Precondition: A list of all required network protocols and services containing at least the following information shall be included in the documentation accompanying the Network Product:

- i. protocol handlers and services needed for the operation of network product;
- ii. their open ports and associated services;
- iii. and a description of their purposes.
- iv. The tool used shall be capable to detect and identify the protocol handlers and running services in the system.

7. Test Objective: To ensure that on all network interfaces, there are no unsecure services or protocols that might be running.

8. Test Plan:

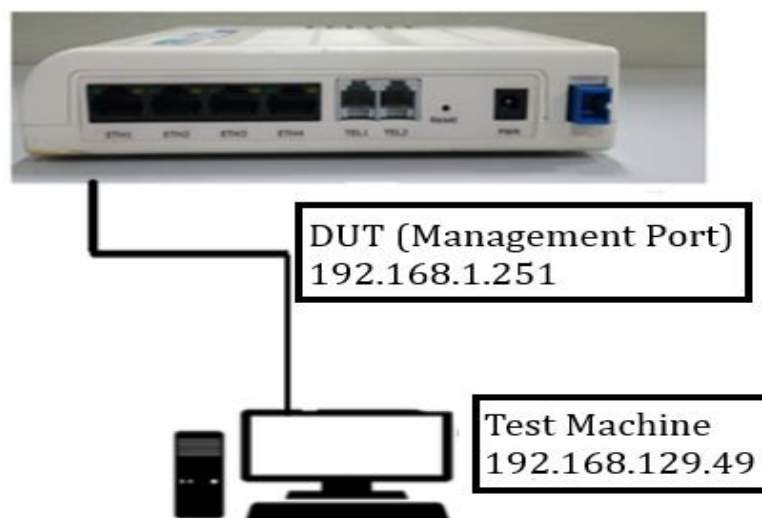
8.1 Number of Test Case Scenarios: 3

8.1.1 Test case 01: Verify that only required services are active on the ONU/ONT and compare with the OEM-provided list of services.

8.1.2 Test case 02: To verify that Unsecure Service are disabled by default

8.1.3 Test case 03: Verify Running Services and their Vulnerabilities.

8.2 Test Setup Diagram



8.3 Tools Used: - Port scanning tool (Nmap)

8.4 Test Execution Steps

8.4.1 Verify that only required services are active on the ONU/ONT and compare with the OEM-provided list of services.

i. Perform factory reset on the DUT and Run the port scanning tool (Nmap) on 192.168.1.251 of DUT

ii. List the running services in the DUT by Nmap

iii. Compare port scanning results with OEM document

8.4.2 To verify that Unsecure Service are disabled by default

i. Perform factory reset on the DUT

ii. Run the port scanning tool (Nmap) on 192.168.1.1 (default IP) of DUT

iii. Compare Nmap results with our ITSAR document,

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP - SNMPv1 and v2
- SSHv1, HNAP
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service
- PAD
- MOP

8.4.3 Verify Running Services and their Vulnerabilities.

i. Run the port scanning tool (Nmap) on 192.168.1.1 of DUT

ii. List the running services with version details in the DUT by Nmap

iii. Check the running services have affected by any known vulnerability (NIST)

9. Expected Results for Pass: *Securing Networks*

- i. No unnecessary service running in the DUTs
- ii. No vulnerable service running in the DUT

10. Expected Format of Evidence: Screenshots of CLI, Tool report (Nmap)

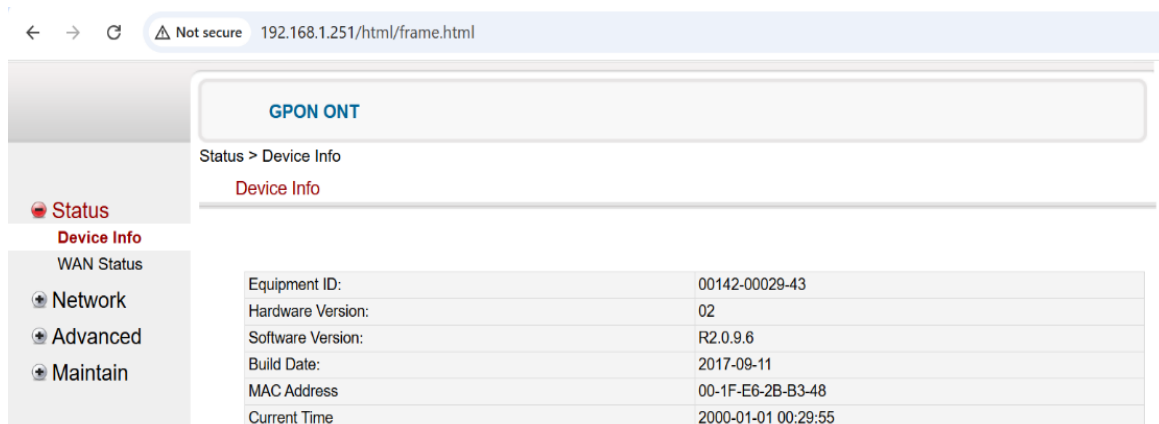
11. Test Execution:

11.1 Test Case Number: 01

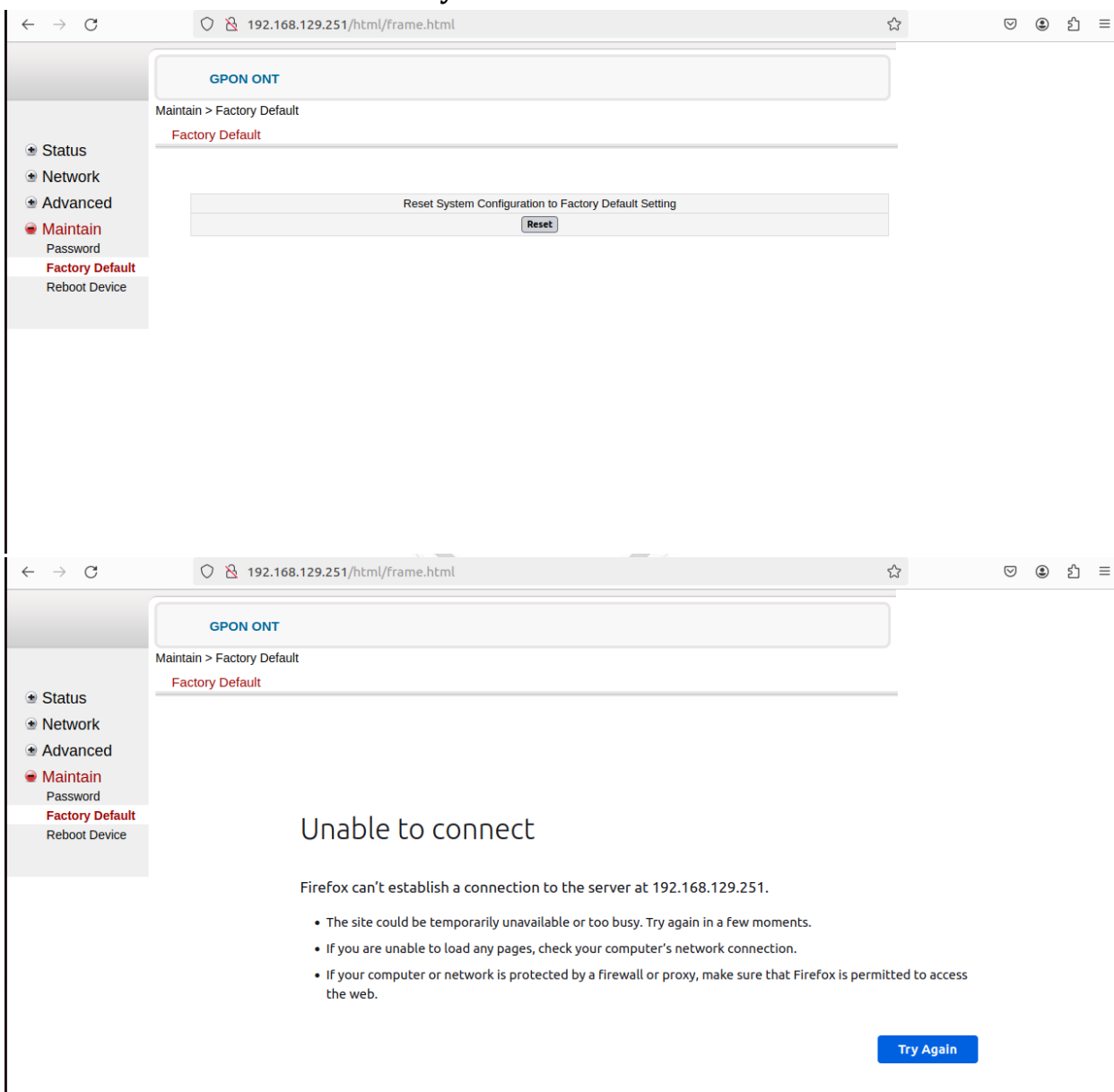
11.1.1. **Test Case Description:** Verify that only required services are active on the ONU/ONT and compare with the OEM-provided list of services.

11.1.2. Execution Steps:

1. Login to the ONT GUI(<http://192.168.1.251:80>)



2. Go to Maintain -> Factory Default and click “Reset” in the ONT GUI



3. Perform port scanning on ONT Interface(Default)

Command for TCP : `sudo nmap -p- -sT -A -Pn 192.168.1.251`

[illegible]

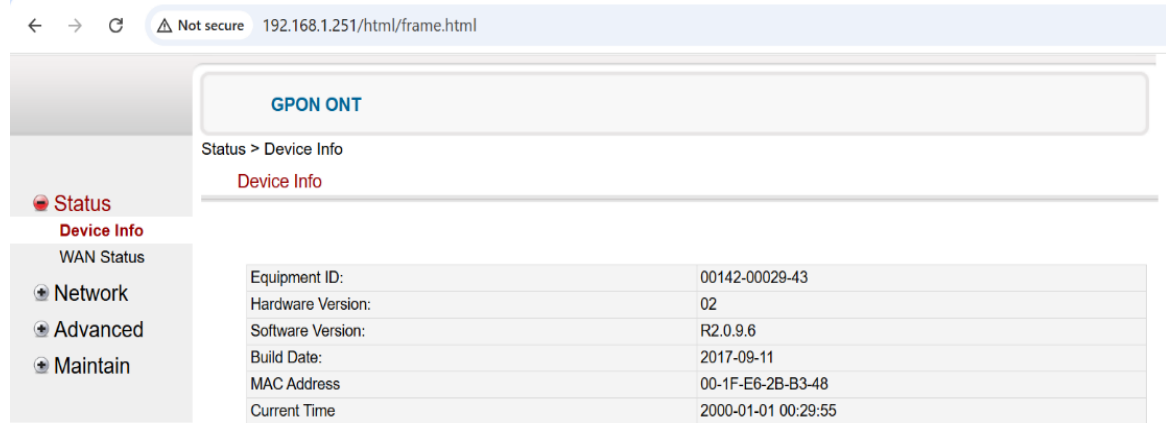
11.2 Test Case Number: 02

11.2.1. Test Case Name: 8.1.2

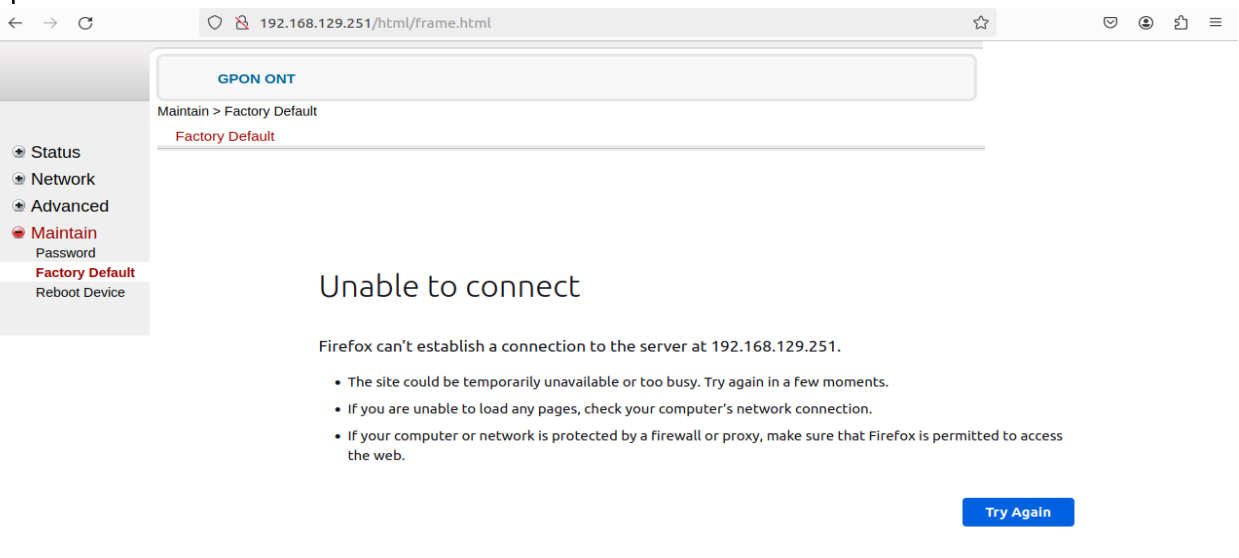
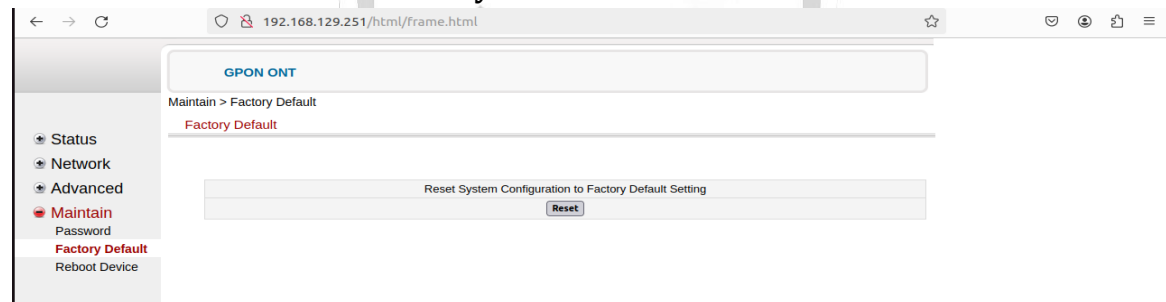
11.2.2. **Test Case Description:** To verify that Unsecure Service are disabled by default

11.2.3. Execution Steps:

1. Login to the ONT GUI(<http://192.168.1.251:80>)



2. Go to Maintain -> Factory Default and click "Reset" in the ONT GUI



3. Perform port scanning on ONT Interface(Default)

Command for TCP : sudo nmap -p- -sT -A -Pn 192.168.1.251)

```

[ossec-practice] Tower-3620: $ sudo nmap -p -sT -A -Pn 192.168.1.251
[sudo] password for acer:
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-13 12:57:15T
Nmap scan report for _gateway (192.168.1.251)
Host is up (0.00058s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet
|_ fingerprint-strings:
|_   GenericLines:
|_     Login as:
|_     Login as: Login as:
|_     GetRequest:
|_     Login as: GET / HTTP/1.0
|_     Password:
|_   Help:
|_     Login as: HELP
|_     Password:
|_   NCP:
|_     Login as: Dmd!AqAqAq
|_     AqAqAqAqAqAqAqAq
|_   NULL:
|_     Login as:
|_     RPCCheck:
|_     Login as:
|_     AqAq(r
|_   SIPOptions:
|_     Login as: OPTIONS sip;m SIP/2.0
|_     Via: SIP/2.0/TCP nm;branch=foo
|_     From: <slp:nm@nm>;tag=root
|_     <slp:nm2@nm2>
|_     Call-ID: 50000
|_     CSeq: 42 OPTIONS
|_     Max-Forwards: 70
|_     Content-Length: 0
|_     Contact: <slp:nm@nm>
|_     Accept: application/sdp
|_     Password:
|_   tn3270:
|_     Login as: @IBM-3279-4-E
53/tcp    open  domain dnsmaq 2.41
|_   dns-nsid:
|_   |_ bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   SF: as:\x20"Nr(GenericLines,31, "\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x20
|_   bind.version: dnsmaq-2.41
80/tcp    open  http      GoAhead WebServer
|_   http-auth:
|_   HTTP/1.1 401 Unauthorized;x00
|_   |_ Basic realm=GPON
|_   http-title: Document Error: Unauthorized
|_   Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF-Port23-TCP-V=7.80N1=7002/13KTime=67AD9F0E9P=X86_64-pc-linux-gnuNR(NULL
|_   SF: 19, "\xff\xfd\x01\xff\xfd\x1f\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03LogIn\x2
```

Command for SCTP : `sudo nmap -p- -sY -A -Pn 192.168.1.251`

```
acer@acer-Precision-Tower-3620:~$ sudo nmap -p- -sY -A -Pn 192.168.1.251
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-13 13:02 IST
Nmap scan report for _gateway (192.168.1.251)
Host is up (0.00066s latency).
All 65535 scanned ports on _gateway (192.168.1.251) are filtered
MAC Address: 00:1F:E6:2B:B3:48 (Alphion)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.66 ms  _gateway (192.168.1.251)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.78 seconds
```

Command for UDP : `sudo nmap -p- -sU -A -Pn 192.168.1.251`

4. Compare port scan results with ITSAR unsecure services (enabled by default)

11.3 Test Case Number: 03

11.3.1. Test Case Name: 8.1.3

11.3.2. Test Case Description: Verify Running Services and their Vulnerabilities.

11.3.3. Execution Steps:

1. Perform port scanning on ONT Interface(Default)

Command for TCP : sudo nmap -p- -sT -A -Pn 192.168.1.251)

[illegible]

Command for SCTP : `sudo nmap -p- -sY -A -Pn 192.168.1.251`

```

acer@acer-Precision-Tower-3620:~$ sudo nmap -p- -sY -A -Pn 192.168.1.251
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-13 13:02 IST
Nmap scan report for _gateway (192.168.1.251)
Host is up (0.00066s latency).
All 65535 scanned ports on _gateway (192.168.1.251) are filtered
MAC Address: 00:1F:E6:2B:B3:48 (Alphion)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.66 ms _gateway (192.168.1.251)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.78 seconds

```

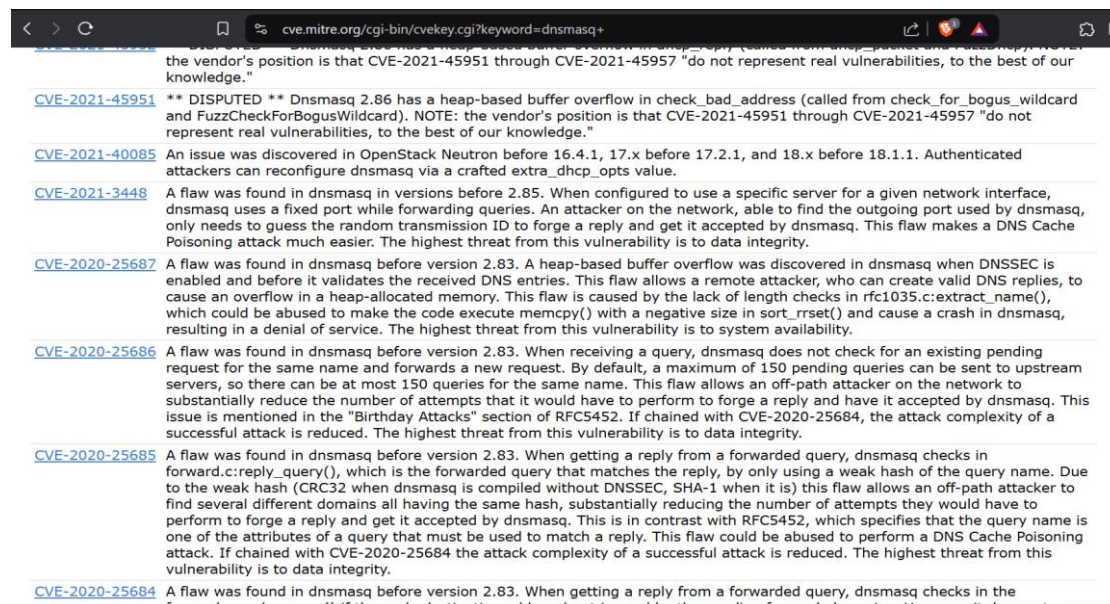
Command for UDP : sudo nmap -p- -sU -A -Pn 192.168.1.251

2. Check the version name and version of running services In the nmap result

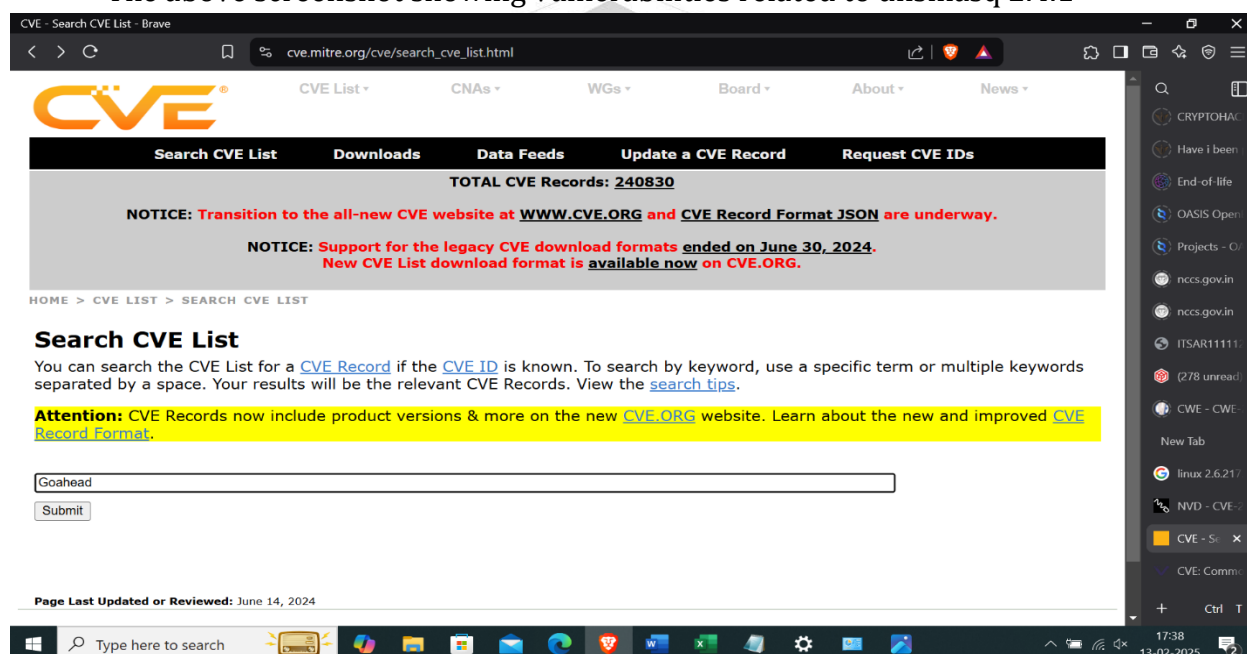
Sl.No	Service Name	Application name	Service version
1.	Telnet	telnetd	
2.	DNS	dnsmasq	2.4.1
3.	HTTP	GoAhead Webserver	

3. Check the vulnerability details in https://cve.mitre.org/cve/search_cve_list.html

The screenshot shows the CVE Mitre search interface. At the top, there are navigation links: Search CVE List, Downloads, Data Feeds, Update a CVE Record, and Request CVE IDs. Below these, it states 'TOTAL CVE Records: 240830'. A notice indicates a transition to the new CVE website at WWW.CVE.ORG and that support for legacy download formats ended on June 30, 2024. The main section is titled 'Search CVE List' and provides instructions on how to search. A search bar contains the text 'dnsmasq', and a dropdown menu shows 'dnsmasq 2.4.1'. The page footer includes links to the CVE.ORG website, terms of use, and contact information.



The above screenshot showing vulnerabilities related to dnsmasq 2.4.1



CVE - Search Results - Brave

cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Goahead

CVE

CVE List ▾ CNA's ▾ WGs ▾ Board ▾ About ▾ News ▾

Search CVE List Downloads Data Feeds Update a CVE Record Request CVE IDs

TOTAL CVE Records: 240830

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024. New CVE List download format is available now on CVE.ORG.

HOME > CVE > SEARCH RESULTS

Search Results

There are **62** CVE Records that match your search.

Name	Description
CVE-2024-48419	Edimax AC1200 Wi-Fi 5 Dual-Band Router BR-6476AC 1.06 suffers from Command Injection issues in /bin/goahead. Specifically, these issues can be triggered through /goform/tracerouteDiagnosis, /goform/pingDiagnosis, and /goform/fromSysToolPingCmd Each of these issues allows an attacker with access to the web interface to inject and execute arbitrary shell commands, with "root" privileges.
CVE-2024-48417	Edimax AC1200 Wi-Fi 5 Dual-Band Router BR-6476AC 1.06 is vulnerable to Cross Site Scripting (XSS) in : /bin/goahead via /goform/setStaticRoute, /goform/fromSetFilterUrlFilter, and /goform/fromSetFilterClientFilter.
CVE-2024-46215	A vulnerability was discovered in KM08-708H-v1.1. There is a buffer overflow in the sub_445BDC() function within the /usr/sbin/goahead program; The strcpy function is executed without checking the length of the string, leading to a buffer overflow.
CVE-2024-3187	This issue tracks two CWE-416 Use After Free (UAF) and one CWE-415 Double Free vulnerabilities in Goahead versions <= 6.0.0. These are caused by JST values not being nulled when freed during parsing of JST templates. If the ME GOAHEAD JAVASCRIPT flag is enabled, a remote attacker with the privileges to modify JavaScript template (JST) files

CVE - Search CVE List - Brave

cve.mitre.org/cve/search_cve_list.html

CVE

CVE List ▾ CNA's ▾ WGs ▾ Board ▾ About ▾ News ▾

Search CVE List Downloads Data Feeds Update a CVE Record Request CVE IDs

TOTAL CVE Records: 240830

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024. New CVE List download format is available now on CVE.ORG.

HOME > CVE LIST > SEARCH CVE LIST

Search CVE List

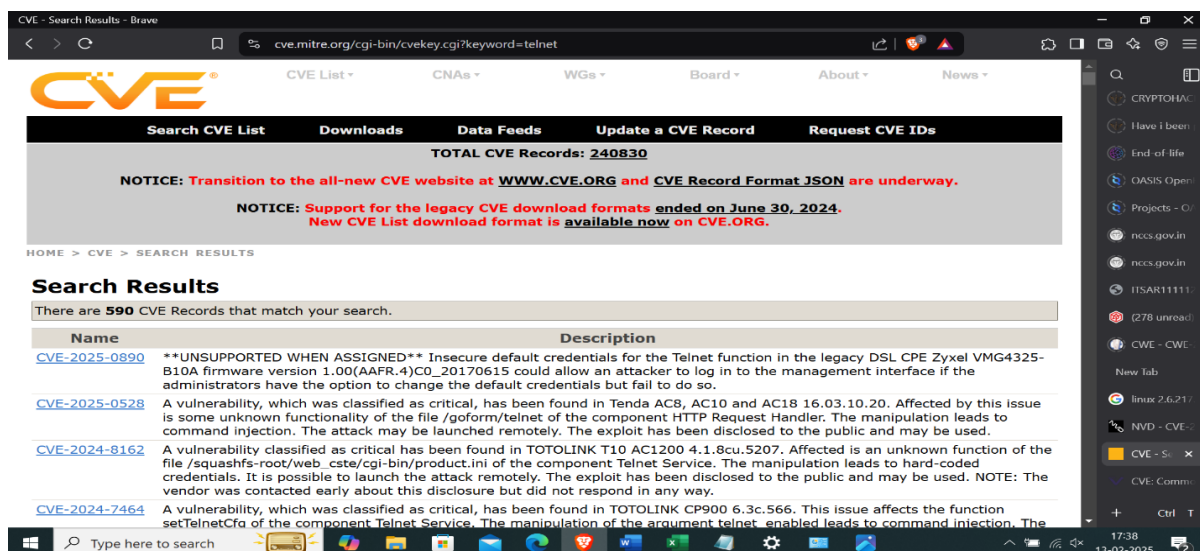
You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records. View the [search tips](#).

Attention: CVE Records now include product versions & more on the new CVE.ORG website. Learn about the new and improved [CVE Record Format](#).

telnet

Submit

Page Last Updated or Reviewed: June 14, 2024



11.3.4. Test Observation:

i. **Test case 01:** By default, the following services are open in the ONT,

- telnet (23),
- DNS (53)
- HTTP (80)

ii. **Test Case 02:** It is observed that, ONT using following unsecure services enabled by default,

- Telnet (23)
- HTTP (80)

iii. **Test case 03:** It is observed that dnsmasq 2.4.1, Goahead and telnet having known vulnerabilities

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Based OEM document
2	8.1.2	FAIL	
3	8.1.3	FAIL	

2.3.7 TSTP for Evaluation of Restricting System Boot Source

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.7
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
DOCA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 3: Software Security

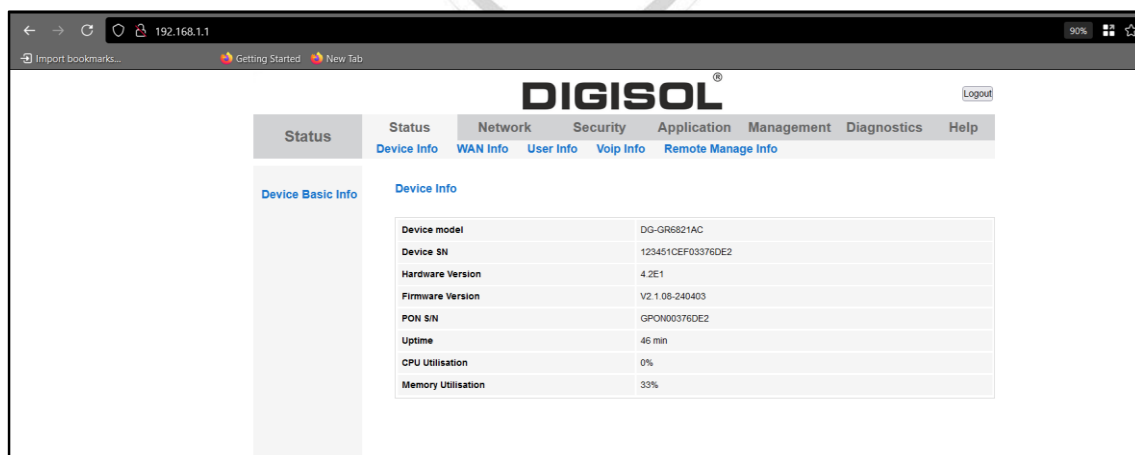
2. <Security Requirement No & Name > 2.3.7 Restricting System Boot Source

3. <Requirement Description: > ONU/ONT shall boot only from memory devices intended for this purpose

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.2]

4. DUT Confirmation Details:

- Use the command line/GUI interface to get details of the machine on which test is conducted.
- Use GUI to get Application No/Version No & hardware Info
- The below screenshot shows the firmware version of the DUT



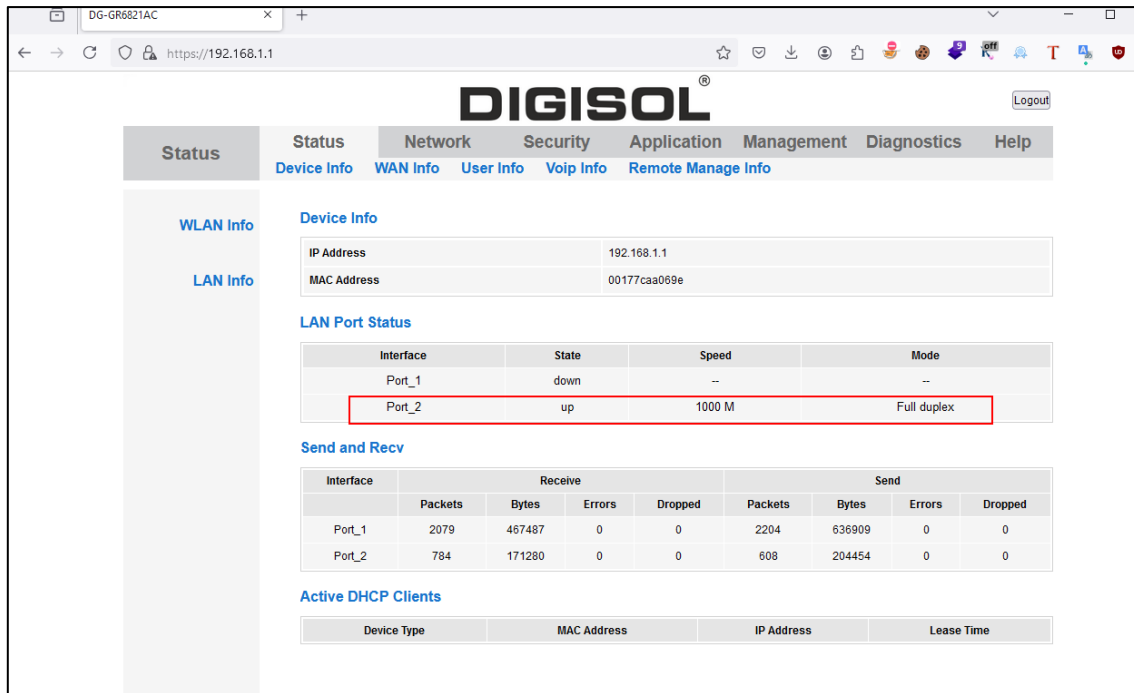


Securing Networks

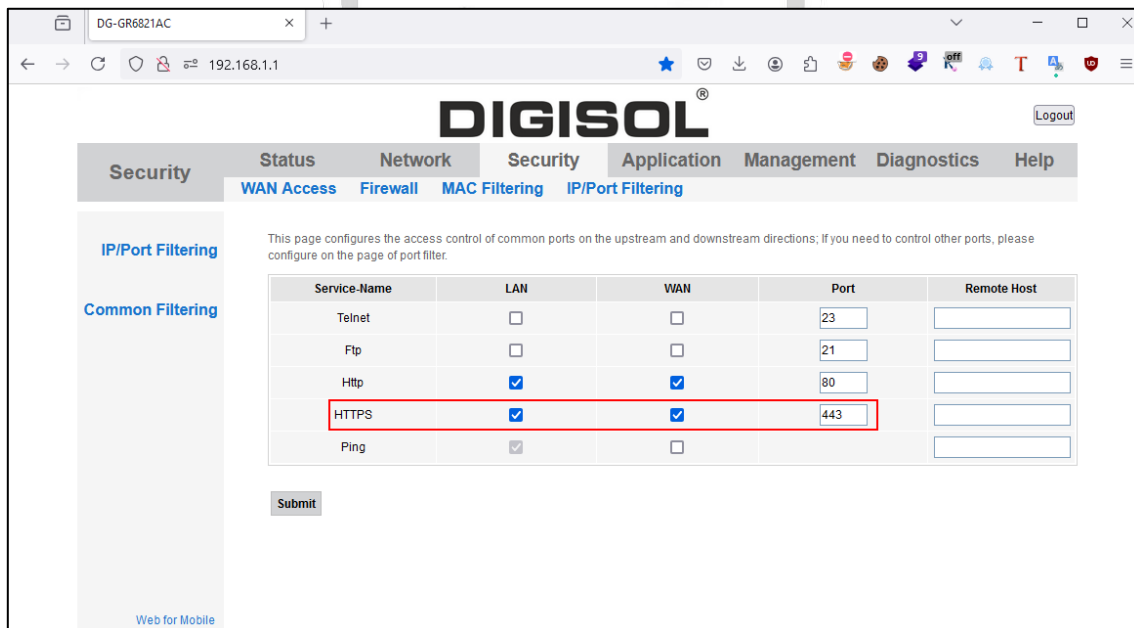
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.



ii. HTTPS is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~
aravind@Aravind_V:~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN
aravind@Aravind_V:~$

```

6. Precondition:

- i. OEM clarity on which specific memory devices are designated for booting the device by default.
- ii. The OEM should provide documentation describing how to boot through external device (like USB, network, etc), if external booting is possible.
- iii. OEM document clarifying if any mechanisms are used to detect and prevent tampering with the boot process or firmware access.

7. Test Objective: Verify that the network product can only boot from memory devices intended for this purpose (e.g. not from external memory like USB key, network if not mentioned in the manual/document).

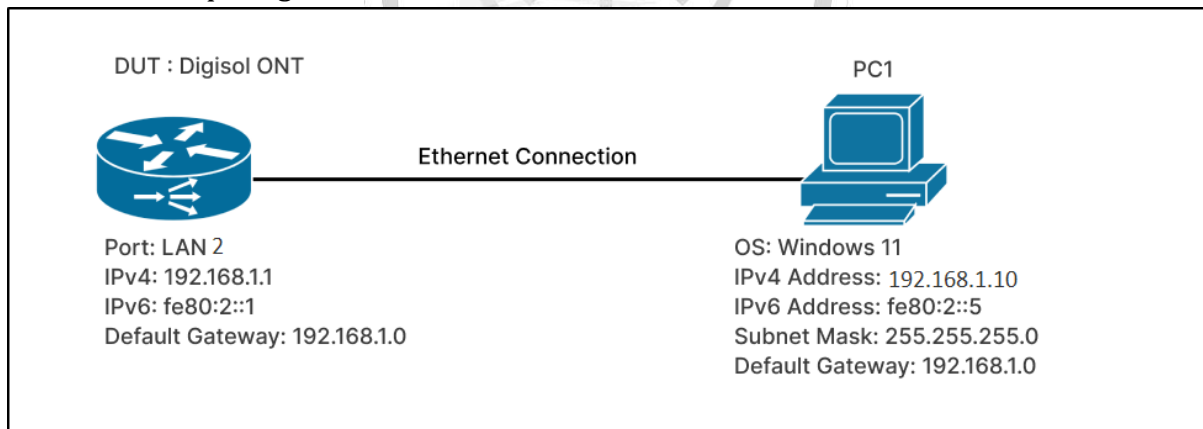
8. Test Plan:

8.1 Number of Test Case Scenarios: 2

8.1.1 Verify that the DUT can boot only from memory device intended for this purpose.

8.1.2 The tester verifies that there is no possibility to access and modify the firmware of the network product without successful authentication and the authenticated subject (e.g., person or process) has no possibility to access and modify the firmware without privileged access rights.

8.2 Test Setup Diagram



8.3 Tools Used: - Network file transfer protocols (FTP, TFTP, SCP, BOOTP), Web browser (For access GUI of DUT), USB

8.4 Test Execution Steps

8.4.1 Access the DUT.

1. Wait till the reboot process is completed.
2. Check whether after reboot, the boot image address is same as mentioned in the OEM document.

8.4.2 Boot from TFTP

1. Configure TFTP server over same subnet.
2. Store the firmware file that is to be booted, in TFTP-Root directory.
3. Check whether TFTP server is reachable from the DUT.
4. Initiate TFTP boot using TFTP server and verify whether boot is successful from TFTP server.

8.4.3 Boot with external USB drive

- 1) Connect testing machine to the DUT through serial console using terminal emulator tool like PuTTY.
- 2) Store the firmware file that is to be booted, in USB Drive.
- 3) Login using highest/root privilege user.
- 4) Connect USB Drive to the DUT and try to boot from External memory device (USB).

9. Expected Results for Pass: DUT should boot firmware from OEM documented devices only

10. Expected Format of Evidence: Screenshots of terminal

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

11.1.2. Test Case Description: Verify that the DUT can boot only from memory device intended for this purpose.

11.1.3. Execution Steps:

- i. Access the DUT.
- ii. Wait till the reboot process is completed.
- iii. Check whether after reboot, the boot image address is same as mentioned in the OEM document.

11.2 Test Case Number: 02

11.2.1. Test Case Name: 8.1.2

11.2.2. Test Case Description: The tester verifies that there is no possibility to access and modify the firmware of the network product without successful authentication and the authenticated subject (e.g., person or process) has no possibility to access and modify the firmware without privileged access rights

11.2.3. Execution Steps:

1. Boot from TFTP
2. Configure TFTP server over same subnet.
3. Store the firmware file that is to be booted, in TFTP-Root directory.
4. Check whether TFTP server is reachable from the DUT.
5. Initiate TFTP boot using TFTP server and verify whether boot is successful from TFTP server.
6. Boot with external USB drive
7. Connect testing machine to the DUT through serial console using terminal emulator tool like PuTTY.
8. Store the firmware file that is to be booted, in USB Drive.

9. Login using highest/root privilege user.

10. Connect USB Drive to the DUT and try to boot from External memory device (USB).

11.2.4. **Test Observation:** Hence the testcase is “Not Tested.”

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not tested
2	8.1.2		Not Tested



2.3.8 TSTP for Evaluation of Secure Time Synchronization

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.8
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3: Software Security
2. **<Security Requirement No & Name >** 2.3.8 Secure Time Synchronization
3. **<Requirement Description: >** The ONU/ONT shall support time synchronization feature for its core functionality or for the additional supported functionality. For ONU/ONT 's that have time synchronization feature, it shall support the secure time synchronization feature preferably by using Network Time Protocol NTP. The ONU/ONT clock shall be synchronized with NTP server in a secure manner. The ONU/ONT client should be able to verify the authentication and authorization of the NTP Server. OEM shall plugin well known vulnerabilities, input validation vulnerabilities related to NTP feature.
4. **DUT Confirmation Details:**
 - i. Use the command line/GUI interface to get details of the machine on which test is conducted.
 - ii. Use GUI to get Application No/Version No & hardware Info
 - iii. The below screenshot shows the firmware version of the DUT

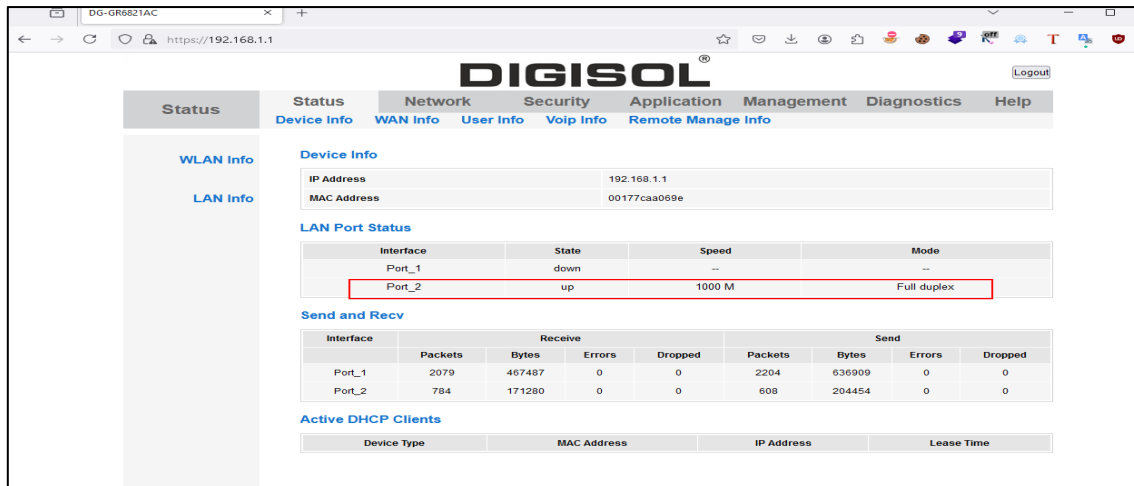




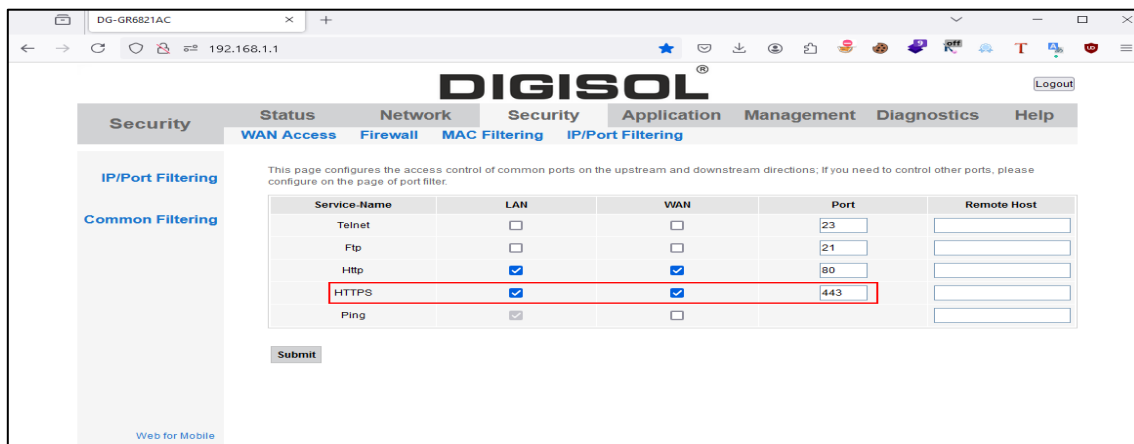
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

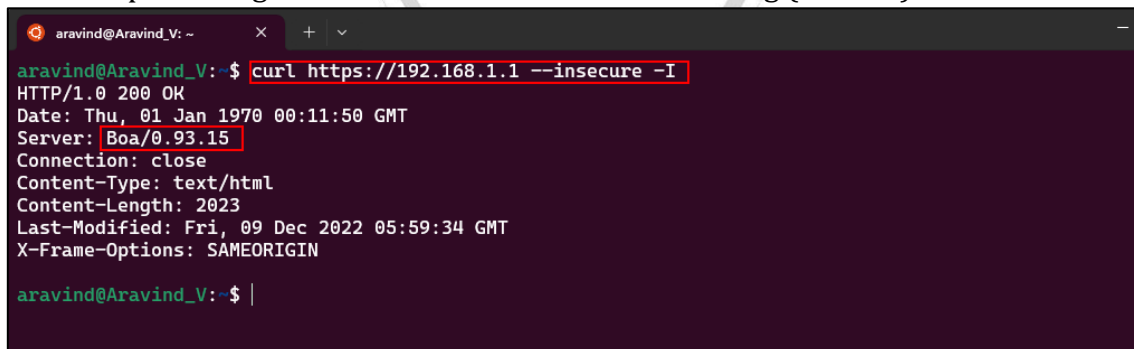
- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.



ii. HTTPS is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.



iv. Configure the NTP server ip address in the ONT GUI

6. Precondition:

- OEM should provide the document related to NTP configuration in the DUT
- OEM document describing well-known NTP vulnerabilities and applied patches on the ONT.

7. **Test Objective:** Verify that the DUT support NTP based time synchronization in a secure manner

8. Test Plan:

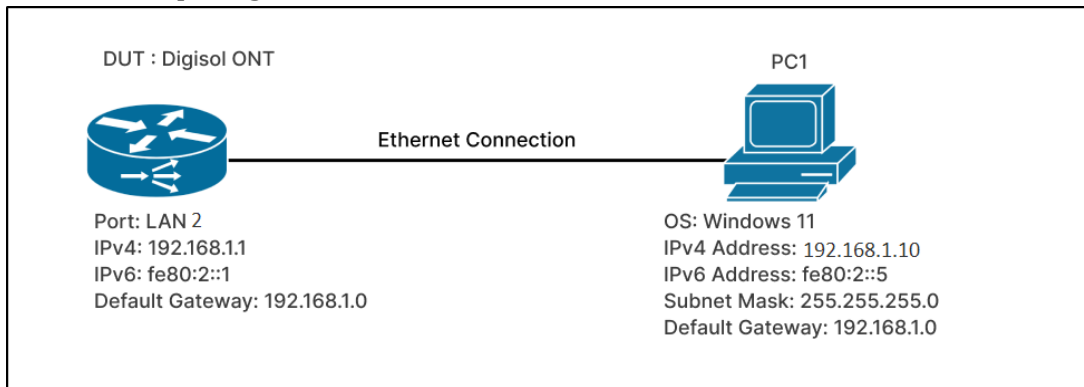
8.1 Number of Test Case Scenarios : 3

8.1.1 Verify that the DUT supports the time synchronization feature as part of its core or additional functionality.

8.1.2 Confirm that the DUT can securely synchronize its clock with an NTP server and validate the server's authentication and authorization.

8.1.3 Validate that the OEM has addressed well-known vulnerabilities and implemented proper input validation in the NTP feature.

8.2 Test Setup Diagram



8.3 Tools Used:- Wireshark, python script for spoof NTP packet

8.4 Test Execution Steps

8.4.1 (A)

1. Log into the DUT on PC1 using the admin account with the username admin and password admin123. Then, navigate to Network > Time > Time Server and check the current time.
2. Choose the time zone, enter the NTP server IP address, select Sync via LAN(NTP server), and apply all changes.
3. Verify that the ONT supports time synchronization functionality.

8.4.2 (B) Confirm that the DUT can securely synchronize its clock with an NTP server and validate the server's authentication and authorization.

1. To verify secure clock synchronization with the NTP server.
2. Log into the DUT on PC1 using the admin account with the username admin and password admin123. Then, navigate to Network > Time > Time Server and check the current time.
3. Choose the time zone, enter the NTP server IP address, select Sync via LAN(NTP server-PC1), and apply all changes.
4. Use Wireshark to capture the traffic between DUT and PC1
5. Open Wireshark on PC1, which is connected to the OLT, and verify that the ONT securely synchronizes its clock with the NTP server, ensuring the server's authentication and authorization are validated.

8.4.3 (C) Validate that the OEM has addressed well-known vulnerabilities and implemented proper input validation in the NTP feature.

a. Manual:

- i. Check the running version of NTP server
- ii. Check the vulnerability details in MITRE website.

- iii. Verify the identified well-known NTP vulnerabilities and applied patches on the DUT against the information provided in the OEM documentation.

b. Automatic:

- i. Use vulnerability Assessment tool for finding the NTP related vulnerabilities

9. Expected Results for Pass:

- 1.1.13. DUT have a NTP time sync with NTP server in a secure manner
- 1.1.14. DUT doesn't have any known vulnerabilities related to NTP

10. Expected Format of Evidence: PCAP, screenshot of wireshark, GUI/CLI configuration, MITRE (or) Vulnerability Assessment tool

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

11.1.2. Test Case Description: Verify that the DUT supports the time synchronization feature as part of its core or additional functionality.

11.1.3. Execution Steps:

1. Log into the DUT on PC1 using the admin account with the username admin and password admin123. Then, navigate to Network > Time > Time Server and check the current time.
2. Choose the time zone, enter the NTP server IP address, select Sync via LAN (NTP server), and apply all changes.
3. Verify that the ONT supports time synchronization functionality.

11.2 Test Case Number: 02

11.2.1. Test Case Name: 8.1.2

11.2.2. Test Case Description: Confirm that the DUT can securely synchronize its clock with an NTP server and validate the server's authentication and authorization.

11.2.3. Execution Steps:

1. To verify secure clock synchronization with the NTP server.
2. Log into the DUT on PC1 using the admin account with the username admin and password admin123. Then, navigate to Network > Time > Time Server and check the current time.
3. Choose the time zone, enter the NTP server IP address, select Sync via LAN (NTP server-PC1), and apply all changes.
4. Check the NTP server time and DUT time is sync or not
5. To Perform NTP spoof, send an NTP spoofed packet to the DUT
6. Check the time of DUT is changed or not after spoofed NTP packet
7. If time settings not changed, execution steps 8 & 9 will be applicable.
8. Use Wireshark to capture the traffic between DUT and PC1
9. Open Wireshark on PC1, which is connected to the ONT, and verify that the ONT securely synchronizes its clock with the NTP server, ensuring the server's authentication and authorization are validated using as per the "Crypto-Controls-V1.0.0" ITSAR crypto algorithms.

11.3 Test Case Number: 03

11.3.1. Test Case Name: 8.1.3

11.3.2. Test Case Description: Validate that the OEM has addressed well-known vulnerabilities and implemented proper input validation in the NTP feature.

11.3.3. Execution Steps:

a. Manual:

1. Check the running version of NTP server
2. Check the vulnerability details in MITRE website.
3. Verify the identified well-known NTP vulnerabilities and applied patches on the DUT against the information provided in the OEM documentation.

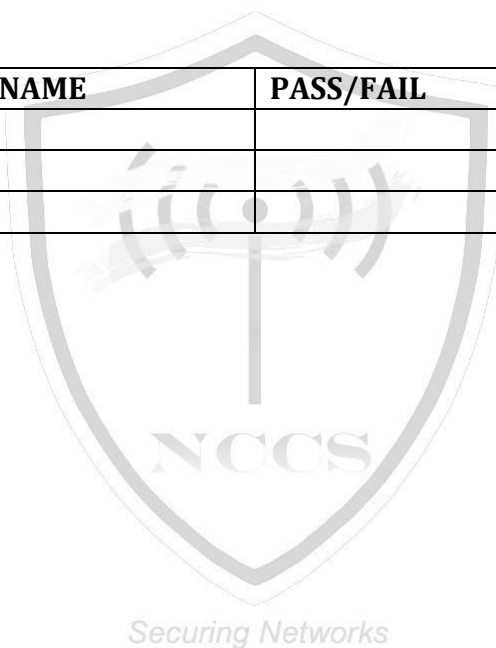
b. Automatic:

1. Use vulnerability Assessment tool for finding the NTP related vulnerabilities

11.3.4. Test Observation: Not Tested

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not tested
2	8.1.2		Not Tested
3	8.1.3		Not Tested



2.3.9 TSTP for Evaluation of Restricted reachability of services

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.9
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

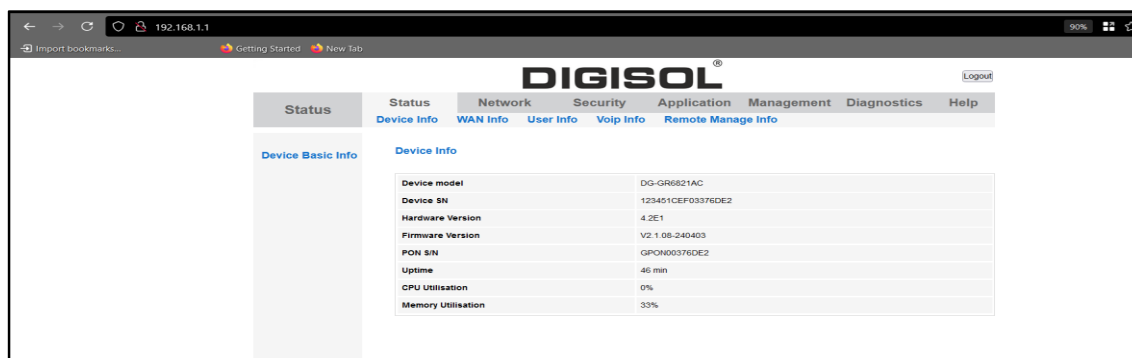
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 3: Software Security
2. **<Security Requirement No & Name >** 2.3.9 Restricted reachability of services
3. **<Requirement Description: >** The ONU/ONT shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. OEM to map the essential services required to be accessed from WAN side, LAN side to limit access to services only on need / functionality basis. For Interfaces on which services are active, the reachability to be limited to legitimate communication peers. One such Use-case scenario is to restrict web-management access of ONU/ONT to only LAN ports and not to permit access on Wi-Fi, WAN side

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0 Section 4.3.2.2]

4. DUT Confirmation Details:

- i. Use the command line/GUI interface to get details of the machine on which test is conducted.
- ii. Use GUI to get Application No/Version No & hardware Info
- iii. The below screenshot shows the firmware version of the DUT

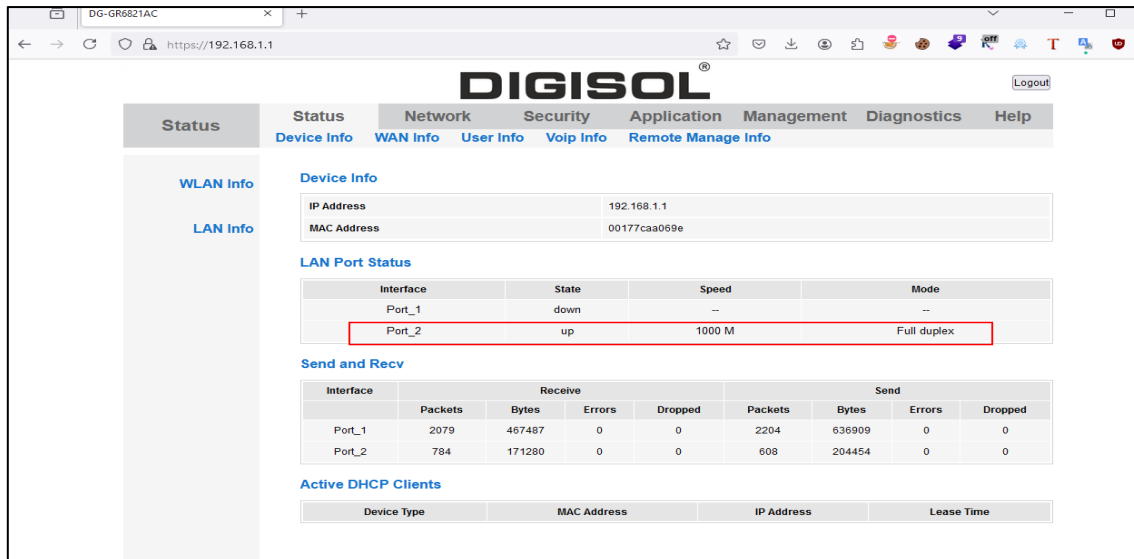




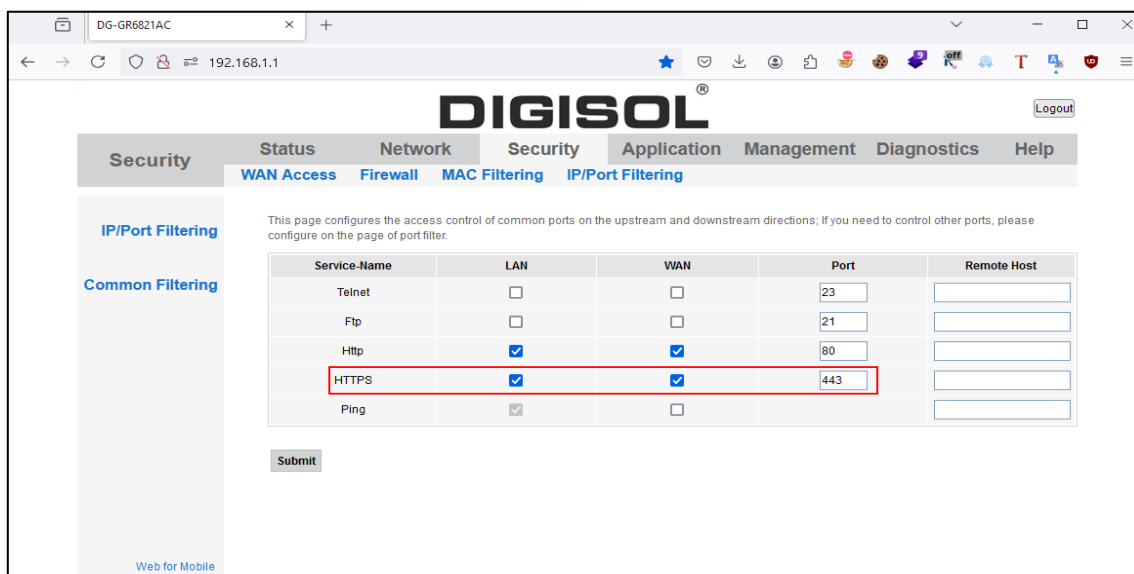
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

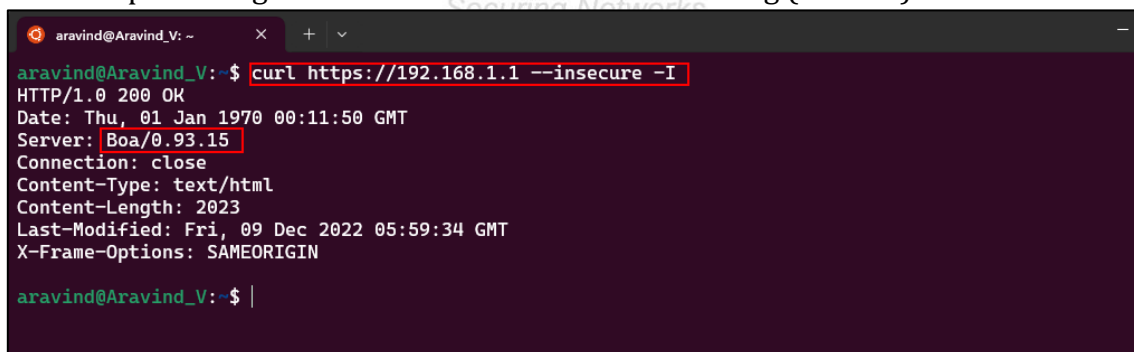
- i. The DUT (192.168.1.1) is connected to the Lab's Testing Machine's (192.168.1.2 and 192.168.1.3) via LAN1 interface.
- ii. The DUT (192.168.2.1) is connected to the Lab's Testing Machine's (192.168.2.2 and 192.168.2.3) via LAN2 interface.



iii. HTTPS is enabled.



iv. DUT is pre-configured with BOA as a webserver having (0.93.15) version.



v. Configure the NTP server ip address in the ONT GUI

6. **Precondition:** OEM need to provide document regarding the DUT have the capability to restrict services reachability to only declared ports and the nodes authorized to access them. In case, the OEM shall detail how this capability can be configured.

7. **Test Objective:** To verify that it is possible to bind the services only to the interfaces from which they are expected to be reachable.

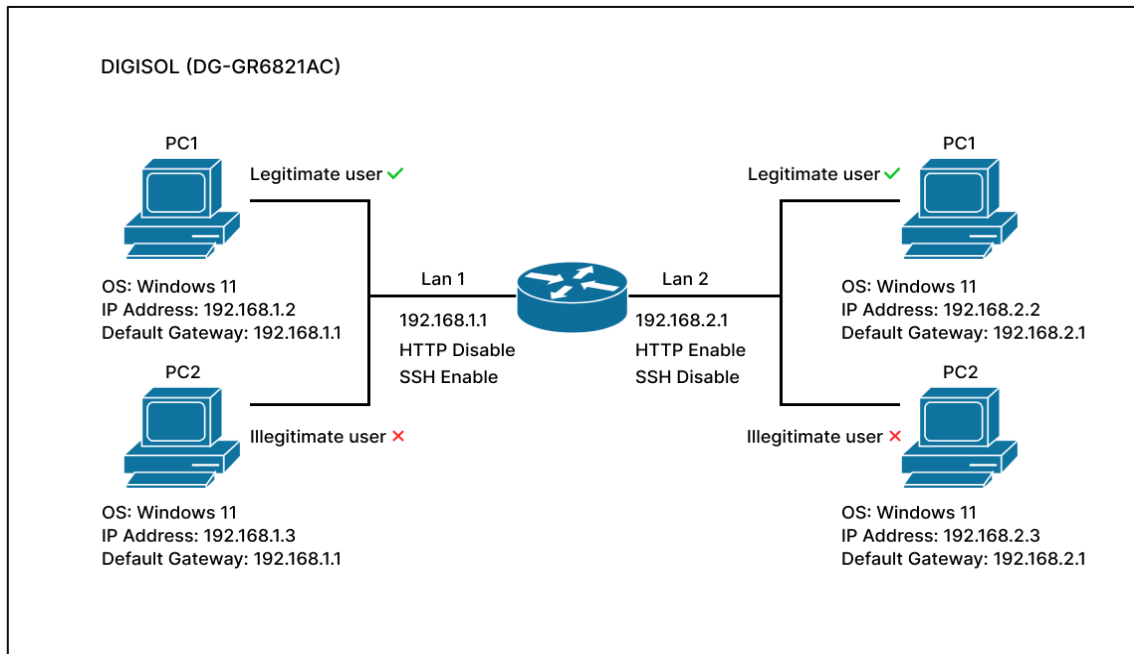
8. Test Plan:

8.1 Number of Test Case Scenarios: 3

8.1.1 To verify that it is possible to bind the services such as HTTP and SSH only to the authorized interfaces (LAN) and legitimate user.

8.1.2 To verify that services such as HTTP and SSH are not accessible from unauthorized interface (WAN) and illegitimate user.

8.2 Test Setup Diagram



8.3 Tools Used: - GUI/CLI of DUT, Port scan tool

8.4 Test Execution Steps

8.4.1 (A) To verify that it is possible to bind the services such as HTTP and SSH only to the authorized interfaces (LAN) and legitimate user.

1. Launch PuTTY, Enter the DUT's IP address 192.168.1.1 in the "Host Name" field, set connection type SSH, specify port 22 and Click "Connect".
2. Enter the username "admin" and password "admin123".
3. Create firewall rules on the DUT to accept SSH and HTTP connections for all the legitimate users connected on authorized ports.
4. To check for services that are open and filtered on all connected authorized ports, utilize the Nmap tool to verify the status of services.
5. Using Putty, login into the DUT's SSH service from a legitimate user.
6. Check the logs for SSH attempt via authorized interface and legitimate user.
7. Attempt HTTP connection via authorized interface and legitimate user, open a web browser and enter the default gateway address (DUT's ip) in the address bar. Then, login with the admin user.
8. Check the logs for HTTP attempt via authorized interface and legitimate user.

1.1.15.

8.4.2 (B) To verify that services such as HTTP and SSH are not accessible from unauthorized interface (WAN) and illegitimate user.

- i. Launch PuTTY, Enter the DUT's IP address 192.168.1.1 in the "Host Name " field, set connection type SSH, specify port 22 and Click "Connect".
- ii. Enter the username "admin" and password "admin123".
- iii. Create a Firewall rule on DUT to drop SSH connection for any interface and user except authorized interface and legitimate user.
- iv. Try to access SSH via unauthorized interface, open PuTTY, enter the DUT's IP address in the "Host Name" field and set the port to your desired number 22 for SSH. Then click "Open" and log in.
- v. Check the logs for SSH attempt via unauthorized interface.
- vi. Try to access SSH via illegitimate user and authorized interface, open PuTTY, enter the DUT's IP address in the "Host Name" field and set the port to your desired number 22 for SSH. Then click "Open" and log in.
- vii. Check the logs for SSH attempt via illegitimate user via authorized interface.
- viii. Attempt HTTP connection via unauthorized interface, open a web browser and enter the default gateway address (DUT's ip) in the address bar.
- ix. Check the logs for HTTP attempt via unauthorized interface.
- x. Attempt HTTP connection via illegitimate user and authorized interface, open a web browser and enter the default gateway address (DUT's ip) in the address bar. Then, login with admin user.
- xi. Check the logs for HTTP attempt via unauthorized interface.

9. Expected Results for Pass:

- 1.1.16. DUT should be accessed through authorized interface only
- 1.1.17. DUT should be accessed through authorized entity only

10. Expected Format of Evidence: GUI/CLI configuration, Nmap results

11. Test Execution:

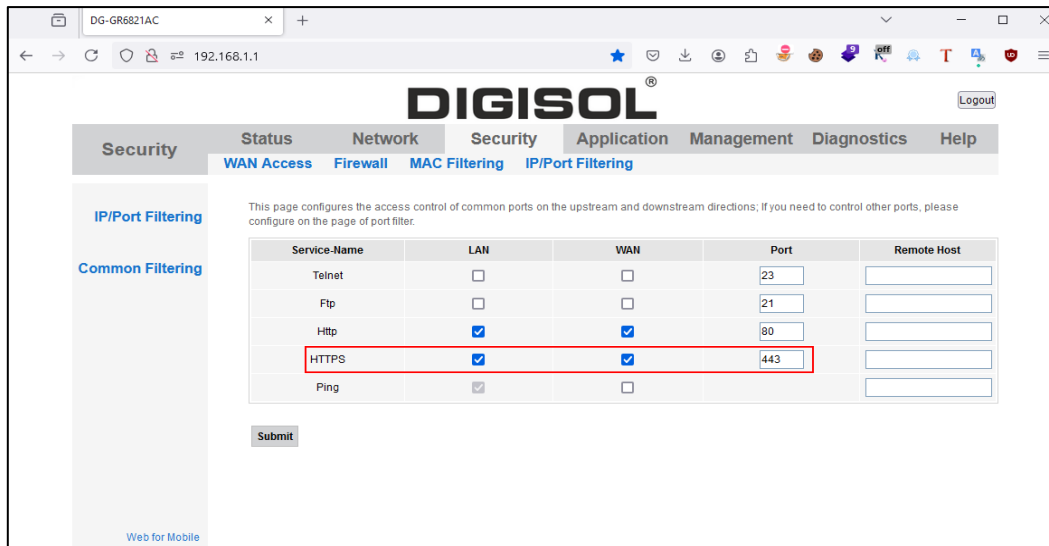
11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

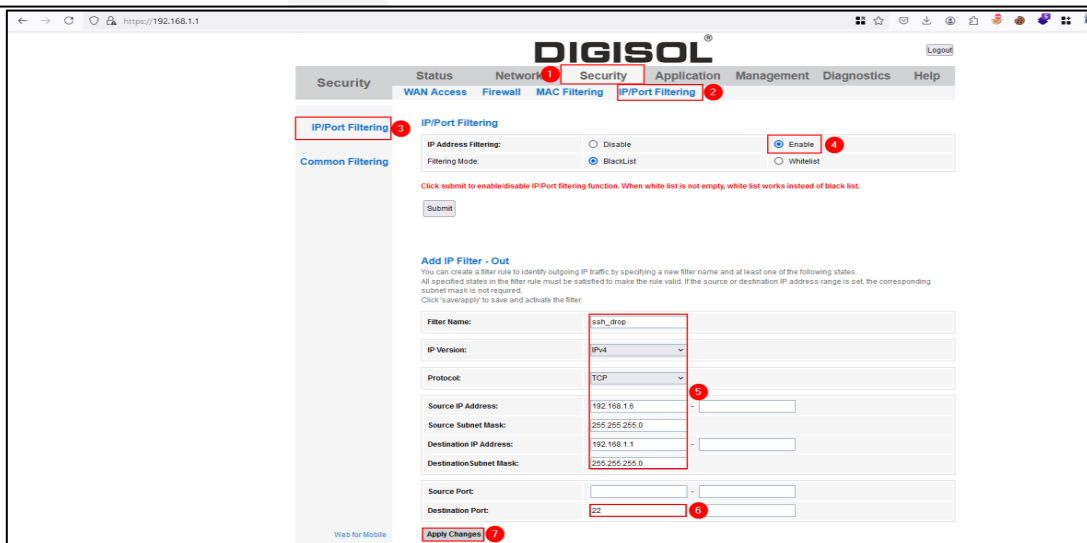
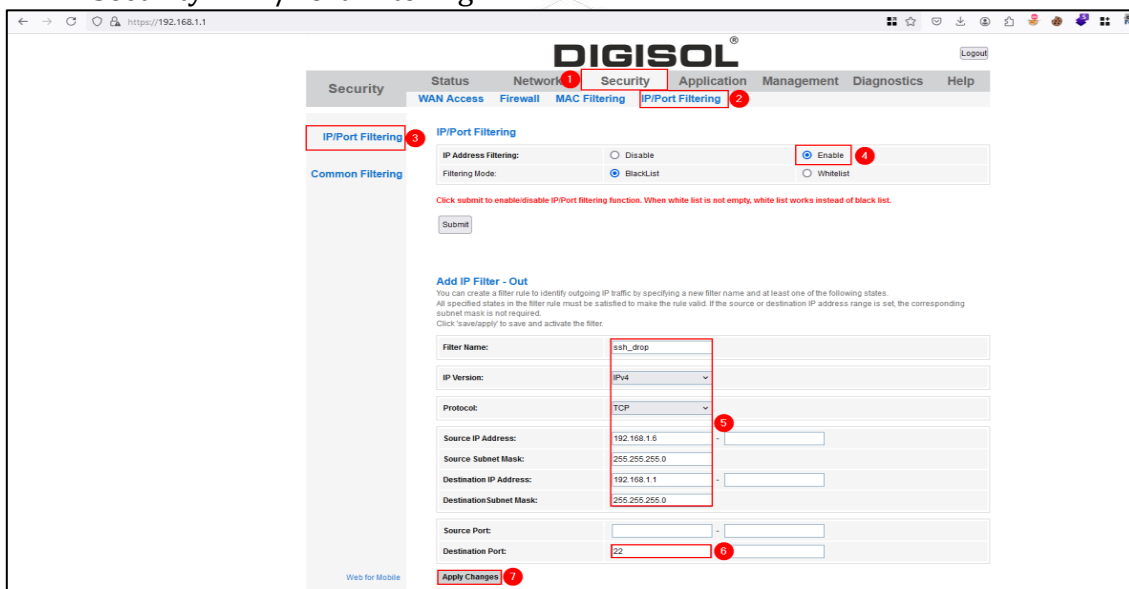
11.1.2. Test Case Description: To verify that it is possible to bind the services such as HTTP and SSH only to the authorized interfaces (LAN) and legitimate user.

11.1.3. Execution Steps:

1. Log into the DUT on PC1 using the admin account with the username admin and password admin123.
2. Then go to the "Security -> IP/Port filtering" in the GUI.
3. Enable the management protocols (SSH, HTTP/HTTPS) on the LAN side and disable it on WAN side.



4. Create IP filter rule for only legitimate user(entity) able to access the DUT.
Security -> IP/Port Filtering



5. Try to access the DUT from LAN side (legitimate user) – ping , ssh, http/http

```
aravind@Aravind_V: ~  
aravind@Aravind_V:~$ sudo hping3 -p 22 192.168.1.1  
[sudo] password for aravind:  
HPING 192.168.1.1 (eth0 192.168.1.1): NO FLAGS are set, 40 headers + 0 data bytes  
^C  
--- 192.168.1.1 hping statistic ---  
97 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
aravind@Aravind_V:~$
```

11.1.4. **Test Observation:** Not tested

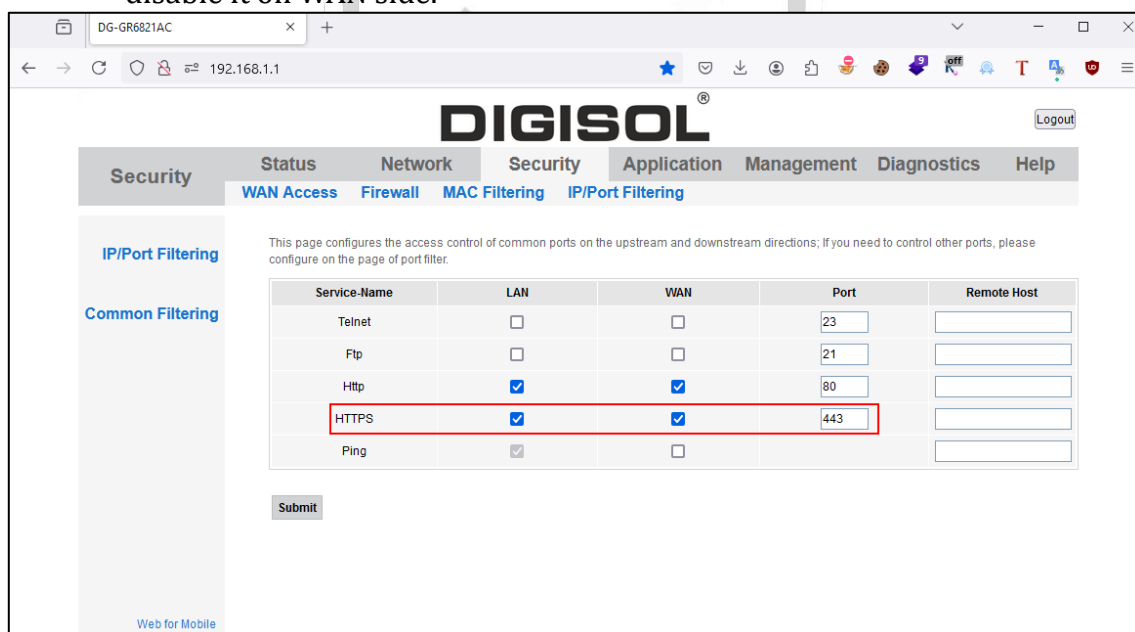
11.2 **Test Case Number:** 02

11.2.1. **Test Case Name:** 8.1.2

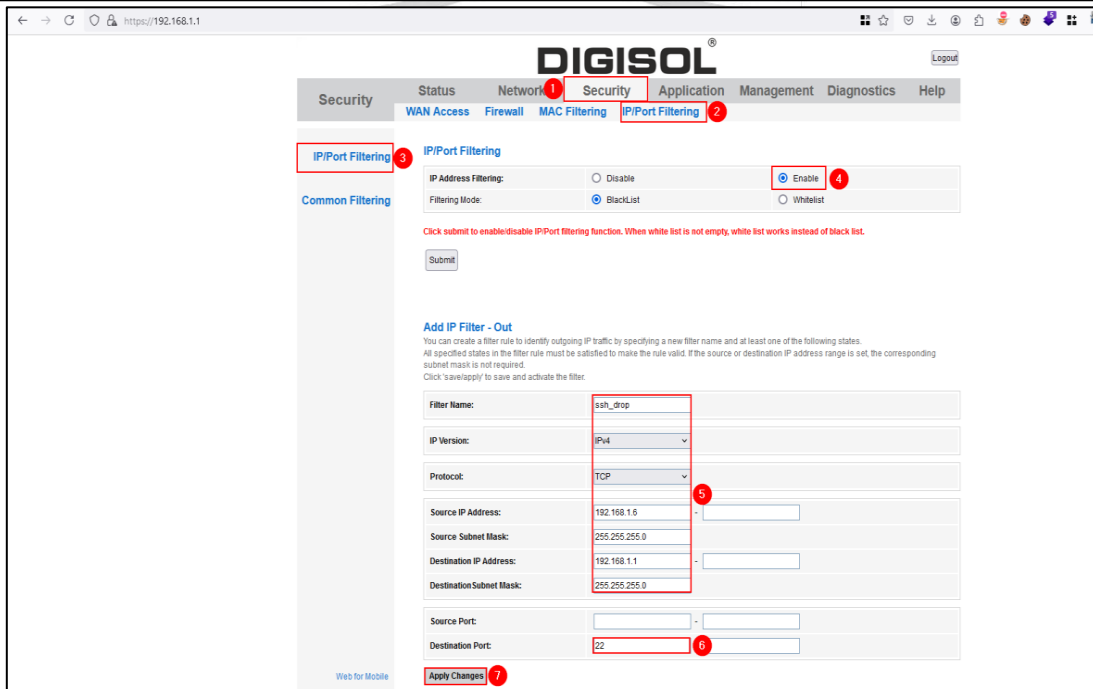
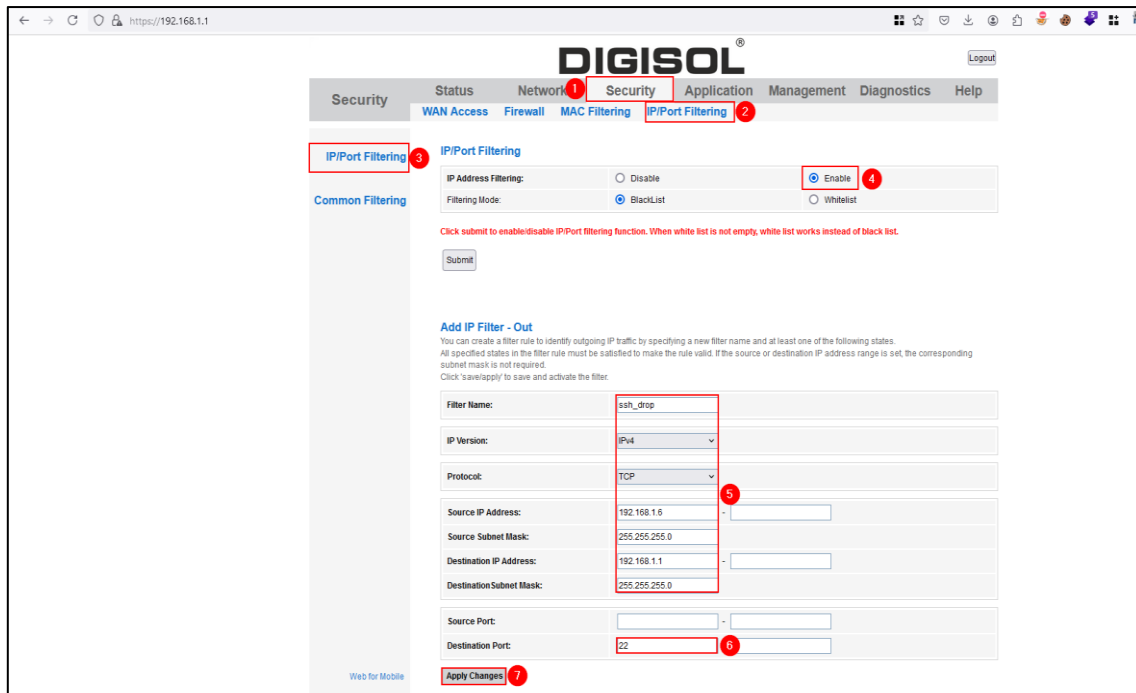
11.2.2. **Test Case Description:** To verify that services such as HTTP and SSH are not accessible from unauthorized interface (WAN) and illegitimate user.

11.2.3. **Execution Steps:**

1. Log into the DUT on PC1 using the admin account with the username admin and password admin123.
2. Then go to the “Security-> IP/Port filtering” in the GUI.
3. Enable the management protocols (SSH, HTTP/HTTPS) on the LAN side and disable it on WAN side.



4. Create IP filter rule for only legitimate user(entity) able to access the DUT.
Security -> IP/Port Filtering



5. Try to access the DUT from WAN side (illegitimate user) – ping, ssh, http/http

```

aravind@Aravind_V: ~$ sudo hping3 -p 22 192.168.1.1
[sudo] password for aravind:
HPING 192.168.1.1 (eth0 192.168.1.1): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.1.1 hping statistic ---
97 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
aravind@Aravind_V:~$

```

11.2.4. Test Observation: Not Tested

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not tested
2	8.1.2		Not Tested



2.3.10 TSTP for Evaluation of Avoidance of Unspecified Mode of Access

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.3.10
---	--------------------------	------------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

2. <ITSAR Section No & Name> Section 3: Software Security

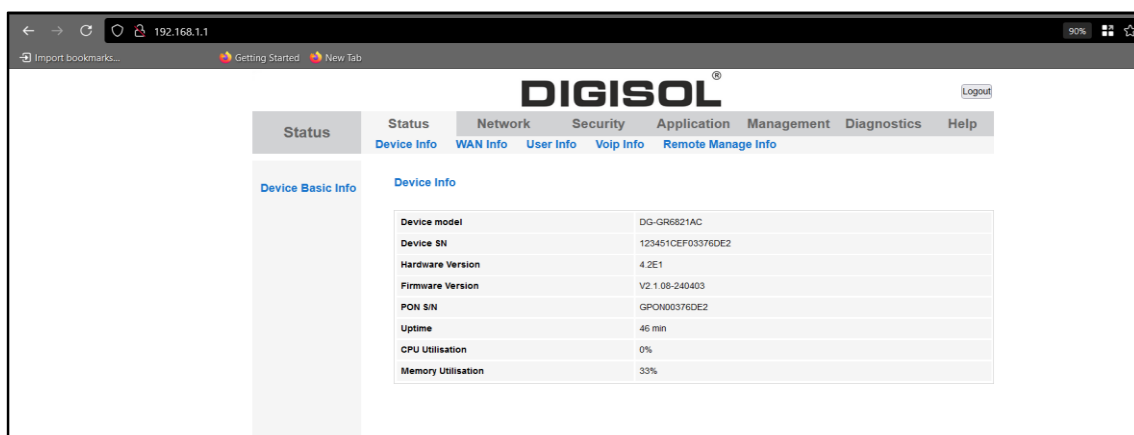
3. <Security Requirement No & Name > 2.3.10 Avoidance of Unspecified Mode of Access

4. <Requirement Description: > An undertaking shall be given by the vendor as follows:
"The ONU/ONT does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.3.4.6.1]

5. DUT Confirmation Details:

- Use the command line/GUI interface to get details of the machine on which test is conducted.
- Use GUI to get Application No/Version No & hardware Info
- The below screenshot shows the firmware version of the DUT

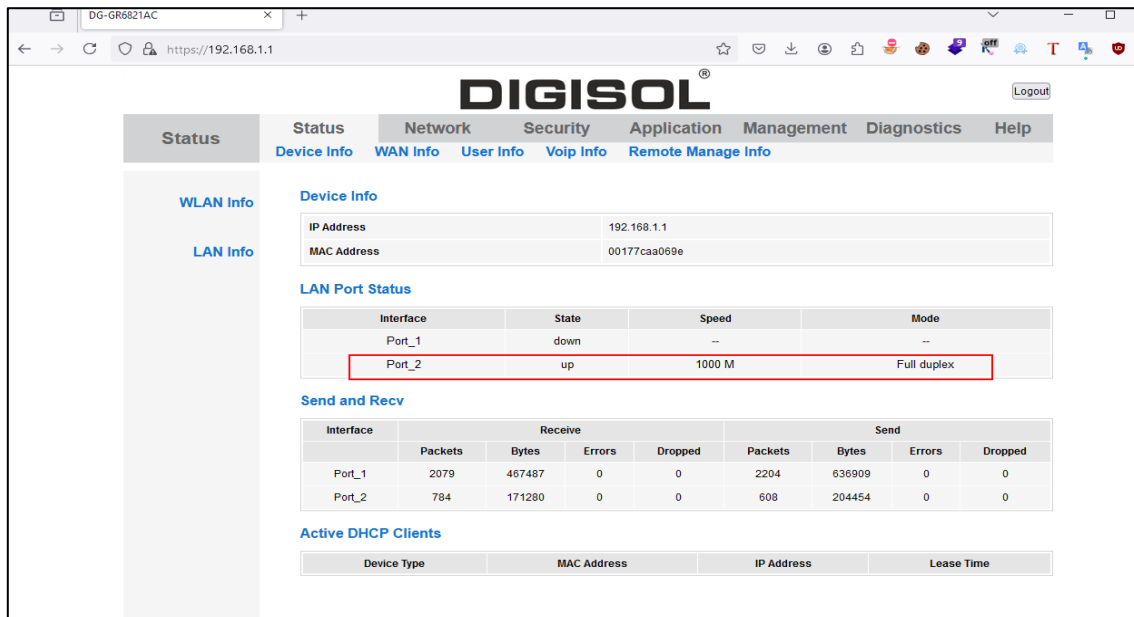




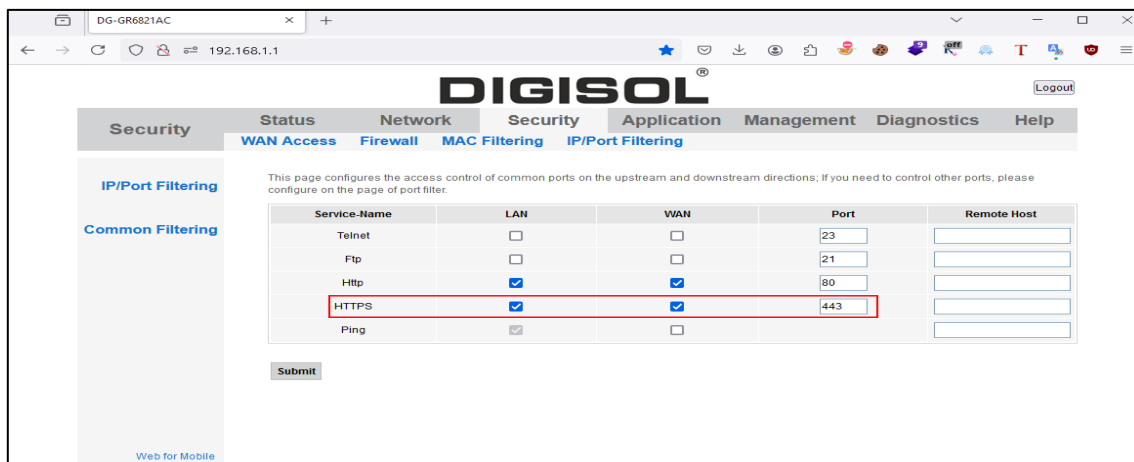
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

6. DUT Configuration:

- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.



ii. HTTPS is enabled.



iii. DUT is pre-configured with **BOA** as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~
aravind@Aravind_V:~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN
aravind@Aravind_V:~$ |

```

iv. Configure the NTP server ip address in the ONT GUI

7. **Precondition:** OEM should provide the undertaking as per the ITSAR requirement

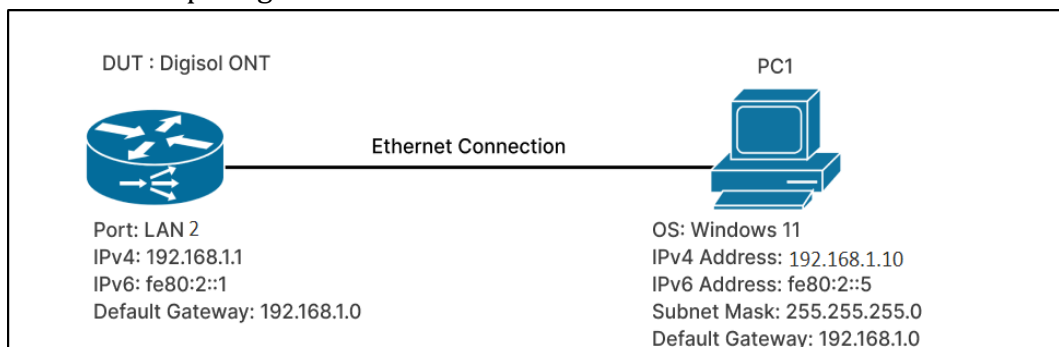
8. **Test Objective:** Verify that the DUT does not have any covert channel

9. **Test Plan:**

8.1 Number of Test Case Scenarios: 1

8.1.1 Verify that the DUT does not support covert channel with support of undertaking document

8.2 Test Setup Diagram



8.3 Tools Used:- Monitoring tools, logs of DUT

8.4 Test Execution Steps

- i. Check the OEM undertaking, as per the ITSAR requirement or not
- ii. Check the DUT logs for any traffic initiated by external devices or not
- iii. Monitor the DUT incoming/outgoing traffic

10. Expected Results for Pass:

- i. OEM undertaking document stating that “The ONU/ONT does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel”.
- ii. There should not be any unauthorized (Undocumented) communication channel present.

11. Expected Format of Evidence: Wireshark screenshots, DUT Logs

12. Test Execution:

11.1 Test Case Number: 01

12.1.1. Test Case Name: 8.1.1

Test Case Description:

Verify that the DUT does not support covert channel with support of undertaking document

Execution Steps:

- i. Check the OEM undertaking, as per the ITSAR requirement or not
- ii. “The ONU/ONT does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel”.
- iii. Check the DUT logs for any traffic initiated by external devices or not
- iv. Monitor the DUT incoming/outgoing traffic

Test Observation: - Not tested

13. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not tested

Section 4: System Secure Execution Environment

2.4.1 TSTP for Evaluation of No unused functions

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.4.1
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF

D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

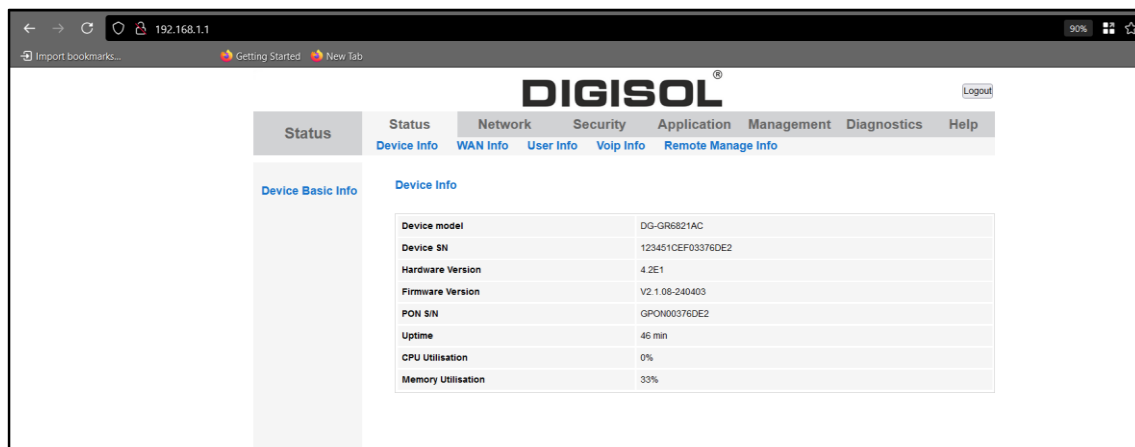
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 4: System Secure Execution Environment
2. **<Security Requirement No & Name >** 2.4.1 No unused functions
3. **<Requirement Description: >** Unused functions i.e. the software and hardware functions which are not needed for operation or functionality of the ONU/ONT shall not be present in the ONU/ONT's software and/or hardware. List of the used functions of the Networks s software and hardware as given by the vendor shall match the list of used software and hardware functions that are necessary for the operation of the ONU/ONT.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]

4. DUT Confirmation Details:

- i. Use the command line/GUI interface to get details of the machine on which test is conducted.
- ii. Use GUI to get Application No/Version No & hardware Info
- iii. The below screenshot shows the firmware version of the DUT





Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.

DIGISOL Logout

Status | Status | Network | Security | Application | Management | Diagnostics | Help

Device Info | WAN Info | User Info | Voip Info | Remote Manage Info

WLAN Info

LAN Info

Device Info

IP Address: 192.168.1.1

MAC Address: 00177caa069e

LAN Port Status

Interface	State	Speed	Mode
Port_1	down	--	--
Port_2	up	1000 M	Full duplex

Send and Recv

Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
Port_1	2079	467487	0	0	2204	636909	0	0
Port_2	784	171280	0	0	608	204454	0	0

Active DHCP Clients

Device Type	MAC Address	IP Address	Lease Time
-------------	-------------	------------	------------

ii. HTTPS is enabled.

DIGISOL Logout

Security | Status | Network | Security | Application | Management | Diagnostics | Help

WAN Access | Firewall | MAC Filtering | IP/Port Filtering

IP/Port Filtering

Common Filtering

This page configures the access control of common ports on the upstream and downstream directions; if you need to control other ports, please configure on the page of port filter.

Service-Name	LAN	WAN	Port	Remote Host
Telnet	☐	☐	23	
Ftp	☐	☐	21	
Http	☒	☒	80	
HTTPS	☒	☒	443	
Ping	☒	☐		

Submit

Web for Mobile

iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.

```
aravind@Aravind_V: ~
aravind@Aravind_V:~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN
aravind@Aravind_V:~$
```

6. **Precondition:** OEM have to provide document regarding a list of all available software or hardware and associated components containing at least the following information shall be included in the documentation accompanying the Network Product:

- 13.1.1. name of the software or hardware;
- 13.1.2. version of the software or hardware installed;
- 13.1.3. list of dependencies and versions;
- 13.1.4. any add-ons and functions;
- 13.1.5. any special hardware/debugging ports;
- 13.1.6. software or hardware support type;
- 13.1.7. licensing information;
- 13.1.8. requirement during functioning of system;
- 13.1.9. brief description of their purpose.
- 13.1.10.

7. **Test Objective:** To verify that DUT does not have any unused hardware and software functions

8. Test Plan:

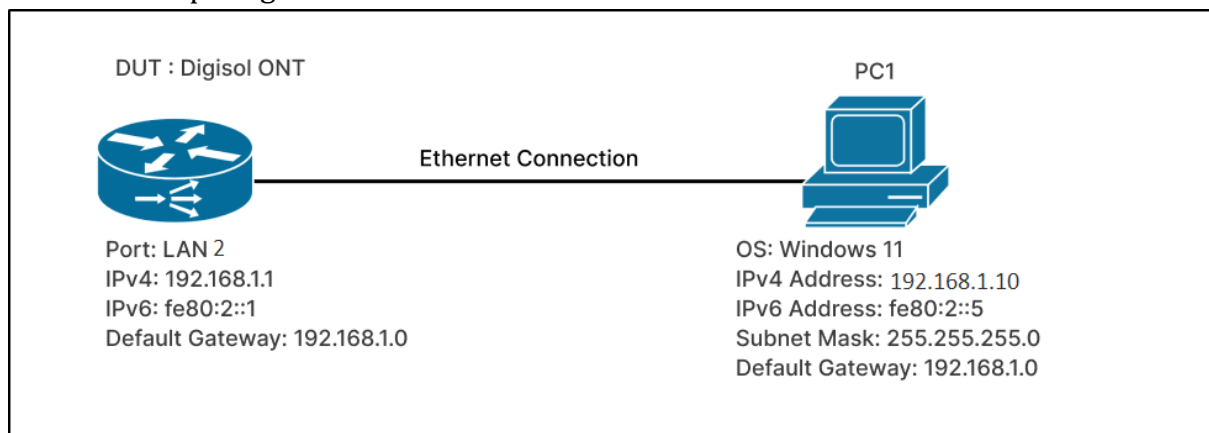
8.1 Number of Test Case Scenarios: 3

8.1.1 Verify that the OEM submitted document as per the precondition

8.1.2 Verify that the no unused hardware functions present in the DUT compare with OEM document

8.1.3 Verify that the no unused software functions present in the DUT compare with OEM document

8.2 Test Setup Diagram



8.3 Tools Used: - Web browser (For access GUI of DUT), CLI of DUT

8.4 Test Execution Steps

8.4.1. (A) Verify that the OEM submitted document as per the precondition,

- i. Verify that submitted BOM will be as per the precondition
- ii. To verify software function from software bill of materials (SBOM)
- iii. To verify hardware function from hardware bill of materials (HBOM)

8.4.2. (B) Verify that there is no unused hardware functions present in the DUT compare with OEM document

- i. Login to the DUT by CLI(SSH)

- ii. Check the any unused (which may not be needed for DUT functionality) hardware functions (USB) present in the CLI of DUT
- iii. Validate with OEM document

8.4.3. (C) Verify that there is no unused software functions present in the DUT compare with OEM document

- i. Login to the DUT by CLI(SSH)
- ii. Check the any unused (which may not be needed for DUT functionality) software functions (File transfer) present in the CLI of DUT
- iii. Validate with OEM document

9. **Expected Results for Pass:** There is no unused software/hardware functions present in the DUT

10. **Expected Format of Evidence:** Screenshots of terminal

11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1. **Test Case Name:** 8.1.1

11.1.2. **Test Case Description:** Verify that the OEM submitted document as per the precondition

11.1.3. **Execution Steps:**

- i. Verify that submitted BOM will be as per the precondition
- ii. To verify software function from software bill of materials(SBOM)
- iii. To verify hardware function from hardware bill of materials(HBOM)

11.2 **Test Case Number:** 02

11.2.1. Test Case Name: 8.1.2

11.2.2. Test Case Description: Verify that there is no unused hardware functions present in the DUT compare with OEM document

11.2.3. Execution Steps:

- i. Login to the DUT by CLI(SSH)
- ii. Check the any unused (which may not be needed for DUT functionality) hardware functions (USB) present in the CLI of DUT
- iii. Validate with OEM document

11.3 **Test Case Number:** 03

11.3.1. Test Case Name: 8.1.3

11.3.2. Test Case Description: Verify that there is no unused software functions present in the DUT compare with OEM document

11.3.3. Execution Steps:

- i. Login to the DUT by CLI(SSH)
- ii. Check the any unused (which may not be needed for DUT functionality) software functions (File transfer) present in the CLI of DUT
- iii. Validate with OEM document

12. **Test observation:** The testcase is “Not Tested”

13. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not tested
2	8.1.2		Not tested
3	8.1.3		Not tested

2.4.2 TSTP for Evaluation of No unsupported components

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.4.2
---	--------------------------	-----------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
DOCA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

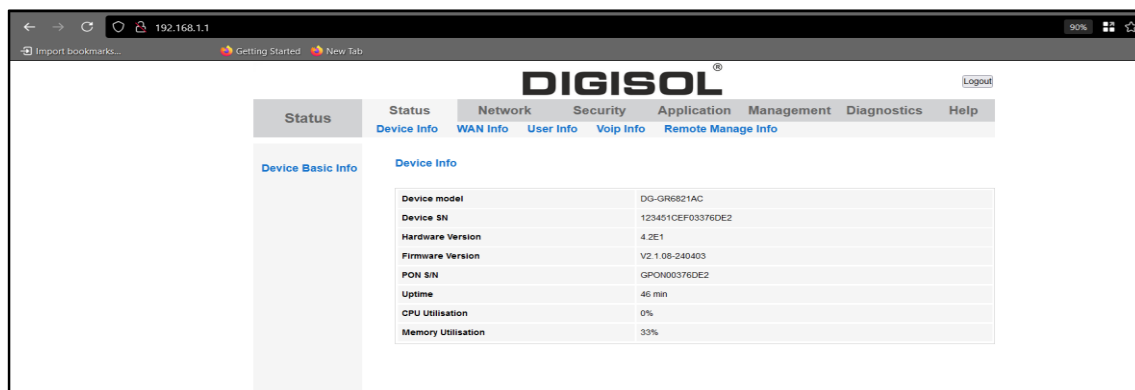
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 4: System Secure Execution Environment
2. **<Security Requirement No & Name >** 4.2 No unsupported components
3. **<Requirement Description: >** The ONU/ONT shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end-of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime. OEM to provide report and declaration to this effect.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.5]

4. DUT Confirmation Details:

- i. Use the command line/GUI interface to get details of the machine on which test is conducted.
- ii. Use GUI to get Application No/Version No & hardware Info
- iii. The below screenshot shows the firmware version of the DUT

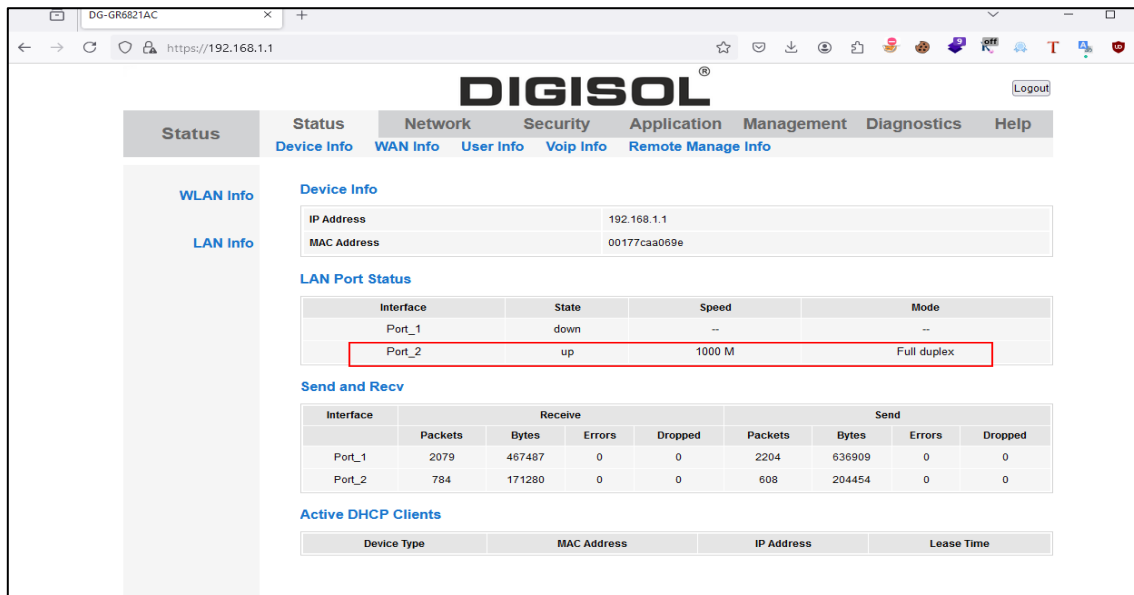




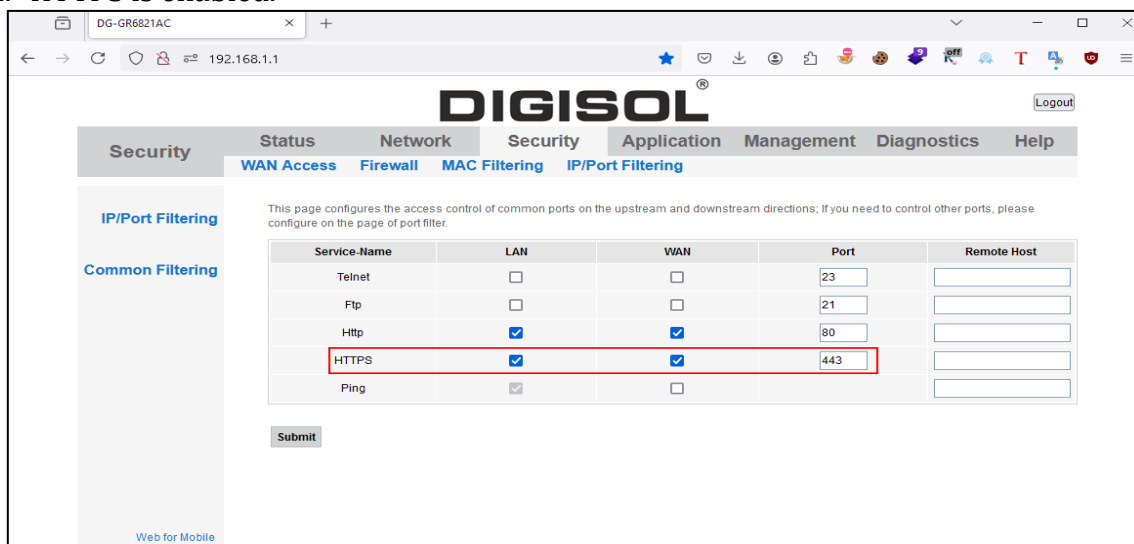
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

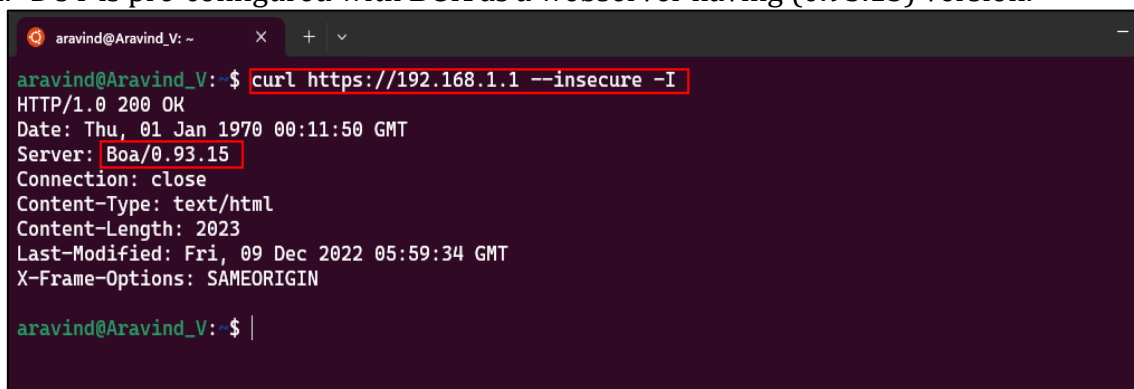
- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.



ii. HTTPS is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.



6. **Precondition:** OEM have to provide document regarding a list of all available software or hardware and associated components containing at least the following information shall be included in the documentation accompanying the Network Product:

- 13.1.11. name of the software or hardware;
- 13.1.12. version of the software or hardware installed;

- 13.1.13. list of dependencies and versions;
- 13.1.14. any add-ons and functions;
- 13.1.15. any special hardware/debugging ports;
- 13.1.16. software or hardware support type;
- 13.1.17. licensing information;
- 13.1.18. requirement during functioning of system;
- 13.1.19. brief description of their purpose.
- 13.1.20.

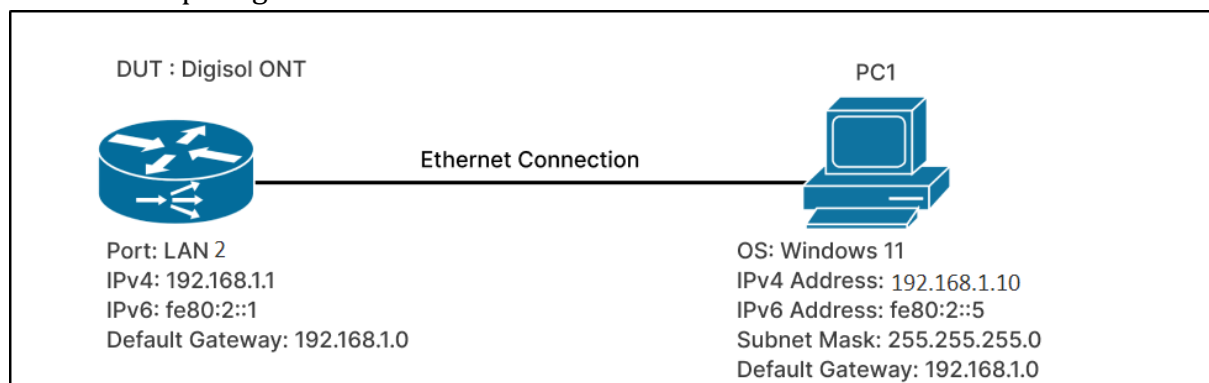
7. **Test Objective:** To ensure that all software and hardware components running in the network product are still supported and have not reached either their end-of-life or end-of-support.

8. Test Plan:

8.1 Number of Test Case Scenarios: 3

- 8.1.1 Verify that the OEM submitted document as per the precondition
- 8.1.2 Verify that the no EoL hardware functions present in the DUT compare with OEM document
- 8.1.3 Verify that the no EoL software functions present in the DUT compare with OEM document

8.2 Test Setup Diagram



8.3 Tools Used: - Web browser (For access GUI of DUT), CLI of DUT, XEOL

8.4 Test Execution Steps

- 8.4.1 (A) Verify that the OEM submitted document as per the precondition,
 - i. Verify that submitted BOM will be as per the precondition
 - ii. To verify software function from software bill of materials (SBOM)
 - iii. To verify hardware function from hardware bill of materials (HBOM)
- 8.4.2 (B) Verify that there is no EoL hardware functions present in the DUT compare with OEM document
 - i. Login to the DUT by CLI(SSH)
 - ii. Check the list of installed hardware functions in the CLI of DUT
 - iii. Check the EoL of software by internet search/automated tool
 - iv. Validate with OEM document
- 8.4.3 (C) Verify that there is no EoL software functions present in the DUT compare with OEM document
 - i. Login to the DUT by CLI(SSH)

- ii. Check the list of installed software functions in the CLI of DUT
 - iii. Check the EoL of software by internet search/automated tool(XEOL)
 - iv. Validate with OEM document
9. **Expected Results for Pass:** There is no EoL software/hardware functions present in the DUT
10. **Expected Format of Evidence:** Screenshots of terminal
11. **Test Execution:**
- 11.1 **Test Case Number:** 01
- 11.1.1. **Test Case Name:** 8.1.1
- 11.1.2. **Test Case Description:** Verify that the OEM submitted document as per the precondition
- 11.1.3. **Execution Steps:**
- i. Verify that submitted BOM will be as per the precondition
 - ii. To verify software function from software bill of materials (SBOM)
 - iii. To verify hardware function from hardware bill of materials (HBOM)
- 11.2 **Test Case Number:** 02
- 11.2.1. Test Case Name: 8.1.2
- 11.2.2. Test Case Description: Verify that there is no EoL hardware functions present in the DUT compare with OEM document
- 11.2.3. Execution Steps:
- i. Login to the DUT by CLI(SSh)
 - ii. Check the list of installed hardware functions in the CLI of DUT
 - iii. Validate with OEM document
- 11.3 **Test Case Number:** 03
- 11.3.1. Test Case Name: 8.1.3
- 11.3.2. Test Case Description: Verify that there is no EoL software functions present in the DUT compare with OEM document
- 11.3.3. Execution Steps:
- i. Login to the DUT by CLI(SSh)
 - ii. Check the list of installed software functions in the CLI of DUT
 - iii. 3. Validate with OEM document
- 11.3.4. **Test observation:** The testcase is "Not Tested"
12. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not tested
2	8.1.2		Not tested
3	8.1.3		Not tested

Section 5: User Audit

2.5.1 TSTP for Audit Event Generation

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.5.1
---	--------------------------	-----------------

<TSTP Document ID:>

<Applicant Name:>

<Application Number>

<DUT Details: > Ex: Router

<DUT Software Version:>

<Digest Hash of OS>

<Digest Hash of Configuration>

<Applicable ITSAR: >

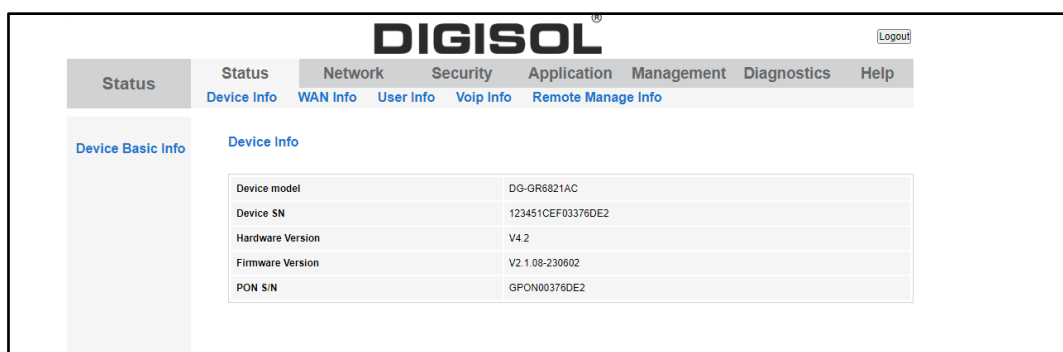
<ITSAR Version No:>

<OEM Supplied Document list: >

1. **<ITSAR Section No & Name>** Section 5– User Audit
2. **<Security Requirement No & Name >** 2.5.1 Audit Event Generation
3. **<Requirement Description: >** ONU/ONT to have capability to log important Security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.6.1;
2) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.5]

4. DUT Confirmation Details:



The screenshot displays the DIGISOL web management interface. At the top, the 'DIGISOL' logo is centered, with a 'Logout' link on the right. Below the logo is a navigation bar with tabs: 'Status', 'Network', 'Security', 'Application', 'Management', 'Diagnostics', and 'Help'. The 'Status' tab is active, showing sub-links: 'Device Info', 'WAN Info', 'User Info', 'Voip Info', and 'Remote Manage Info'. The 'Device Info' sub-link is selected, leading to a 'Device Basic Info' section. This section contains a table with the following details:

Device model	DG-GR6821AC
Device SN	123451CEF03376DE2
Hardware Version	V4.2
Firmware Version	V2.1.08-230602
PON S/N	GPON00376DE2



i. The DUT (IP: 192.168.1.1) is connected to the Lab Testing Machine over LAN 2.



- ii. HTTPS, SSH and FTP services are enabled

DIGISOL Logout

Security | Status | Network | Security | Application | Management | Diagnostics | Help

WAN Access | Firewall | MAC Filtering | IP/Port Filtering

IP/Port Filtering

This page configures the access control of common ports on the upstream and downstream directions; If you need to control other ports, please configure on the page of port filter.

Common Filtering

Service-Name	LAN	WAN	Port	Remote Host
Telnet	☐	☐	23	
Ftp	☒	☐	21	
Http	☐	☐	80	
HTTPS	☒	☐	443	
Secure Shell(SSH)	☒	☐	22	
Tftp	☐	☐		
Ping	☒	☐		

- iii. DUT is pre-configured with **BOA** as a webserver having (0.93.15) version.

```
aravind@Aravind_V: ~  
aravind@Aravind_V: $ curl https://192.168.1.1 --insecure -I  
HTTP/1.0 200 OK  
Date: Thu, 01 Jan 1970 00:11:50 GMT  
Server: Boa/0.93.15  
Connection: close  
Content-Type: text/html  
Content-Length: 2023  
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT  
X-Frame-Options: SAMEORIGIN
```

6. Preconditions:

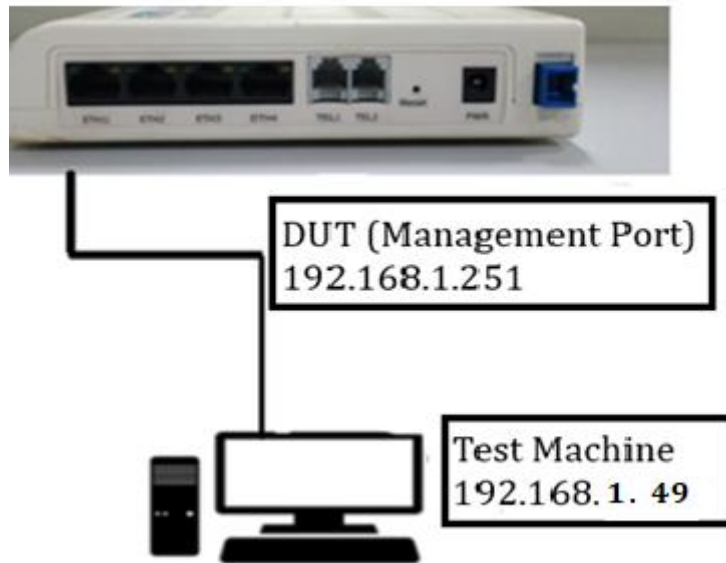
- Vendor to provide documentation (administration guide or any other document) on how to configure audit logs to be access controlled for various privilege levels.
 - The following information shall be provided by the documentation (administration guide or any other document) accompanying the network product:
 - The log where the event is recorded and how it can be accessed (e.g., the complete path).
 - If the event type is enabled by default or how to enable it.
 - Documentation (administration guide or any other document) describing where logs are stored and how these logs are accessed, and the Network Product interfaces that these logs can be accessed from.
 - Tester has the highest level of access to DUT.
7. **Test Objective:** - To verify that all the Security events are logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred. For each security event, the log entry shall include user name and/or timestamp and/or performed action and/or result and/or length of session and/or values exceeded and/or value reached.

8. Test Plan:

8.1 Number of Test Scenarios:

- 8.1.1 To verify that DUT logs important security events.
- 8.1.2 To verify that provision for secure log export is present in DUT.
- 8.1.3 To verify that audit logs preferably stored in Non-volatile memory.
- 8.1.4 To verify that High privilege user can read the logs but not to delete the logs.
- 8.1.5 To verify that low privilege users cannot read the logs also are not able to delete the logs.

8.2 Test Setup Diagram:



8.3 Tools Used: - Wireshark

8.4 Test Execution Steps

- i. The Tester sequentially triggers each security event,
- ii. The Tester verifies whether the security events, and their individual options, were correctly logged. In particular it is verified whether they include at least the event data specified as required to be logged.

9. **Expected Results to Pass:** The security events are properly logged along with the minimum required details as mentioned.

10. **Expected Evidence:** The testing report contains the following information for each security event:

- i. List of O&M services.
- ii. Commands executed per O&M services
- iii. The relevant parts of the logs in appropriate form (e.g. file, screenshot).

11. Test Execution:

11.1 Test Case Number: 1

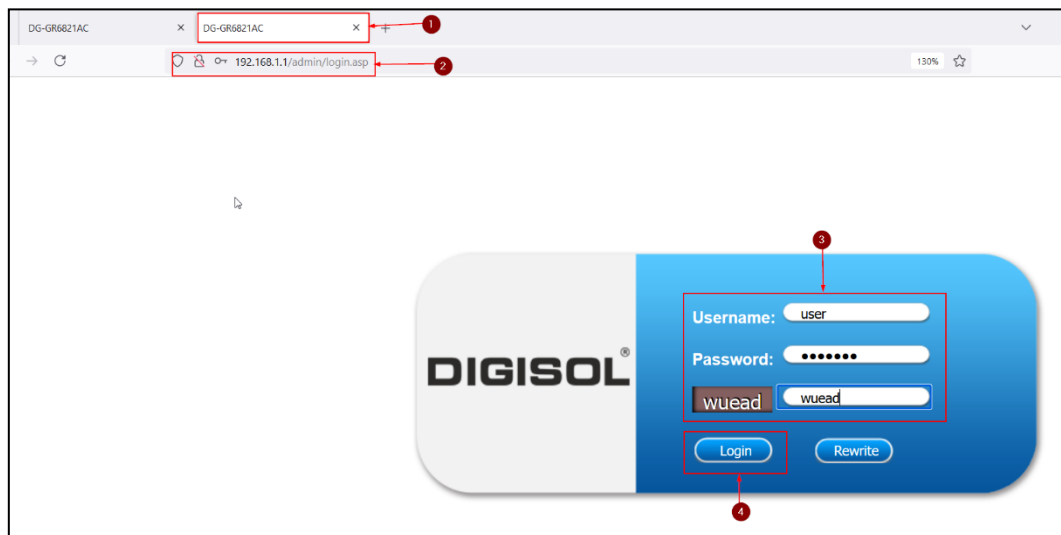
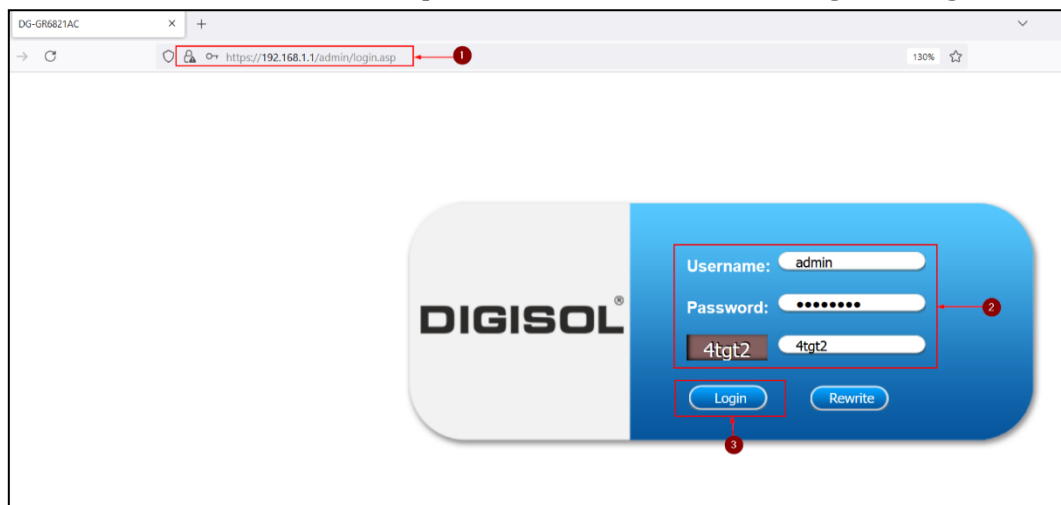
11.1.1 Test Case Name: TC_AUDIT_EVENT_GENERATION

11.1.2 Test Case Description: To verify that the network product correctly logs all required security event.

11.1.3 Execution Steps:

11.1.4 Execution Steps:

- i. Launch Wireshark to capture packets on the "Ethernet" interface.
- ii. To log into the web interface of the ONT, open a web browser and enter the default gateway address (**192.168.1.1**) in the address bar.
- iii. To login through Administration Account, enter the username **admin** and password "**admin123**" in the login dialog box.
- iv. Open the new private window to login DUT through Lowest Privilege user, enter the username "**user**" and password "**user123**" in the login dialog box.



- v. Check the logs in DUT for below mention security events occurred in DUT.

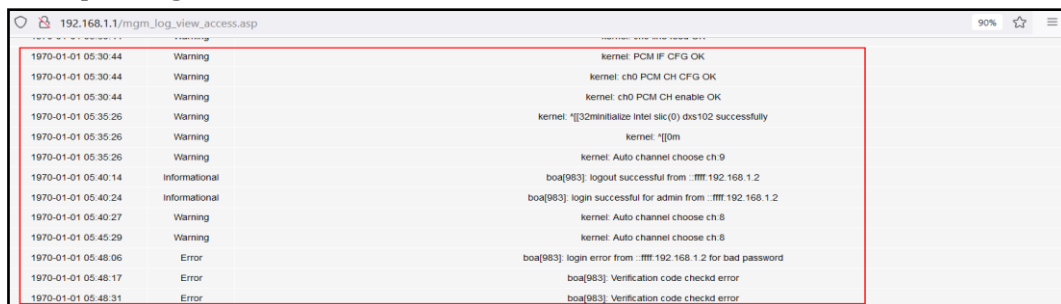
A. Log Generation 1: Incorrect Log In attempts (Mandatory)

Check the initial logs before incorrect login.

- b. To access the DUT's web interface, login with administrative privilege user **"admin"** and low privilege user **"user"** with correct credentials



- c. Check the logs for administrative access privilege user **"admin"** and low level privilege **"user"**.



C. Log Generation 3: Account Administration (Mandatory)

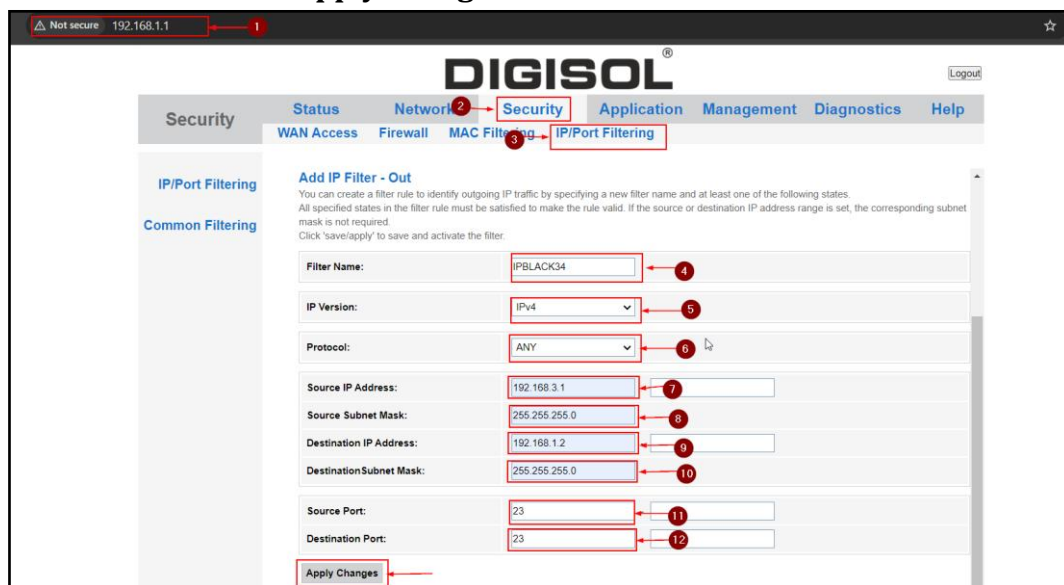
- a. Check the initial logs before all account administration activity configure, deleting, enabling, and disabling any activity.
- b. To test the ability to **create, modify, and manage activities** using both administrative **"admin"** and low-privilege **"user"** accounts.
- c. Following are some activity to check if logs are generated for above mention ability:

Try to configure IP/Port filtering to check if logs are generated for the same, navigate to the **Security** tab and select **IP/Port Filtering**. Enable IP address filtering and activate the **blacklist** option, then click **Submit** to save your changes.

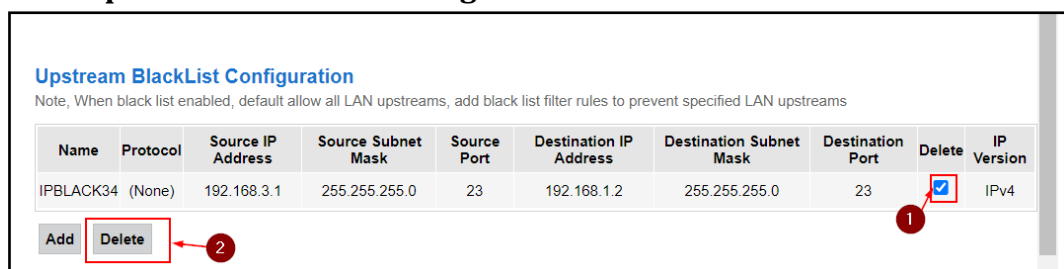


d. To check if logs are generated for the below blacklist activity, configure the **Upstream Blacklist**, click "ADD" and enter the necessary details as follows.

- **Filter Name:** IPBLACK34
- **Select IP Version:** IPv4
- **Select Protocol:** ICMP
- **Enter Source IP Address :** 192.168.3.1
- **Enter Source Subnet Address:** 255.255.255.0
- **Enter Destination IP address :** 192.168.1.2
- **Enter Destination Subnet Address:** 255.255.255.0
- **Enter Source PORT:** 23
- **Enter Destination PORT :23**
- Click on **Apply changes** Button



e. To check if logs are generated for delete configuration activity, delete selected **Upstream Black List Configuration**.



f. Verify that DUT generates log.

D. Log Generation 4: Resource Usage (Mandatory)

Note: The features to set the parameter values such as disk space, CPU load are not available in this DUT. Hence the tester has provided general guidelines for performing this test.

a. Check the initial logs before resource usage.

b. Locate the option to define thresholds for critical resource utilization levels (These thresholds indicate when resource usage becomes excessive. For example: Disk space, CPU load threshold etc.)

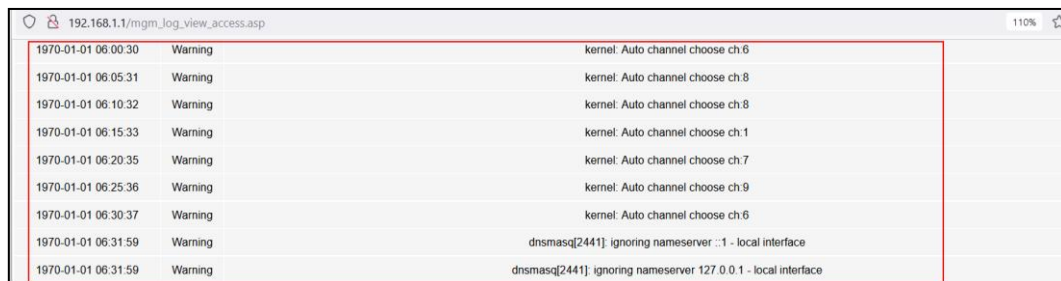
c. To test resource usage exceeding the defined thresholds by following:

- Transferring large amounts of data to test disk space limitations
- Running resource-intensive applications to increase CPU load.

d. Verify that DUT generates log.

e. Log Generation 5: Configuration change (Mandatory)

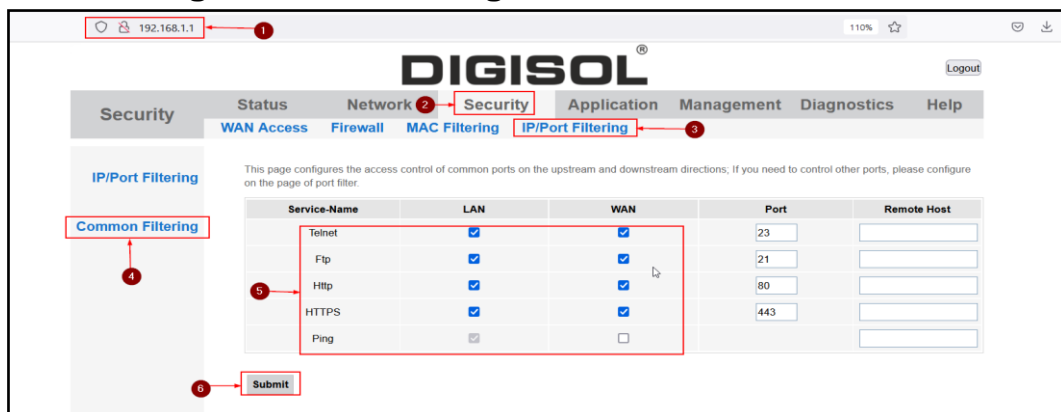
- Check initial logs before changing configuration



The screenshot shows a web browser window with the URL 192.168.1.1/mgm_log_view_access.asp. It displays a table of log entries. A red box highlights the first seven rows, which all show 'Warning' messages from the kernel about auto channel choices. The last two rows show 'Warning' messages from dnsmasq[2441] ignoring nameserver ::1 - local interface.

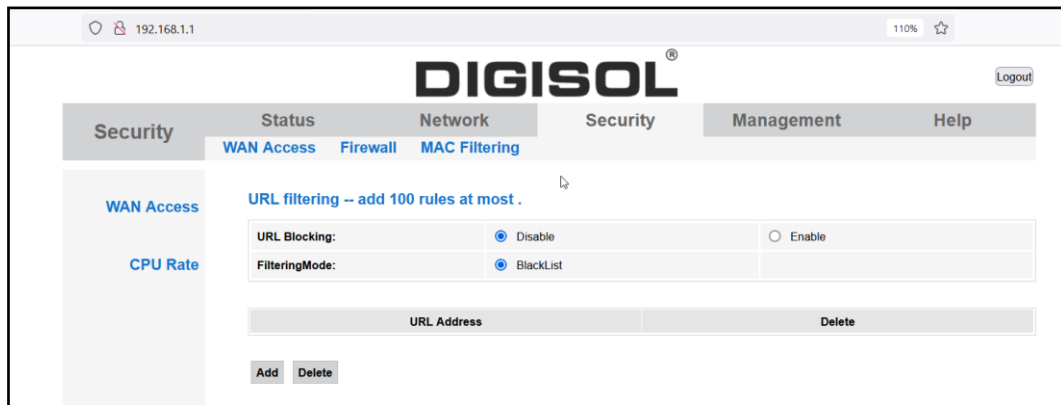
Time	Level	Message
1970-01-01 06:00:30	Warning	kernel: Auto channel choose ch.6
1970-01-01 06:05:31	Warning	kernel: Auto channel choose ch.8
1970-01-01 06:10:32	Warning	kernel: Auto channel choose ch.8
1970-01-01 06:15:33	Warning	kernel: Auto channel choose ch.1
1970-01-01 06:20:35	Warning	kernel: Auto channel choose ch.7
1970-01-01 06:25:36	Warning	kernel: Auto channel choose ch.9
1970-01-01 06:30:37	Warning	kernel: Auto channel choose ch.6
1970-01-01 06:31:59	Warning	dnsmasq[2441]: ignoring nameserver ::1 - local interface
1970-01-01 06:31:59	Warning	dnsmasq[2441]: ignoring nameserver 127.0.0.1 - local interface

f. To enable all services for both the "admin" user with administrative privileges and the "user" with lower privileges on the DUT. Navigate **Security > IP/Port Filtering > Common Filtering** click radio button to enable.



The screenshot shows the DIGISOL web interface. The 'Security' tab is selected, and within it, 'IP/Port Filtering' is chosen. The 'Common Filtering' radio button is selected. A table lists services and their status for LAN and WAN. A red box highlights the 'Common Filtering' section and the 'Submit' button. Red numbers 1 through 6 are placed around the interface to indicate the steps: 1. Address bar, 2. Security tab, 3. IP/Port Filtering sub-tab, 4. Common Filtering radio button, 5. Table, 6. Submit button.

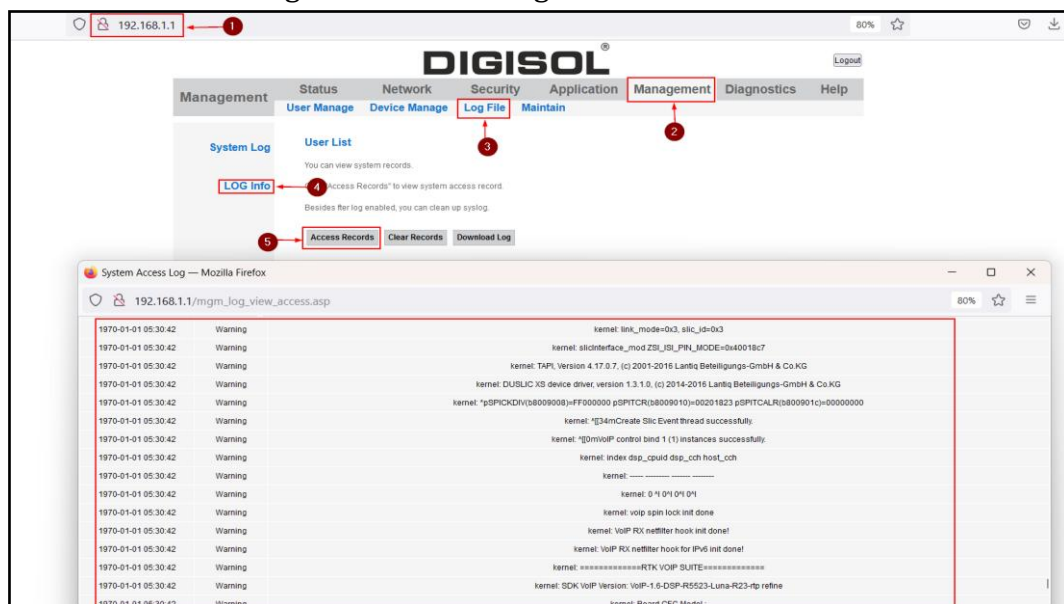
Service-Name	LAN	WAN	Port	Remote Host
Telnet	☒	☒	23	
Ftp	☒	☒	21	
Http	☒	☒	80	
HTTPS	☒	☒	443	
Ping	☒	☐		



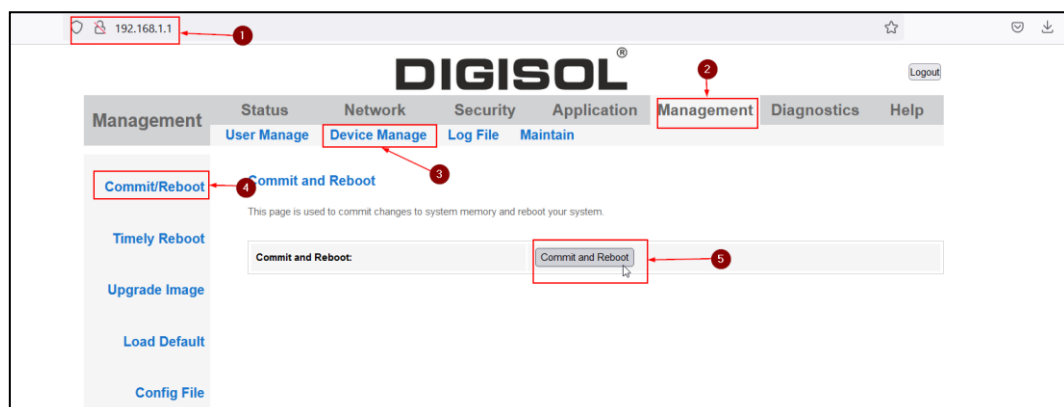
g. Check the logs for changes made in configuration of DUT via administration privilege user “admin” and privilege user “user”.

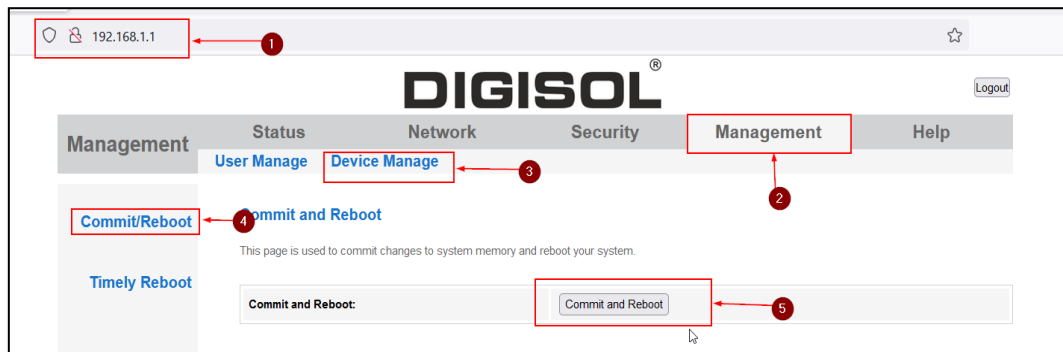
E. Log Generation 6: Reboot/shutdown/crash (Mandatory)

a. Check initial logs before rebooting DUT.



b. Reboot the DUT via administration privilege user “admin” and low privilege user

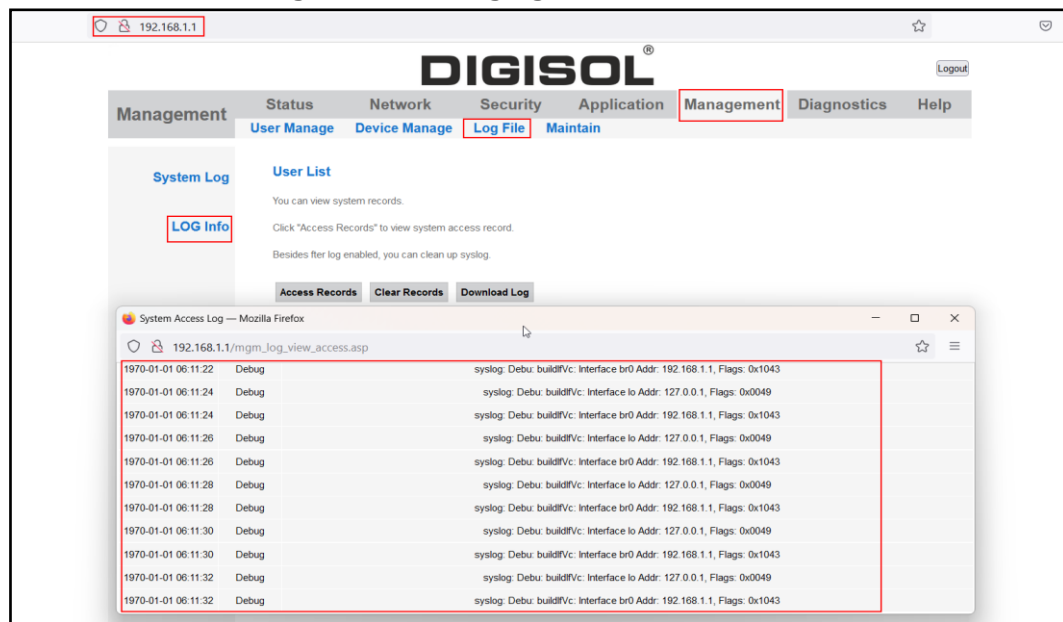




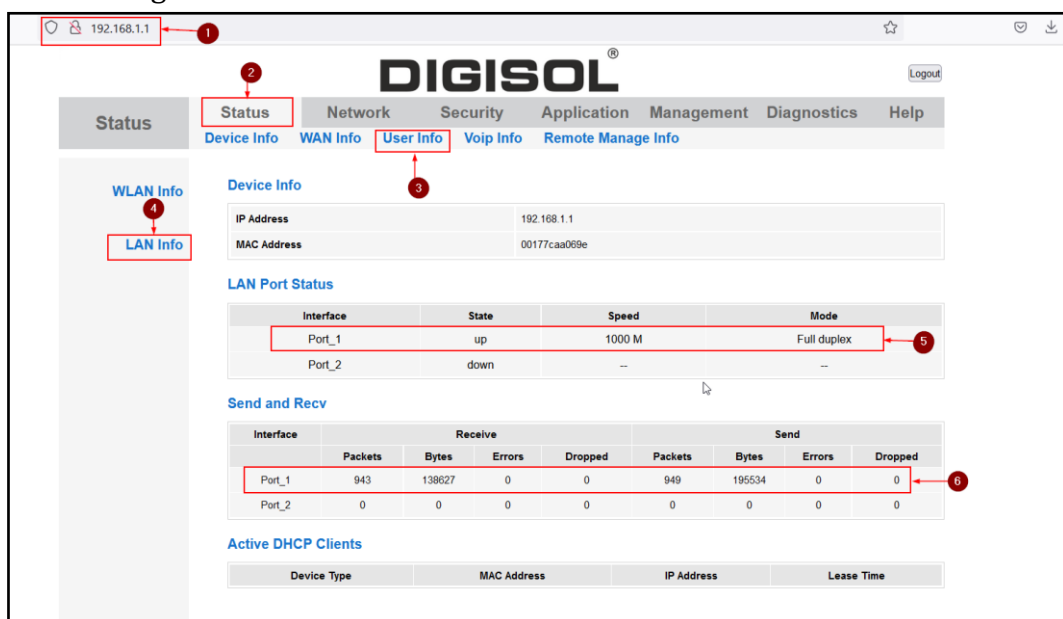
c. Check the logs post reboot.

E. Log Generation 7: Interface status change (Mandatory)

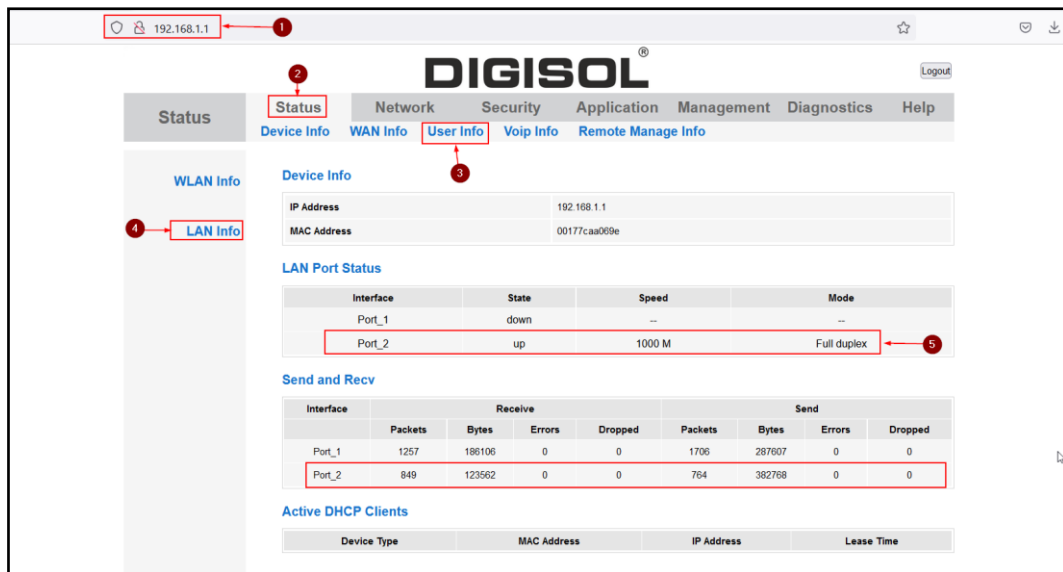
a. Check initial logs before changing interface status.



b. Initially plug the ethernet cable in "LAN-1" and check the status of LAN-1, Navigate to **Status > user info > LAN info > LAN-1-**



- c. Now remove the ethernet cable from LAN-1 and insert it into LAN-2 and check the status of LAN-2, Navigate to **Status > user info > LAN info > LAN-2**.



- d. Check the logs for interface status changes.

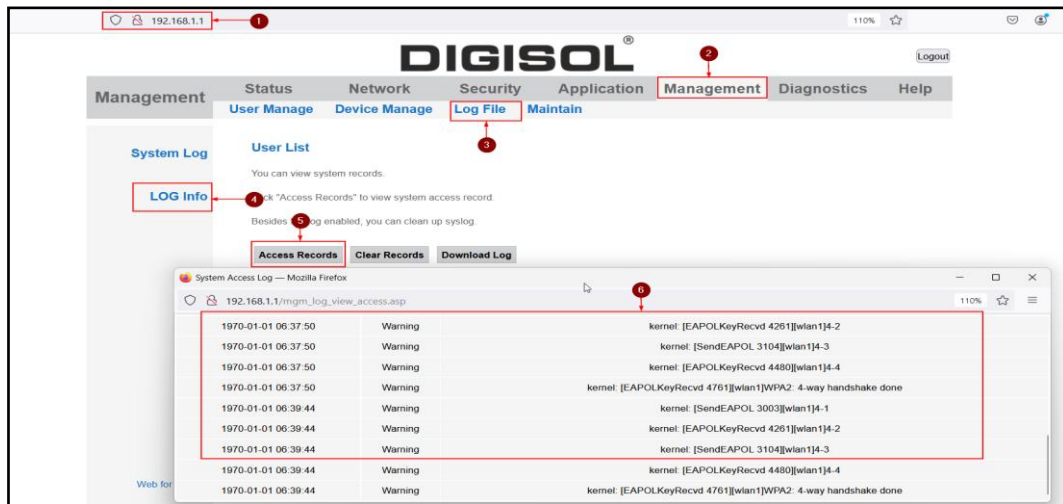
G. Log Generation 8: Change of group membership or accounts (Optional)

Note: The features Change of group membership or accounts are not available on this

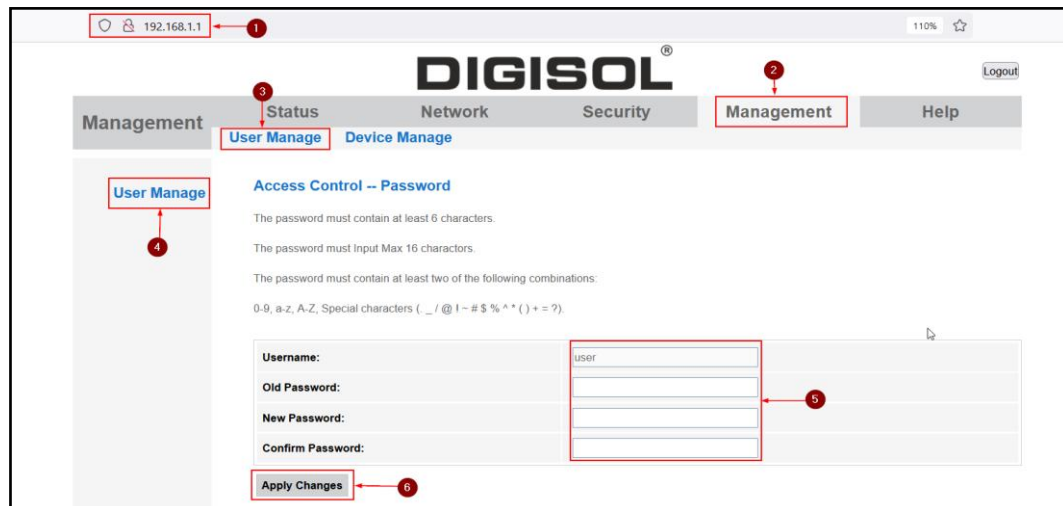
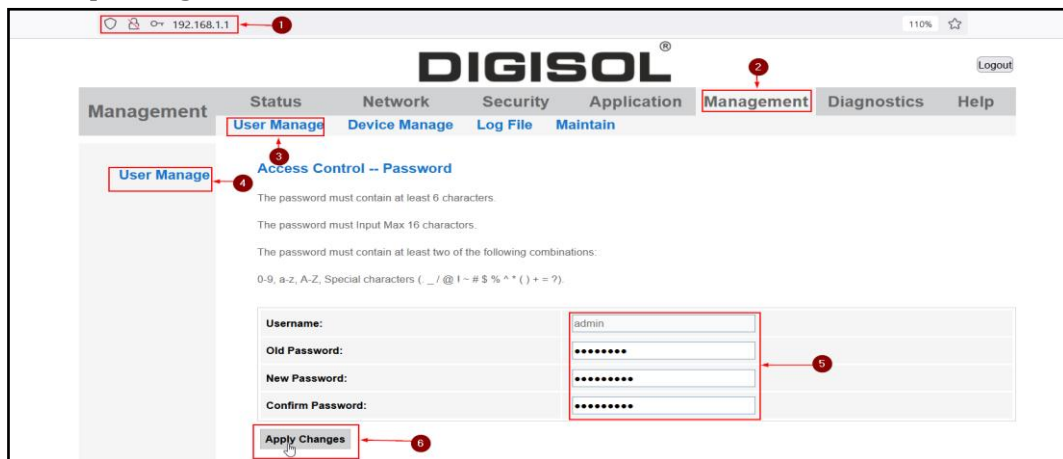
- Check initial logs before changing group via administration privilege user “admin” and low privilege user “user”.
- (Browser A) login with low privilege user and check whether this user can have any change of group membership for accounts. Then logout from the current user account.
- (Browser B) login with admin privilege user and check whether this user can have any change of group membership for accounts.
Check the logs for changes made via administration privilege user “admin” and low privilege user “user”.

H. Log Generation 9: Resetting Passwords (Optional)

- Check initial logs before resetting password of administration privilege user “admin” and access privilege user “user”.



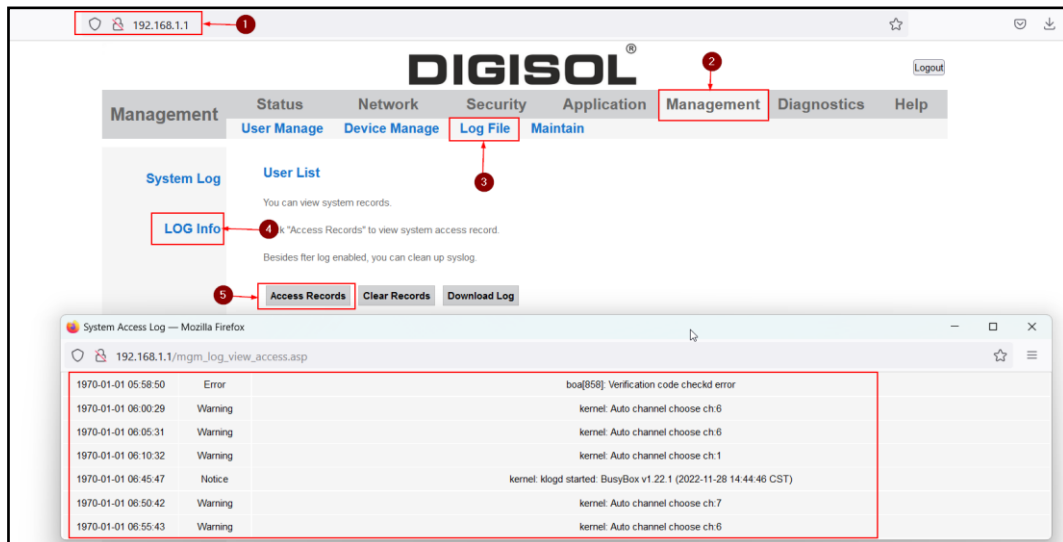
b. Steps to reset password of administration privilege user “admin” and low privilege user “user”.



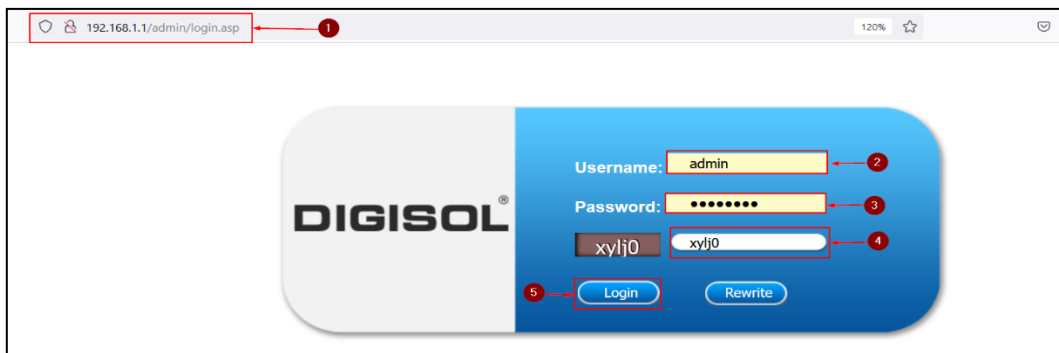
c. Check the logs for changes made in password of administration privilege user “admin” and low privilege user “user”.

I. Log Generation 11: user Login (Mandatory)

a. Check initial logs.



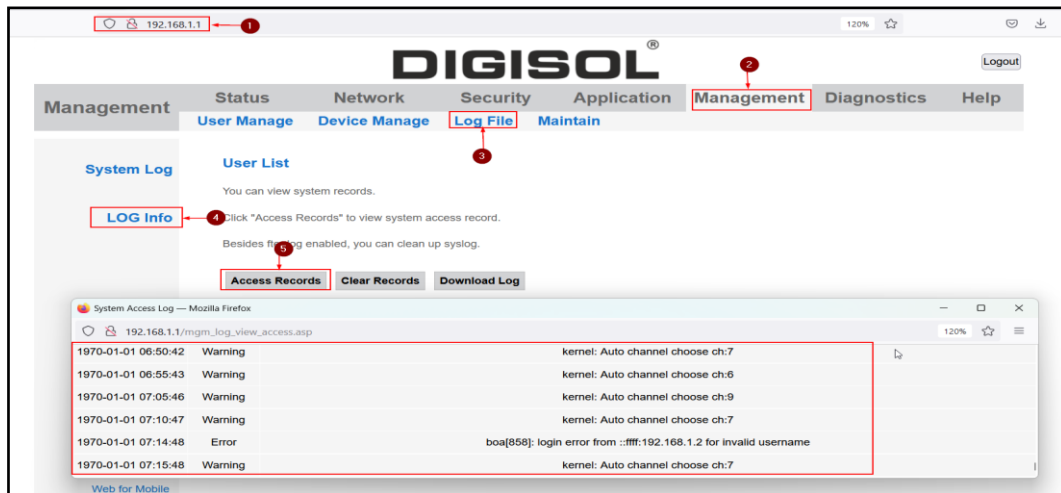
- b. Below is the sample to check if logs are generated for the authentication mechanism used in the DUT while accessing:
- Login into DUT via administration privilege user “admin” and low privilege user “user”



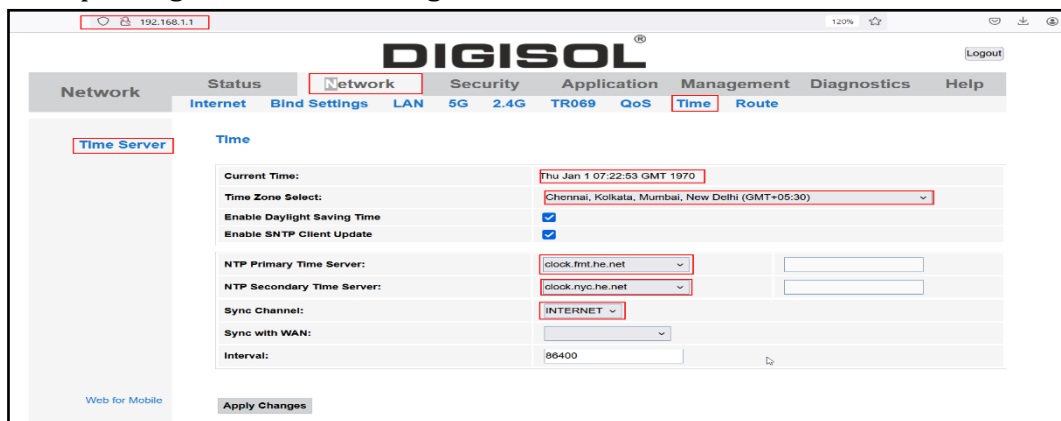
- c. Check logs for user identification details.

L Log Generation 14: Time Change (Mandatory)

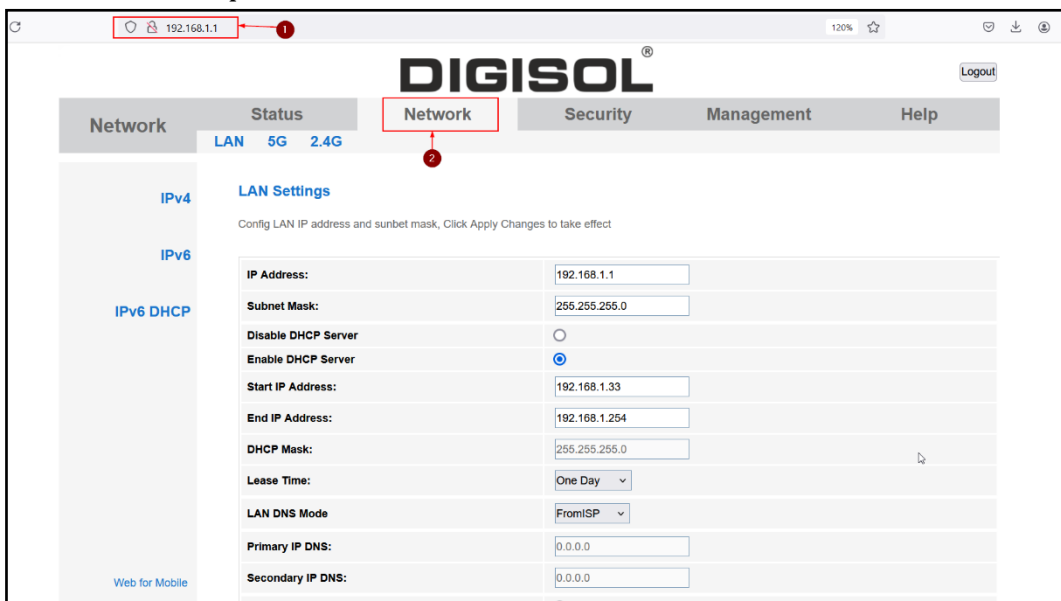
- a. Check initial logs before making changes in DUT time.



b. To change time of DUT via administration privilege user “admin” and low privilege user “user”, navigate **Network > Time**.



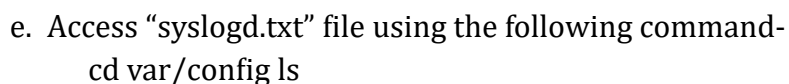
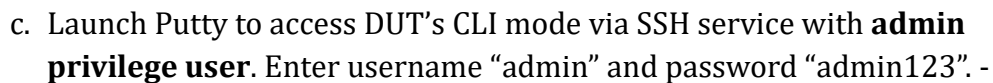
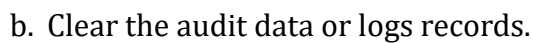
Note: In this DUT, users with low privilege cannot modify the date and time. If the date and time modification functionality is available for a normal user, the OEM must provide the relevant OEM documentation.



c. Check logs for changes made in time of DUT via administration privilege user “admin” and low access privilege user “user”.

- a. Check initial logs before making changes in DUT log.

- a. Check initial logs before making changes in DUT log.



- f. Check “syslogd.txt” file before manually add logs using the following command. – cat syslogd.txt

```
# cat syslogd.txt
Manufacturer:DIGISOL;
ProductClass:DG-GR6821AC;
SerialNumber:00177C-GPON00A9D06E;
IP:192.168.1.1;
HwVer:V4.2C1;
SwVer:V3.2.02-240516;

1970-01-01 09:27:34 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:32:35 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:37:37 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:42:38 [Warning] kernel: Auto channel choose ch:8
1970-01-01 09:47:39 [Warning] kernel: Auto channel choose ch:9
#
```

- g. Add manually fake logs in syslogd.txt file using the following command.
echo “1971-04-01 01:47:39 [Warning] kernel:DUT Fake log” >> syslogd.txt

```
1970-01-01 09:52:40 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:54:32 [Warning] kernel: [SendEAPOL 3003][wlan1]4-1
1970-01-01 09:54:32 [Warning] kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
1970-01-01 09:54:36 [Warning] kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
#
# echo 1971-04-01 01:47:39 [Warning] kernel:DUT Fake log? >> syslogd.txt
```

- h. Check “syslogd.txt” file before manually add logs using the following command. cat syslogd.txt

```
# echo 1971-04-01 01:47:39 [Warning] kernel:DUT Fake log? >> syslogd.txt
# cat syslogd.txt
Manufacturer:DIGISOL;
ProductClass:DG-GR6821AC;
SerialNumber:00177C-GPON00A9D06E;
IP:192.168.1.1;
HwVer:V4.2C1;
SwVer:V3.2.02-240516;

1970-01-01 09:27:34 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:32:35 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:37:37 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:42:38 [Warning] kernel: Auto channel choose ch:8
1970-01-01 09:47:39 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:52:40 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:54:32 [Warning] kernel: [SendEAPOL 3003][wlan1]4-1
1970-01-01 09:54:32 [Warning] kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
1970-01-01 09:54:36 [Warning] kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
1971-04-01 01:47:39 [Warning] kernel:DUT Fake log?
#
```

- i. To confirm that logs are added, login into DUT Web interface via administration privilege user “admin.”

11.1.5 Evidence Provided:

1. Log Generation 1: Incorrect Log In attempts (Mandatory)

- Logs for Incorrect login attempts present in DUT with following details.

- username: Not Present
- Source IP: Present
- Outcome of Event: Present
- Timestamp: Present

Timestamp	Event Type	Message
1970-01-01 09:00:21	Error	boa[915]: malformed request: "(null)"
1970-01-01 12:04:09	Error	boa[915]: Error opening web/favicon.ico for ::ffff:192.168.1.8: No such file or directory
1970-01-01 12:04:15	Error	boa[915]: Error opening web/favicon.ico for ::ffff:192.168.1.8: No such file or directory
1970-01-01 12:07:46	Emergency	kernel: reboot: Restarting system
1970-01-01 08:55:22	Error	boa[854]: login error from ::ffff:192.168.1.2 for bad password
1970-01-01 08:58:23	Error	boa[854]: login error from ::ffff:192.168.1.2 for invalid username

2. Log Generation 2: Administrator Access (Mandatory)

- In This DUT administrator can access web GUI access. But normal user can't access administrator level feature in this DUT.
 - i. **Username:** Present
 - ii. **Timestamp:** Present
 - iii. **Length of session:** Not Present
 - iv. **Outcome of event (Success or failure) :** Present
 - v. **Source (IP address) if remote access :** Present

1970-01-01 05:30:44	Warning	kernel: PCM IF CFG OK
1970-01-01 05:30:44	Warning	kernel: ch0 PCM CH CFG OK
1970-01-01 05:30:44	Warning	kernel: ch0 PCM CH enable OK
1970-01-01 05:35:26	Warning	kernel: "[32]initialize intel sic(0) dxs102 successfully
1970-01-01 05:35:26	Warning	kernel: "[0m
1970-01-01 05:35:26	Warning	kernel: Auto channel choose ch.9
1970-01-01 05:40:14	Informational	boa[963]: logout successful from :ffff:192.168.1.2
1970-01-01 05:40:24	Informational	boa[963]: login successful for admin from :ffff:192.168.1.2
1970-01-01 05:40:27	Warning	kernel: Auto channel choose ch.8
1970-01-01 05:45:29	Warning	kernel: Auto channel choose ch.8
1970-01-01 05:48:06	Error	boa[963]: login error from :ffff:192.168.1.2 for bad password
1970-01-01 05:48:17	Error	boa[963]: Verification code checked error
1970-01-01 05:48:31	Error	boa[963]: Verification code checked error

3. Log Generation 3: Account Administration (Mandatory)

- Logs for IP Port filtering configuration in DUT with following details.
 - i. **Administrator username:** Not Present
 - ii. **Administered account:** Not Present
 - iii. **Source IP:** Not Present
 - iv. **Activity performed (configure, delete, enable**
 - v. **and disable):** Not Present
 - vi. **Timestamp:** Not Present

1970-01-01 05:30:24	Warning	kernel: IPv4+IPv6 both bridge
1970-01-01 05:30:24	Warning	kernel: get mntr error!!!
1970-01-01 05:30:24	Warning	kernel: get mntr error!!!
1970-01-01 05:30:24	Warning	kernel: get mntr error!!!
1970-01-01 05:30:24	Warning	kernel: get mntr error!!!
1970-01-01 05:30:24	Warning	kernel: get mntr error!!!
1970-01-01 05:30:25	Warning	kernel: get mntr error!!!
1970-01-01 05:30:25	Warning	kernel: get mntr error!!!
1970-01-01 05:30:25	Warning	kernel: get mntr error!!!
1970-01-01 05:30:25	Warning	kernel: get mntr error!!!
1970-01-01 05:30:25	Warning	kernel: get mntr error!!!
1970-01-01 05:30:25	Warning	kernel: get mntr error!!!
1970-01-01 05:30:25	Warning	dnsmasq[2323]: ignoring nameserver ::1 - local interface
1970-01-01 05:30:25	Warning	dnsmasq[2323]: ignoring nameserver 127.0.0.1 - local interface
1970-01-01 00:00:11	Critical	dnsmasq[878]: cannot read /var/dnsmasq.conf: No such file or directory
1970-01-01 00:00:11	Critical	dnsmasq[878]: FAILED to start up
1970-01-01 00:00:11	Critical	dnsmasq[881]: cannot read /var/dnsmasq.conf: No such file or directory
1970-01-01 00:00:11	Critical	dnsmasq[881]: FAILED to start up
1970-01-01 00:00:12	Critical	dnsmasq[885]: cannot read /var/dnsmasq.conf: No such file or directory
1970-01-01 00:00:12	Critical	dnsmasq[885]: FAILED to start up
1970-01-01 00:00:12	Critical	dnsmasq[915]: failed to create listening socket: Address already in use
1970-01-01 00:00:12	Critical	dnsmasq[915]: FAILED to start up

4. Log Generation 4: Resource Usage (Mandatory)

Note: The features to set the parameter values such as disk space, CPU load are not available in this DUT.

5. Log Generation 5: Configuration change (Mandatory)

- Lowest privilege user “user” doesn’t have rights to make changes in configuration of DUT hence log is not generated for same.
- Configuration changes via administration privilege user “admin” are visible in DUT log with the following details.
 - i. **username:** not Present
 - ii. **Timestamp:** Present
 - iii. **Changes made:** Present.
 - iv. **Outcome of Event:** Present

1970-01-01 06:31:59	Warning	dnsmasq[2441]: ignoring nameserver 127.0.0.1 - local interface
1970-01-01 06:35:38	Warning	kernel: Auto channel choose ch 6
1970-01-01 06:35:49	Error	routed[2490]: Cannot log to -D: not under /var/log/
1970-01-01 06:35:49	Error	routed[2490]: adding route to nethost 192.168.1.0 through gateway 192.168.1.1: Cannot assign requested address
1970-01-01 06:35:57	Error	routed[2507]: Cannot log to -D: not under /var/log/
1970-01-01 06:35:57	Error	routed[2507]: adding route to nethost 192.168.1.0 through gateway 192.168.1.1: Cannot assign requested address
1970-01-01 06:36:20	Error	routed[2567]: Cannot log to -D: not under /var/log/
1970-01-01 06:36:20	Error	routed[2567]: adding route to nethost 192.168.1.0 through gateway 192.168.1.1: Cannot assign requested address
1970-01-01 06:36:23	Error	routed[2630]: Cannot log to -D: not under /var/log/
1970-01-01 06:36:23	Error	routed[2630]: adding route to nethost 192.168.1.0 through gateway 192.168.1.1: Cannot assign requested address
1970-01-01 06:39:11	Warning	kernel: wifiAccBlock 0 0 0 0 0 0 0 0
1970-01-01 06:39:12	Warning	kernel: wifiAccBlock 0 0 0 0 0 0 0 0
1970-01-01 06:39:12	Warning	kernel: wifiAccBlock 0 0 0 0 0 0 0 0
1970-01-01 06:39:12	Warning	kernel: wifiAccBlock 0 0 0 0 0 0 0 0
1970-01-01 06:39:12	Warning	kernel: wifiAccBlock 0 0 0 0 0 0 0 0
1970-01-01 06:40:40	Warning	kernel: Auto channel choose ch 8

1970-01-01 07:01:04	Error	dhcpd:
1970-01-01 07:01:04	Error	dhcpd: Not configured to listen on any interfaces!
1970-01-01 07:01:04	Error	dhcpd:
1970-01-01 07:01:04	Error	dhcpd: If you did not get this software from ftp.isc.org, please
1970-01-01 07:01:04	Error	dhcpd: get the latest from ftp.isc.org and install that before
1970-01-01 07:01:08	Warning	dnsmasq[3459]: ignoring nameserver ::1 - local interface
1970-01-01 07:01:08	Warning	dnsmasq[3459]: ignoring nameserver 127.0.0.1 - local interface
1970-01-01 07:01:08	Error	radvd[3438]: poll error: Interrupted system call
1970-01-01 07:01:08	Warning	radvd[3438]: received RA from fe80::217:7cff:feaa:69e
1970-01-01 07:01:25	Warning	radvd[3438]: received RA from fe80::217:7cff:feaa:69e

6. Log Generation 6: Reboot/shutdown/crash (Mandatory)

- After rebooting, DUT logs for same are not present in DUT.
 - i. **Action Performed:** Not Present.
 - ii. **Outcome of Event:** Not Present

1970-01-01 05:30:42	Warning	kernel: INITIAL VOIP MANAGER PROGRAM
1970-01-01 05:30:42	Warning	kernel: Inactive PIN_CS:
1970-01-01 05:30:42	Warning	kernel: aipc: (0193)aipc_module_voip_set_pcm_fs iO_MODE_EN=0x00012058
1970-01-01 05:30:42	Warning	kernel: aipc: (0468)aipc_module_voip_slc_reset_rtk_api Pull low GPIO 28
1970-01-01 05:30:42	Warning	kernel: aipc: (0477)aipc_module_voip_slc_reset_rtk_api Pull high GPIO 28
1970-01-01 05:30:42	Warning	kernel: aipc: (0468)aipc_module_voip_slc_reset_rtk_api Pull low GPIO 28
1970-01-01 05:30:42	Warning	kernel: aipc: (0477)aipc_module_voip_slc_reset_rtk_api Pull high GPIO 28
1970-01-01 05:30:42	Warning	kernel: *pSPICKD/IV(b8009008)-FF000000 pSPITCR(b8009010)=00201823 pSPITCALR(b800901c)=00000000
1970-01-01 05:30:43	Warning	kernel: FW dl OK
1970-01-01 05:30:43	Warning	kernel: TAPI init OK
1970-01-01 05:30:43	Warning	kernel: BBD dl OK
1970-01-01 05:30:43	Warning	kernel: ch0 line feed OK
1970-01-01 05:30:43	Warning	kernel: PCM IF CFG OK
1970-01-01 05:30:43	Warning	kernel: ch0 PCM CH CFG OK
1970-01-01 05:30:43	Warning	kernel: ch0 PCM CH enable OK
1970-01-01 05:31:54	Notice	systemd: eth0 2 down
1970-01-01 05:31:54	Warning	kernel: *[[32minitalize intel slic(0) dxt102 successfully
1970-01-01 05:31:54	Warning	kernel: *[[0m
1970-01-01 05:35:23	Warning	kernel: Auto channel choose ch 8
1970-01-01 05:40:24	Warning	kernel: Auto channel choose ch 8
1970-01-01 05:42:59	Notice	systemd: eth0 2 up

7. Log Generation 7: Interface status change (Mandatory)

- After changing interface status log is visible for same in DUT log.

- i. **Interface name and Type:** Present
- ii. **Status:** Present.
- iii. **Outcome of Event:** Not Present

1970-01-01 11:13:52	Notice	systemd: eth0.2 up
1970-01-01 11:15:27	Notice	systemd: eth0.2 down
1970-01-01 11:15:37	Notice	systemd: eth0.3 up
1970-01-01 11:15:59	Warning	kernel: Auto channel choose ch: 8
1970-01-01 11:16:01	Notice	systemd: eth0.3 down
1970-01-01 11:16:06	Notice	systemd: eth0.2 up

8. Log Generation 8: Change of group membership or accounts (Optional)

Note: The features Change of group membership or accounts are not available on this DUT.

9. Log Generation 9: Resetting Passwords (Optional)

- The tester found that a user with low privileges 'user' and a user with high privileges "admin" can change the password. But the DUT does not show the event in the log file.
 - i. **Username:** Not Present
 - ii. **account:** Not Present
 - iii. **Activity performed:** Not Present
 - iv. **Outcome of event:** Not Present
 - v. **Timestamp:** Not Present

1970-01-01 06:40:37	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 06:40:39	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 06:41:10	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 06:41:19	Informational	boa[960]: login successful for admin from : 192.168.1.2
1970-01-01 06:41:41	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 06:41:41	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 06:42:44	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 06:42:44	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 07:02:56	Warning	kernel: Auto channel choose ch: 8
1970-01-01 07:07:57	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:07:58	Warning	kernel: Auto channel choose ch: 8
1970-01-01 07:08:02	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:08:07	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:08:12	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:08:17	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:08:22	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:08:27	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:08:32	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:08:37	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:09:02	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses
1970-01-01 07:09:07	Informational	dnsmasq[2339]: read /var/tmp/hosts - 1 addresses

10. Log Generation 11: user Login (Mandatory)

- user identification details are present in DUT for login activity performed by user Admin.
 - i. **username:** Not Present
 - ii. **Administered account:** Not Present
 - iii. **Activity Performed:** Present
 - iv. **Outcome of Event:** Present
 - v. **Timestamp:** Present

192.168.1.1/mgm_log_view_access.asp					110%
1970-01-01 07:50:57	Warning		kernel: [EAPOLKeyRecvd 4761][wlan1]wlan1: 4-way nanosnake done		
1970-01-01 07:52:03	Notice		systemd: eth0.2 down		
1970-01-01 07:52:08	Notice		systemd: eth0.2 up		
1970-01-01 07:52:46	Notice		systemd: eth0.2 down		
1970-01-01 07:52:51	Notice		systemd: eth0.2 up		
1970-01-01 08:02:28	Informational		boa[960]: logout successful from ::ffff:192.168.1.2		
1970-01-01 08:02:34	Error		boa[960]: login error from ::ffff:192.168.1.2 for bad password		
1970-01-01 08:02:50	Informational		boa[960]: login successful for admin from ::ffff:192.168.1.2		
1970-01-01 08:03:03	Informational		udhcpd: sending ACK to 192.168.1.33		

11. Log Generation 14: Time Change (Mandatory)

- In this DUT Local time configuration feature is not available.
- The lowest privilege user “user” doesn’t have rights to make changes in DUTs time hence log is not generated for same.
- After changing time in DUT via administration privilege user “admin” log is not visible for same in DUT log.
 - i. **Old value of Time:** Present
 - ii. **New value of Time:** Not Present
 - iii. **Origin of attempt to change time:** Not Present
 - iv. **Outcome of Event:** Not Present
 - v. **Timestamp:** Not Present
 - vi. **user Identity:** Not Present

192.168.1.1/mgm_log_view_access.asp					
1970-01-01 06:30:37	Warning		kernel: Auto channel choose ch:8		
1970-01-01 06:35:38	Warning		kernel: Auto channel choose ch:8		
1970-01-01 06:39:52	Notice		systemd: eth0.3 down		
1970-01-01 06:39:55	Notice		systemd: eth0.3 up		
1970-01-01 06:40:38	Notice		systemd: eth0.3 down		
1970-01-01 06:40:40	Warning		kernel: Auto channel choose ch:9		
1970-01-01 06:40:41	Notice		systemd: eth0.3 up		
1970-01-01 06:42:15	Error		boa[897]: Error opening web/favicon.ico for ::ffff:192.168.1.2: No such file or directory		
1970-01-01 06:45:41	Warning		kernel: Auto channel choose ch:8		

12. Log Generation 16: Audit Changes (Mandatory)

- i. Timestamp: Present
- ii. Type of event (audit data deletion, audit data modification) : Present
- iii. Outcome of event (Success or failure, as applicable) : Not Present
- iv. Subject identity: Not Present
- v. user identity: Not Present
- vi. origin of attempt to change time (e.g. IP address) : Not Present
- vii. Details of data deleted or modified: Present

```
# echo 1971-04-01 01:47:39 [Warning] kernel:DUT Fake log? >> syslogd.txt
# cat syslogd.txt
Manufacturer:DIGISOL;
ProductClass:DG-GR6821AC;
SerialNumber:00177C-GPON00A9D06E;
IP:192.168.1.1;
HwVer:V4.2C1;
SwVer:V3.2.02-240516;

1970-01-01 09:27:34 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:32:35 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:37:37 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:42:38 [Warning] kernel: Auto channel choose ch:8
1970-01-01 09:47:39 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:52:40 [Warning] kernel: Auto channel choose ch:9
1970-01-01 09:54:32 [Warning] kernel: [SendEAPOL 3003][wlan1]4-1
1970-01-01 09:54:32 [Warning] kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
1970-01-01 09:54:36 [Warning] kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
1971-04-01 01:47:39 [Warning] kernel:DUT Fake log"
```

Timestamp	Level	Message
1970-01-01 09:27:34	Warning	kernel: Auto channel choose ch:9
1970-01-01 09:32:35	Warning	kernel: Auto channel choose ch:9
1970-01-01 09:37:37	Warning	kernel: Auto channel choose ch:9
1970-01-01 09:42:38	Warning	kernel: Auto channel choose ch:8
1970-01-01 09:47:39	Warning	kernel: Auto channel choose ch:9
1970-01-01 09:52:40	Warning	kernel: Auto channel choose ch:9
1970-01-01 09:54:32	Warning	kernel: [SendEAPOL 3003][wlan1]4-1
1970-01-01 09:54:32	Warning	kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
1970-01-01 09:54:36	Warning	kernel: [EAPOLKeyRecvd 4261][wlan1]4-2
1971-04-01 01:47:39	Warning	kernel: DUT Fake log
1970-01-01 09:59:42	Warning	kernel: Auto channel choose ch:9

11.2 Test Case Number: 2

11.2.1. **Test Case Name:** TC_SECURE_LOG_EXPORT

11.2.2. **Test Case Description:** DUT to have capability to log important Security events. The secure log export is present in DUT.

11.2.3. **Execution Steps:** Execution steps can be referred from TSTP of clause 5.2

11.2.4. **Evidence Provided:** Screenshots to be captured.

11.3 Test Case Number: 3

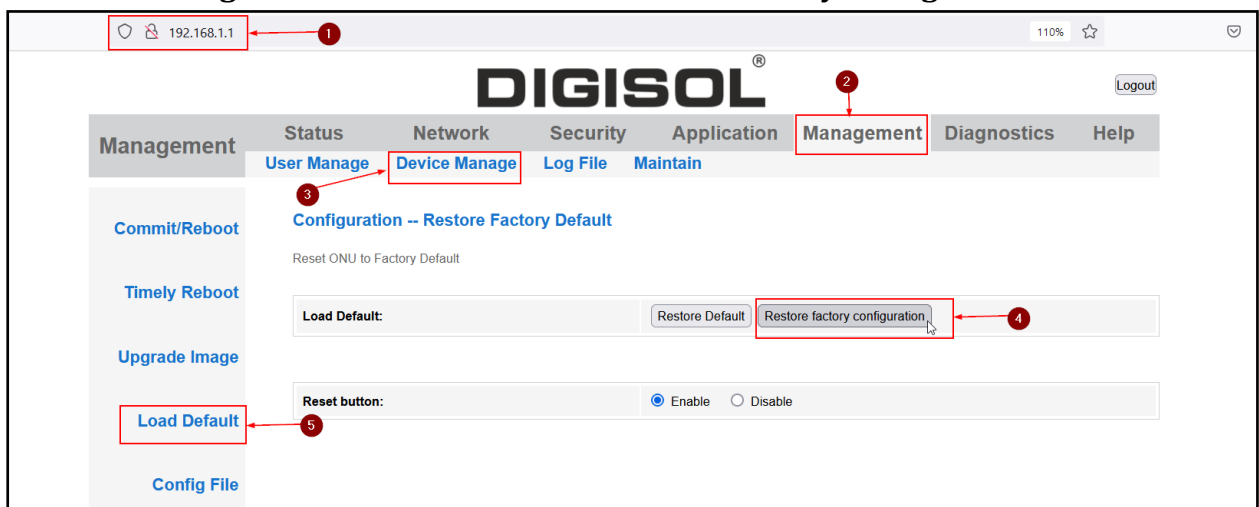
11.3.1. Test Case Name: TC_NON_VOLATILE MEMORY

11.3.2. Test Case Description: DUT to have capability to log important Security events. The audit logs preferably stored in Non-volatile memory.

11.3.3. Execution Steps:

A) Default logs storage to non-volatile memory.

- i. To reset DUT to its default configuration, navigate **management > Device manage > Load Default > click on Restore Factory Configuration**



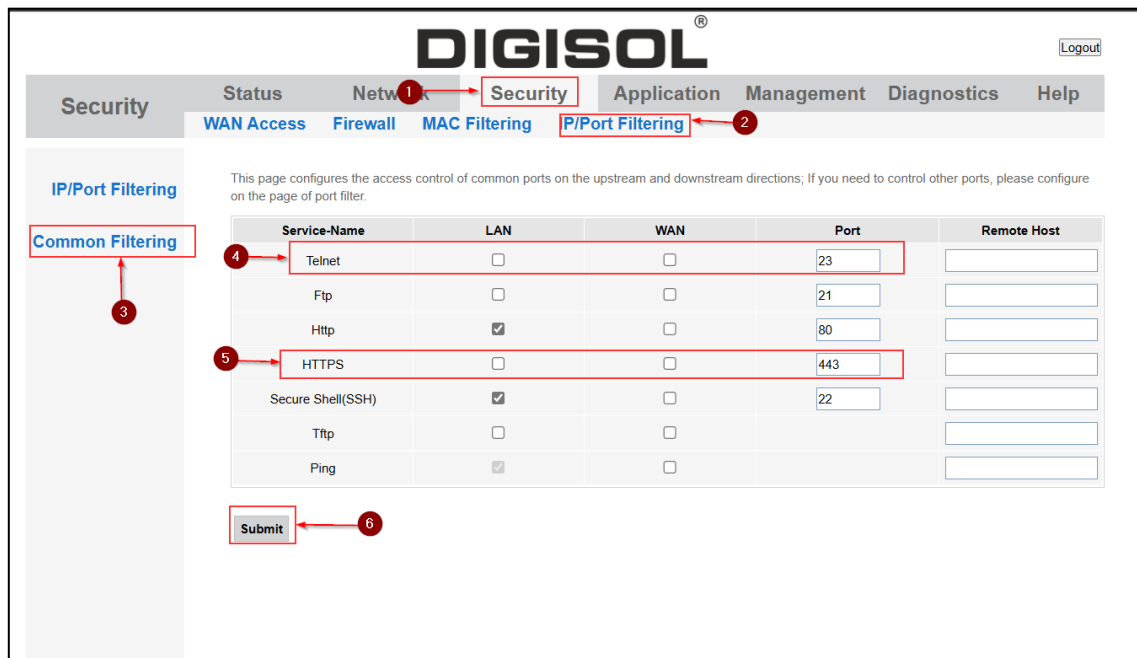
B) Resetting the DUT via High privilege user(admin).

- i. To log into the web interface of the ONT, open a web browser, and enter the default gateway address in the address bar.
- ii. To login through Administration Account, enter the username **admin** and password **"admin123"** in the login dialog box.
- iii. To check the current logs, navigate to **Management> Logs File> check the Logs info**



login to DUT via administrative access user “admin”

- iv. To Disable the services, navigate to **Security > IP/Port Filtering > Common Filtering**, disable Telnet, https service and check the log was generated for Telnet, https service disable



C) Disable the Telnet, Https service.

- i. Reboot the DUT.
- ii. To check the logs post reboot, Log into the Browser of the ONT, enter IP address in the address bar. To login through Administration Account, enter the username **admin** and password “**admin123**” in the login dialog box. Navigate to Logs and check the logs present post reboot
- iii. **Evidence Provided:**

D) Default logs storage to non-volatile memory.

- i. Logs before reboot.

192.168.1.1/mgm_log_view_access.asp		
1970-01-01 05:47:56	Error	boa[905]: Error opening web/help/share.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:57	Error	boa[905]: Error opening web/help/common.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:57	Error	boa[905]: Error opening web/help/share.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:57	Error	boa[905]: Error opening web/help/common.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:57	Error	boa[905]: Error opening web/help/share.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:58	Error	boa[905]: Error opening web/help/common.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:58	Error	boa[905]: Error opening web/help/share.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:59	Error	boa[905]: Error opening web/help/common.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:47:59	Error	boa[905]: Error opening web/help/share.js for :ffff:192.168.1.2: No such file or directory
1970-01-01 05:50:27	Warning	kernel: Auto channel choose ch.8
1970-01-01 05:55:28	Warning	kernel: Auto channel choose ch.8
1970-01-01 06:00:29	Warning	kernel: Auto channel choose ch.3

ii. DUT Logs after disable Telnet and https service.

192.168.1.1/mgm_log_view_access.asp		
1970-01-01 12:21:05	Debug	syslog: Debug: buildIVc: Interface br0 Addr: 192.168.1.1, Flags: 0x1043
1970-01-01 12:22:42	Informational	dnsmasq[3397]: read /var/tmp/hosts - 1 addresses
1970-01-01 12:22:42	Informational	dnsmasq[3397]: read /var/tmp/hosts - 1 addresses
1970-01-01 12:22:47	Informational	dnsmasq[3397]: read /var/tmp/hosts - 1 addresses
1970-01-01 12:22:47	Informational	dnsmasq[3397]: read /var/tmp/hosts - 1 addresses
1970-01-01 12:22:49	Notice	kernel: klogd started: BusyBox v1.22.1 (2022-11-28 14:44:46 CST)
1970-01-01 12:22:50	Debug	syslog: Debug: buildIVc: Interface br0 Addr: 192.168.1.1, Flags: 0x1043

iii. Logs after reboot.

1970-01-01 05:30:42	Warning	kernel: INITIAL VOIP MANAGER PROGRAM
1970-01-01 05:30:42	Warning	kernel: inactive PIN_CS
1970-01-01 05:30:42	Warning	kernel: aipc: (0193)aipc_module_voip_set_pcm_fs IO_MODE_EN=0x00012058
1970-01-01 05:30:42	Warning	kernel: aipc: (0468)aipc_module_voip_slc_reset_rtk_api Pull low GPIO 28
1970-01-01 05:30:42	Warning	kernel: aipc: (0477)aipc_module_voip_slc_reset_rtk_api Pull high GPIO 28
1970-01-01 05:30:42	Warning	kernel: aipc: (0468)aipc_module_voip_slc_reset_rtk_api Pull low GPIO 28
1970-01-01 05:30:42	Warning	kernel: aipc: (0477)aipc_module_voip_slc_reset_rtk_api Pull high GPIO 28
1970-01-01 05:30:42	Warning	kernel: "pSPICKDIV(b8009008)=FF000000 pSPITCR(b8009010)=00201823 pSPITCALR(b800901c)=00000000
1970-01-01 05:30:42	Warning	kernel: FW dl OK
1970-01-01 05:30:43	Warning	kernel: TAPI init OK
1970-01-01 05:30:43	Warning	kernel: BBD dl OK
1970-01-01 05:30:43	Warning	kernel: ch0 line feed OK
1970-01-01 05:30:43	Warning	kernel: PCM IF CFG OK
1970-01-01 05:30:43	Warning	kernel: ch0 PCM CH CFG OK
1970-01-01 05:30:43	Warning	kernel: ch0 PCM CH enable OK

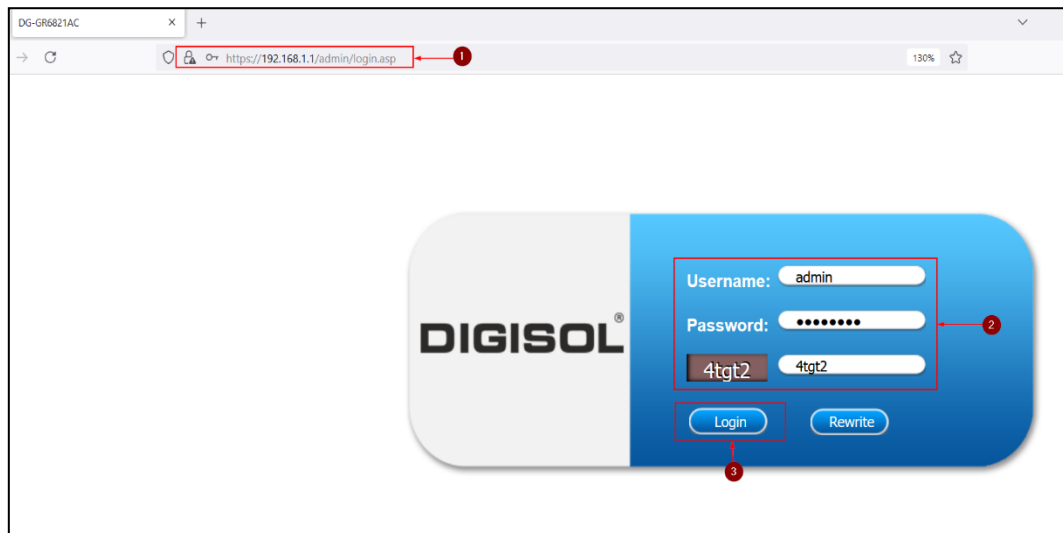
11.4 Test Case Number: 4

11.4.1 Test Case Name: TC_PRIVILEGE_USER_UNABLE_TO_DELETE_LOGS

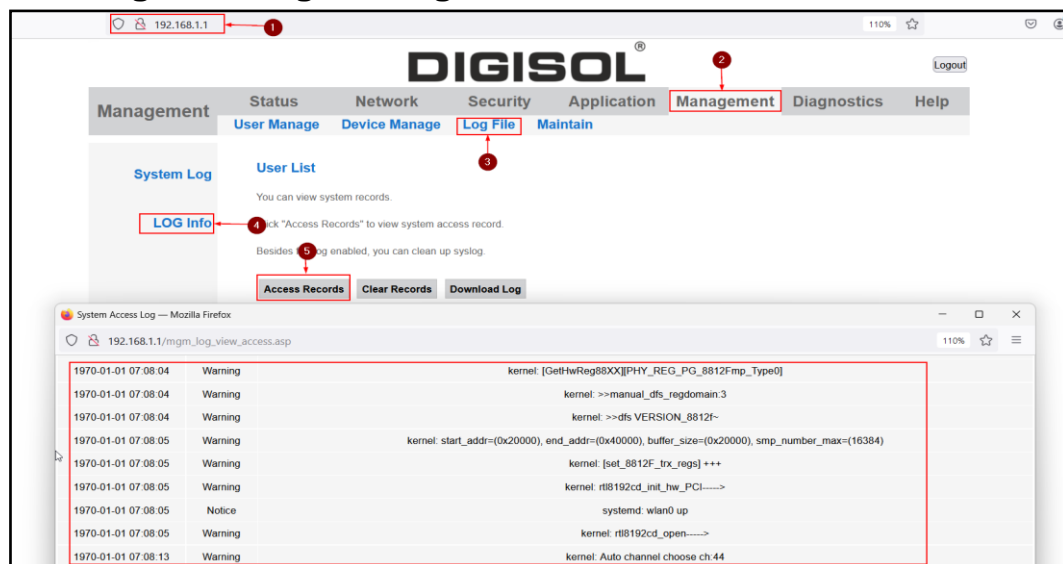
11.4.2 Test Case Description: To verify that the network product correctly logs all required security event types.

11.4.3 Execution Steps:

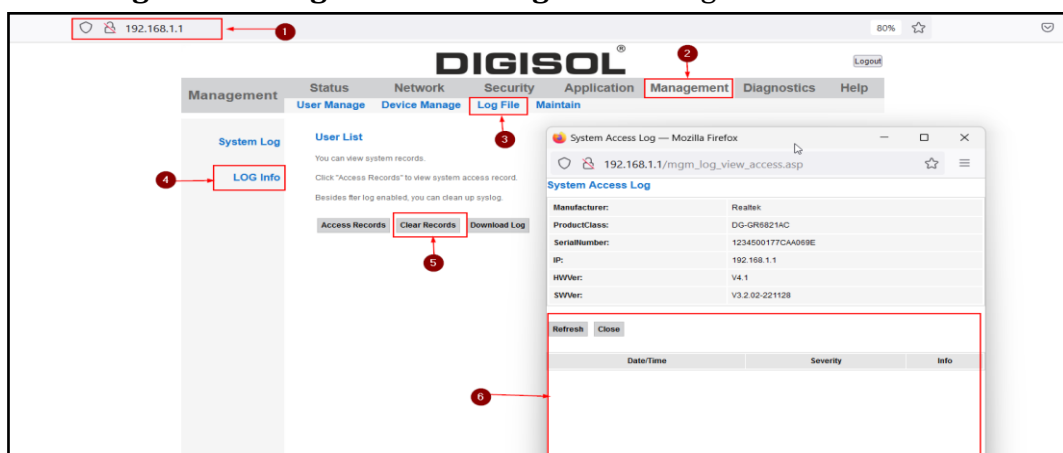
- To log into the web interface of the ONT, open a web browser and enter the default gateway address (**192.168.1.1**) in the address bar.
- To login through Administration Account, enter the username **admin** and password "**admin123**" in the login dialog box.



- iii. All types of logs generated in DUT are stored at a location called “log info” and administrative privilege user “admin” can access that location, **Navigate > Management > Log File > Log Info**

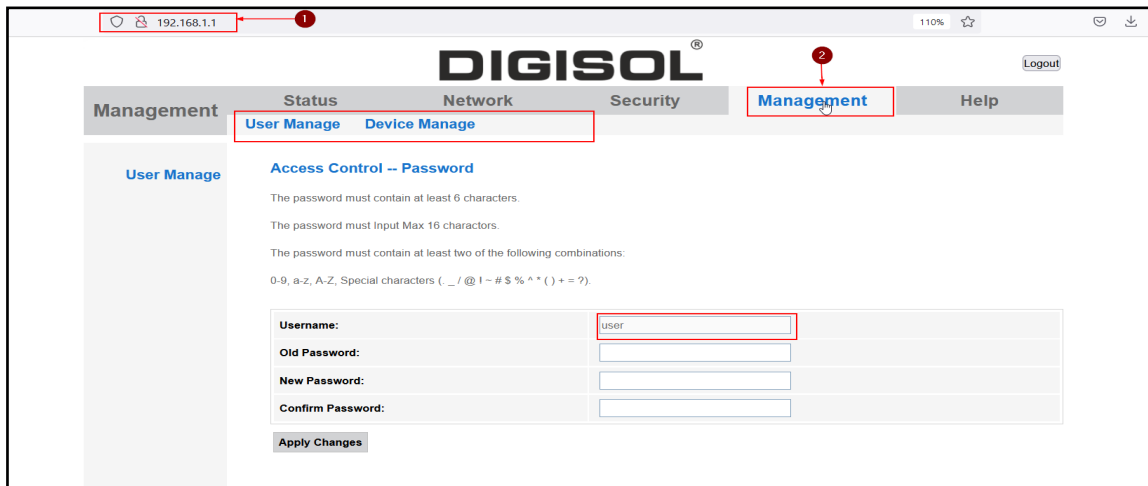


- iv. To verify that High privilege user is not able to delete the log, Navigate **Management > Log File > Clear log > Click “Log level**



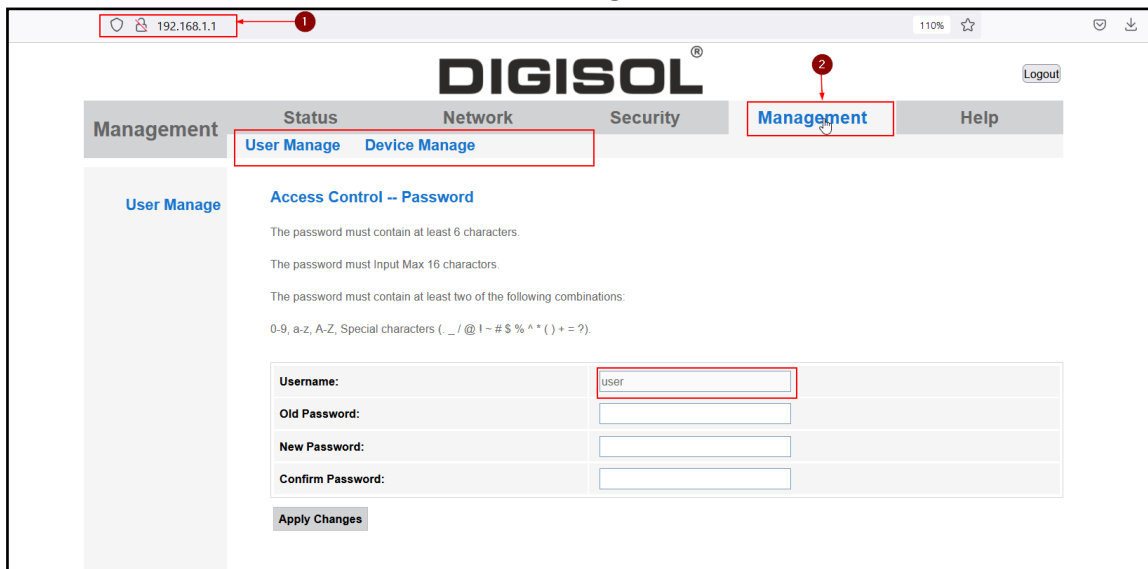
11.4.4 Evidence Provided:

- i. Logs before deletion.



Note: In This DUT Low level privilege user can't access Log File tab in Management.

11.5.4. **Evidence Provided:** In this DUT, a low-level privilege user cannot access the Log File tab under Management. This means users with the lowest privilege level are unable to read or delete logs."



12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_AUDIT_EVENT_GENERATION		
2	TC_SECURE_LOG_EXPORT		
3	TC_NON_VOLATILE MEMORY		
4	TC_PRIVILEGE_USER_UNABLE_TO_DELETE_LOGS		
5	TC_LOW_PRIVILEGE_USER_UNABLE_TO_DELETE_LOGS		

2.5.2 TSTP Evaluation for Secure Log Export.

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.5.2
--	--------------------------	-----------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS>

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

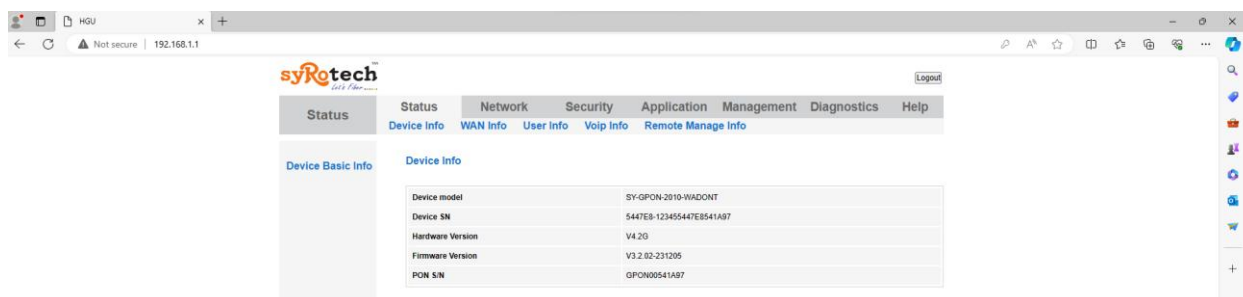
1. <ITSAR Section No & Name> Section 5 - User Audit

2. <Security Requirement No & Name > 2.5.2 Secure Log Export.

3. <Requirement Description: >

- i) (a)The ONT/ONU shall support forward of security event logging data to an external system by push or pull mechanism.
(b)Log functions should support secure uploading of log files to a central location.
- ii) ONT/ONU shall be able to store generated audit data itself, may be with limitations.
- iii) ONT/ONU shall alert administrator when its security log buffer reaches configured threshold limit.
- iv) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), ONT/ONU shall have mechanism to store audit data locally. ONT/ONU shall have sufficient memory (minimum 15 MB) allocated for this purpose. vendor to submit justification document for sufficiency of local storage requirement.
- v) Secure Log export shall comply the secure cryptographic controls as prescribed in Table 1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

4. DUT Confirmation Details:



Below Screenshot is IP address of DUT Test Machine:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\GRL MAS> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:db8::2
    Link-local IPv6 Address . . . . . : fe80::f15:48d0:ec20:8580%5
    IPv4 Address. . . . . : 192.168.1.22
    Subnet Mask . . . . . : 255.255.255.0
    IPv4 Address. . . . . : 192.168.3.1
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 2001:db8::1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::828b:589b:918f:89ec%15
    IPv4 Address. . . . . : 192.168.1.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f620:5e07:cb37:86aa%4
    IPv4 Address. . . . . : 192.168.100.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e92b:1eeb:17bc:293a%25
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1042:cb42:a604:410e%20
    IPv4 Address. . . . . : 169.254.19.174
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 6:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::be98:ec2f:d4cc:6198%2
    IPv4 Address. . . . . : 192.168.169.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Additionally, to ensure the connectivity between the DUT and the test machine, a ping test is conducted. This test verifies the ability to test machine to communicate with the DUT over the Ethernet connection by sending ICMP echo requests and receiving ICMP echo replies. A successful ping indicates that the network connection is established and functioning properly, enabling further testing and data transfer between the DUT and the test machine.

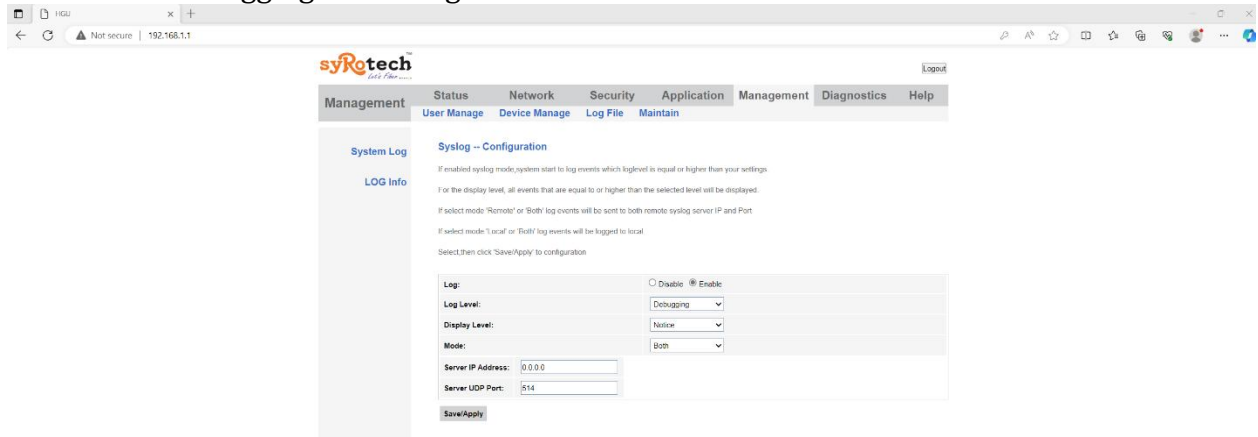
```
PS C:\Users\GRL MAS> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

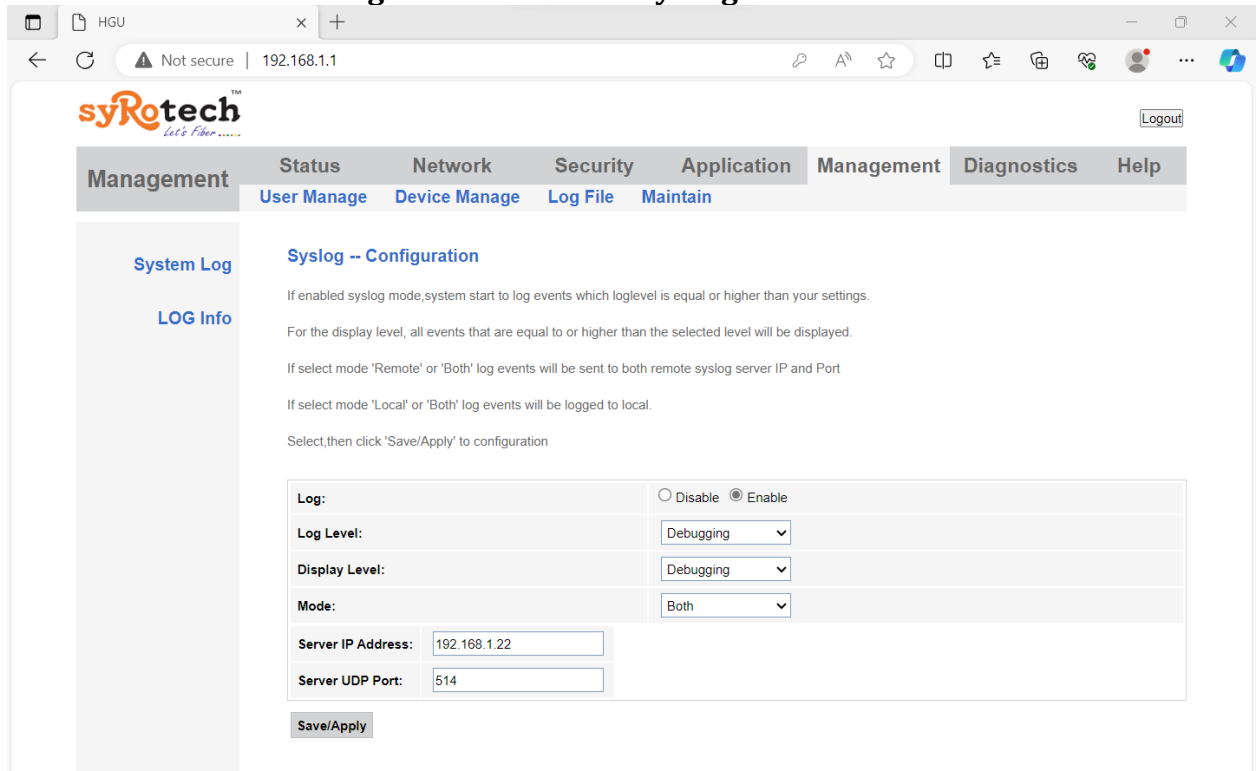
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\GRL MAS>
```

5. DUT Configuration:

- i. The tester accesses the DUT via web browser and navigate to management >> log file and enables logging and changes the mode to both local and remote



- ii. The tester then configures the external sys log



6. Preconditions:

- i. The manufacturer shall list the standard protocols which transfer security event logging data in the Vendor Documentation.
- ii. The Vendor must provide the documentation for the central location / external storage specifying the storage location for log files.
- iii. The session between network product and central location or external system for network product log functions has been set up.
- iv. The tester has privilege to operate network product and related logs can be outputted.
- v. The OEM should provide configuration file path along with the access parameters.

vi. The OEM should provide details about DUT's threshold alert mechanisms.

7. **Test Objective:** To verify that logs are securely transferred to the centralized storage

8. **Test Plan:**

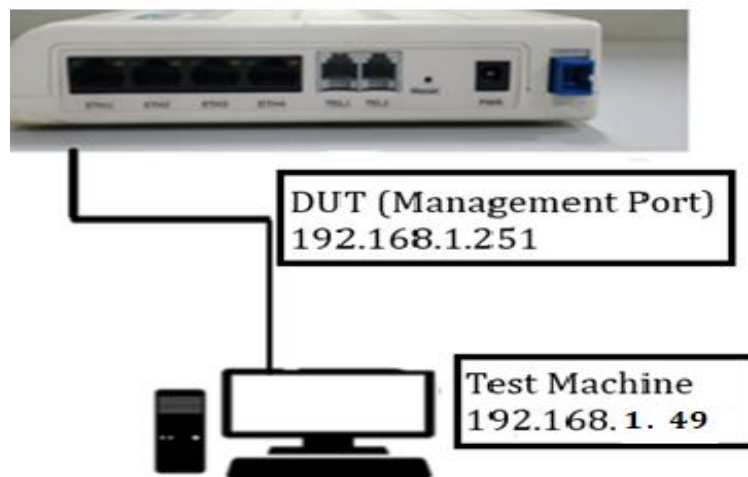
8.1 Number of Test Scenarios:

8.1.1 Test ensures secure log export

8.1.2 Storing the logs locally with sufficient memory

8.1.3 DUT sends alerts to sys admin

8.2 Test Setup Diagram:



8.3 Tools **Used:** Command Line, Wireshark

8.4 Test **Execution Steps:**

- i. The tester configures the network product to forward event logs to an external system (according to bullet a) of requirement) and related logs are sent out.
- ii. The tester checks whether the used transport protocol for log file upload is a secure standard protocol.
- iii. The tester checks whether the central location or external system for network product log functions has stored the related logs.
- iv. The tester configures the network product for secure upload of event log files to an external system (according to bullet b) of requirement) and performs a log file upload.
- v. The tester checks whether the central location or external system for network product log functions has stored the related logs.
- vi. The tester should check the mechanism to alert administrator when its security log buffer reaches configured threshold limit.
- vii. The tester should verify internal log storage mechanisms in case of absence of external systems.

9. **Expected Results to Pass:**

- i. The OEM listed transport protocols are secure protocols as per latest cryptographic

control ITSAR.

- ii. The used transport protocol for log file upload is a secure protocol as per latest cryptographic control ITSAR.
- iii. The DUT should store at least 15MB of security logs locally.
- iv. The central location/external system for network product should store the security related logs.
- v. The DUT alerts the administrator when the security log buffer reaches configured threshold limit.

10. **Expected Format of Evidence:** Screenshot, packet trace of evidence (pcap file)

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test case Name:** Forwarding of the security logs to external secure system.

11.1.2 **Test Case Description:** To verify that the DUT is forwarding security logs to an external secure system

11.1.3 Execution Steps:

- i. Tester triggers event of password changes and checks whether the log export is secure or not by capturing the packets in Wireshark.

syRotech™
Let's Fiber.....

Logout

Management Status Network Security Application Management Diagnostics Help

User Manage Device Manage Log File Maintain

User Manage

Access Control -- Password

The password must contain at least 6 characters.

The password must Input Max 32 characters.

The password must contain at least two of the following combinations:
0-9, a-z, A-Z, Special characters (. _ / @ ! ~ # \$ % ^ * () + = ?).

Username: admin

Old Password: *****

New Password: *****

Confirm Password: *****

Apply Changes

No.	Time	Source	Destination	Protocol	Length	Info
7516	2024-05-03 16:57:57.316700	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7517	2024-05-03 16:57:57.316654	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
7518	2024-05-03 16:57:59.242661	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7519	2024-05-03 16:57:59.242664	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
7520	2024-05-03 16:58:01.336584	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7521	2024-05-03 16:58:01.336661	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
7414	2024-05-03 16:58:03.346639	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7415	2024-05-03 16:58:03.346643	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
7479	2024-05-03 16:58:05.356398	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7471	2024-05-03 16:58:05.356368	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
7478	2024-05-03 16:58:06.149726	192.168.1.1	192.168.1.22	Syslog	95	DADMON.INFO: dnsmasq[5259]: read /var/tmp/hosts - 1 addresses
7479	2024-05-03 16:58:06.151680	192.168.1.1	192.168.1.22	Syslog	81	KERN.INFO: udhcpd: sending ACK to 192.168.1.33
7488	2024-05-03 16:58:06.154803	192.168.1.1	192.168.1.22	Syslog	95	DADMON.INFO: dnsmasq[5259]: read /var/tmp/hosts - 2 addresses
7487	2024-05-03 16:58:07.369912	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7488	2024-05-03 16:58:07.368845	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
7489	2024-05-03 16:58:09.376270	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7519	2024-05-03 16:58:09.378243	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
7516	2024-05-03 16:58:09.529821	192.168.1.1	192.168.1.22	Syslog	186	AUTHPRIV.INFO: boa[916]: useradmin password has been changed successfully
7517	2024-05-03 16:58:11.389271	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
7519	2024-05-03 16:58:11.389383	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
8080	2024-05-03 16:58:13.395588	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
8084	2024-05-03 16:58:13.398935	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
8024	2024-05-03 16:58:15.406239	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
8025	2024-05-03 16:58:15.408292	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
8044	2024-05-03 16:58:17.419328	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
8045	2024-05-03 16:58:17.419347	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
8061	2024-05-03 16:58:19.428005	192.168.1.1	192.168.1.22	Syslog	115	USER.DERBUG: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
8064	2024-05-03 16:58:19.428035	192.168.1.1	192.168.1.22	Syslog	118	USER.DERBUG: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
8091	2024-05-03 16:58:20.250497	192.168.1.1	192.168.1.22	Syslog	112	AUTHPRIV.ERR: boa[916]: login error from :ffff:192.168.1.22 for bad password
8109	2024-05-03 16:58:21.151030	192.168.1.1	192.168.1.22	Syslog	95	DADMON.INFO: dnsmasq[5259]: read /var/tmp/hosts - 1 addresses
8110	2024-05-03 16:58:21.151491	192.168.1.1	192.168.1.22	Syslog	95	DADMON.INFO: dnsmasq[5259]: read /var/tmp/hosts - 2 addresses

Frame 7516: 186 bytes on wire (848 bits), 186 bytes captured (848 bits) on Interface vDevice\NPF_{180B78C1-8322-4008-93F4-89049A34E0D4}, id 0
 Ethernet II, Src: SynchroNet_U5a:1a:97 (94:47:a8:54:1a:97), Dst: LCFElectron_4b:b5:fa (9c:2d:cd:4b:b5:fa)
 Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.22
 User Datagram Protocol, Src Port: 45000, Dst Port: 514
 Syslog message: AUTHPRIV.INFO: boa[916]: useradmin password has been changed successfully
 0081 0... = Facility: AUTHPRIV - security/authorization messages (private) (18)
 118 = Level: INFO - informational (63)
 Message: boa[916]: useradmin password has been changed successfully

Here, tester should verify if the ciphers used during log transfer to external system are compliant with Cryptographic Control ITSAR.

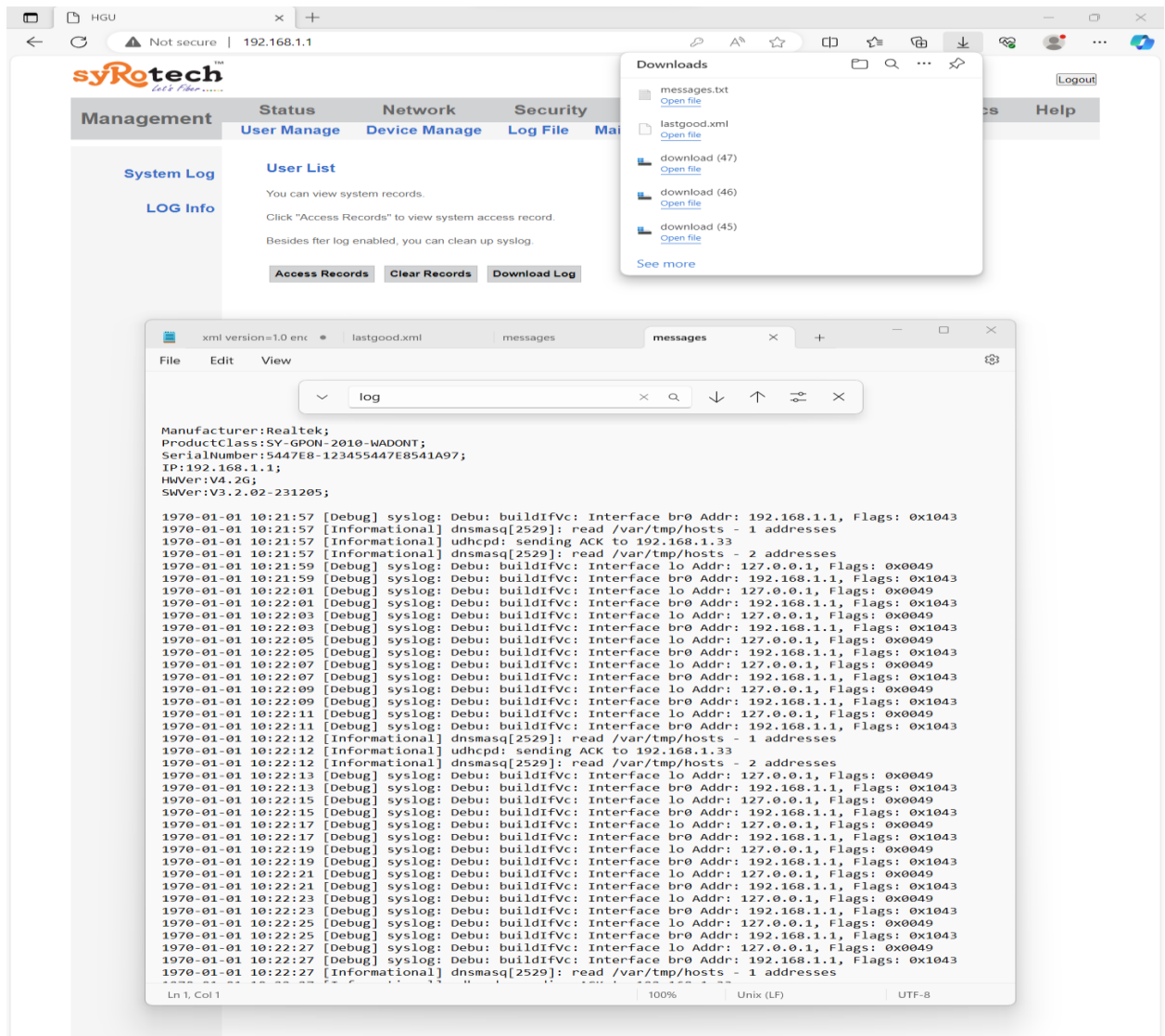
ii. Tester also confirms from the external syslog server.

No.	Priority	Facility	Date/Time	Source	RealSource	Logged Message
964	✓	DERBUG	USER	03-05-2024 17:04:32	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
965	✓	DERBUG	USER	03-05-2024 17:04:30	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
966	✓	DERBUG	USER	03-05-2024 17:04:30	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
967	✓	DERBUG	USER	03-05-2024 17:04:28	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
968	✓	DERBUG	USER	03-05-2024 17:04:28	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
979	✓	DERBUG	USER	03-05-2024 17:04:25	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
977	✓	DERBUG	USER	03-05-2024 17:04:25	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
976	✓	DERBUG	USER	03-05-2024 17:04:23	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
975	✓	DERBUG	USER	03-05-2024 17:04:23	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
974	✓	DERBUG	USER	03-05-2024 17:04:21	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
973	✓	INFO	DADMON	03-05-2024 17:04:21	192.168.1.1	MonitorView: dnsmasq[5259]: read /var/tmp/hosts - 2 addresses
972	✓	INFO	KERN	03-05-2024 17:04:21	192.168.1.1	MonitorView: udhcpd: sending ACK to 192.168.1.33
971	✓	INFO	DADMON	03-05-2024 17:04:21	192.168.1.1	MonitorView: dnsmasq[5259]: read /var/tmp/hosts - 1 addresses
970	✓	DERBUG	USER	03-05-2024 17:04:19	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
969	✓	DERBUG	USER	03-05-2024 17:04:19	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
968	✗	ERROR	USER	03-05-2024 17:04:15	192.168.1.1	MonitorView: boa[916]: login error from :ff:ff:ff:192.168.1.22 for bad password
967	✓	DERBUG	USER	03-05-2024 17:04:17	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
966	✓	DERBUG	USER	03-05-2024 17:04:17	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
965	✓	DERBUG	USER	03-05-2024 17:04:15	192.168.1.1	MonitorView: boa[916]: login error from :ff:ff:ff:192.168.1.22 for bad password
964	✓	DERBUG	USER	03-05-2024 17:04:15	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
963	✓	DERBUG	USER	03-05-2024 17:04:13	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
962	✓	DERBUG	USER	03-05-2024 17:04:13	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
961	✓	DERBUG	USER	03-05-2024 17:04:11	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
960	✓	DERBUG	USER	03-05-2024 17:04:11	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
959	✓	DERBUG	USER	03-05-2024 17:04:09	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
958	✓	DERBUG	USER	03-05-2024 17:04:09	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
957	✓	DERBUG	USER	03-05-2024 17:04:07	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
956	✓	DERBUG	USER	03-05-2024 17:04:07	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
954	✓	INFO	DADMON	03-05-2024 17:04:06	192.168.1.1	MonitorView: dnsmasq[5259]: read /var/tmp/hosts - 2 addresses
953	✓	INFO	KERN	03-05-2024 17:04:06	192.168.1.1	MonitorView: udhcpd: sending ACK to 192.168.1.33
952	✓	DERBUG	USER	03-05-2024 17:04:05	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
951	✓	DERBUG	USER	03-05-2024 17:04:05	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
950	✓	DERBUG	USER	03-05-2024 17:04:03	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
949	✓	DERBUG	USER	03-05-2024 17:04:03	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
948	✓	DERBUG	USER	03-05-2024 17:04:01	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
947	✓	DERBUG	USER	03-05-2024 17:04:01	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
946	✓	DERBUG	USER	03-05-2024 17:03:59	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843
945	✓	DERBUG	USER	03-05-2024 17:03:59	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface lo Addr: 127.0.0.1, Flags: 0x0049
944	✓	DERBUG	USER	03-05-2024 17:03:57	192.168.1.1	MonitorView: syslog: Debu: buildIPv: Interface br0 Addr: 192.168.1.1, Flags: 0x1843

Received Date & Time: 03-05-2024 17:04:15
 Facility: ERROR
 Priority: 3
 Source: 192.168.1.1
 RealSource: 192.168.1.1

iii. Uploading of log file to a central location securely

Securing Networks



The tester should verify if the log files can be uploaded from DUT to the central log server.

11.1.4 Test Observation:

- ONT is forwarding logging data to external system by push mechanism as all the logs are pushed to external syslog server.
- Logs pushed to external sys log server are not secure as it is using UDP and they are in plain text in transit.
- There is no functionality in the DUT to upload log files to a central location, it can be only downloaded to local test machine.

11.1.5 Evidence Provided: Screenshots of logs files and log configuration

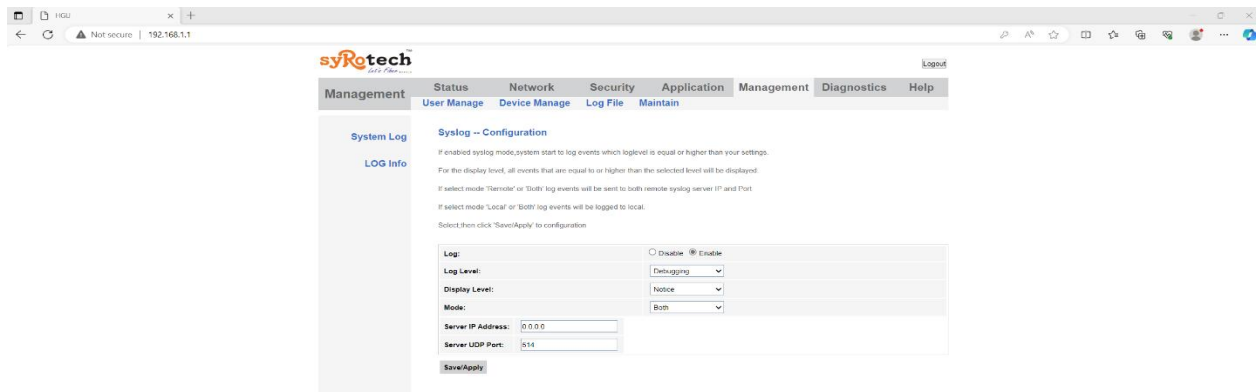
11.2 Test Case Number: 2

11.2.1. Test case Name: Storing the logs locally with sufficient memory

11.2.2. Test Case Description: Logs are stored locally and storage allocated is sufficient (15 mb min)

11.2.3. Execution Steps:

- The tester accesses the DUT via web browser and navigate to management >> log file



ii. Tester navigates to system logs and get access to system logs

System Access Log - Profile 1 - Microsoft Edge

System Access Log

Manufacturer:	Realtek
ProductClass:	SY-GPON-2010-WADONT
SerialNumber:	5447E8-123455447E8541A97
IP:	192.168.1.1
HWVer:	V4.2G
SWVer:	V3.2.02-231205

Refresh Close

Date/Time	Severity	Info
1970-01-01 10:05:42	Informational	dnsmasq[2529]: read /var/tmp/hosts - 2 addresses
1970-01-01 10:05:42	Informational	udhcpd: sending ACK to 192.168.1.33
1970-01-01 10:05:43	Debug	syslog: Debu: buildfVc: Interface lo Addr: 127.0.0.1, Flags: 0x0049
1970-01-01 10:05:43	Debug	syslog: Debu: buildfVc: Interface br0 Addr: 192.168.1.1, Flags: 0x1043
1970-01-01 10:05:45	Debug	syslog: Debu: buildfVc: Interface lo Addr: 127.0.0.1, Flags: 0x0049
1970-01-01 10:05:45	Debug	syslog: Debu: buildfVc: Interface br0 Addr: 192.168.1.1, Flags: 0x1043
1970-01-01 10:05:47	Debug	syslog: Debu: buildfVc: Interface lo Addr: 127.0.0.1, Flags: 0x0049
1970-01-01 10:05:47	Debug	syslog: Debu: buildfVc: Interface br0 Addr: 192.168.1.1, Flags: 0x1043
1970-01-01 10:05:49	Debug	syslog: Debu: buildfVc: Interface lo Addr: 127.0.0.1, Flags: 0x0049
1970-01-01 10:05:49	Debug	syslog: Debu: buildfVc: Interface br0 Addr: 192.168.1.1, Flags: 0x1043

iii. The tester should verify the configuration files and check the memory allocation for logs.

➤ NOTE: The path to configuration file and access parameter should be provided by the OEM.

```

<value Name= MIB_IP_ALG_TFTP Value= 1 />
<Value Name="MIB_IP_ALG_FTP" Value="1"/>
<Value Name="MIB_CTC_ACCOUNT_ENABLE" Value="1"/>
<Value Name="WLAN_VAP3_ITF_GROUP" Value="0"/>
<Value Name="WLAN_VAP2_ITF_GROUP" Value="0"/>
<Value Name="WLAN_VAP1_ITF_GROUP" Value="0"/>
<Value Name="WLAN_VAP0_ITF_GROUP" Value="0"/>
<Value Name="LAN_DHCP_GATEWAY" Value="192.168.1.1"/>
<Value Name="WSC_VERSION" Value="1"/>
<Value Name="WSC_CONFIGBYEXTREG" Value="0"/>
<Value Name="WSC_SSID" Value=""/>
<Value Name="WSC_PSK" Value="12345678"/>
<Value Name="WSC_REGISTRAR_ENABLED" Value="0"/>
<Value Name="WSC_UPNP_ENABLED" Value="1"/>
<Value Name="WSC_MANUAL_ENABLED" Value="1"/>
<Value Name="WSC_ENC" Value="12"/>
<Value Name="WSC_AUTH" Value="34"/>
<Value Name="WSC_PIN" Value="52193590"/>
<Value Name="WSC_CONFIGURED" Value="1"/>
<Value Name="WSC_METHOD" Value="3"/>
<Value Name="WSC_DISABLE" Value="0"/>
<Value Name="DOS_ENABLED" Value="1"/>
<Value Name="MIB_WLAN_MAC_CTRL" Value="0"/>
<Value Name="MIB_ETH_MAC_CTRL" Value="0"/>
<Value Name="MAXLOGLEN" Value="51200"/>
<Value Name="SYSLOG" Value="1"/>
<Value Name="CWMP_CT_SERVICE_TRUSTHOST" Value=""/>
<Value Name="CWMP_FIRMWARE_UPGRADE_MODE" Value="0"/>
<Value Name="CWMP_DELAY_RESTARTWAN_CHECK_TIME" Value="15"/>
<Value Name="CWMP_DELAY_RESTARTWAN_ENABLE" Value="1"/>
<Value Name="CWMP_CT_IP_FORWARD_MODE_ENABLED" Value="0"/>
<Value Name="CWMP_CT_QOE_PORT" Value="8000"/>
<Value Name="CWMP_CT_QOE_TESTDOWNLOADURL" Value="gz.gdqoe.ct"/>
<Value Name="CWMP_CT_QOE_ENABLE" Value="0"/>
<Value Name="TR111_NATDETECTED" Value="0"/>
<Value Name="TR111_STUNPASSWORD" Value=""/>
<Value Name="TR111_STUNUSERNAME" Value=""/>
<Value Name="TR111_STUNMINIMUMKEEPALIVEPERIOD" Value="20"/>
<Value Name="TR111_STUNMAXIMUMKEEPALIVEPERIOD" Value="60"/>
<Value Name="TR111_STUNSERVERPORT" Value="3478"/>
<Value Name="TR111_STUNSERVERADDR" Value=""/>
<Value Name="TR111_STUNENABLE" Value="0"/>
<Value Name="TR111_UDPCONNREQADDR" Value="9.9.9.9:7547"/>
<Value Name="CWMP_CONFIGURABLE" Value="7"/>
<Value Name="CWMP_WAN_INTERFACE" Value="65535"/>
<Value Name="CWMP_PERSISTENT_DATA" Value=""/>
<Value Name="CWMP_CT_PING_ENABLE" Value="0"/>
<Value Name="CWMP_USERINFO_PROVISIONINGCODE" Value=""/>
<Value Name="CWMP_USERINFO_PROV_NAME" Value=""/>

```

11.2.4. Test Observation:

- i. Tester observed that DUT is storing the logs locally.
- ii. There is no information about the logs file size, OEM support may be required to get the information about the storage.
- iii. As per the running configuration max log length is mention as 51200, OEM may provide more information on this.

11.2.5. Evidence Provided: Screenshots of logs files and log configuration

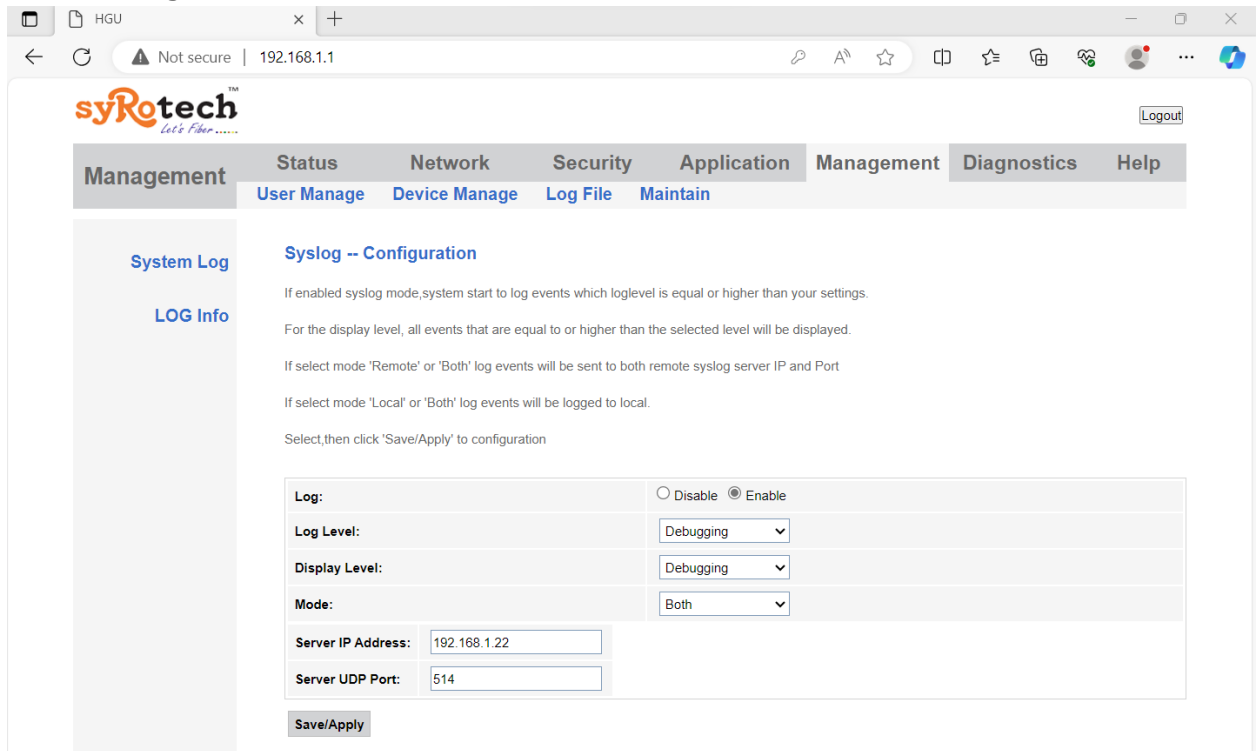
11.3 Test Case Number: 3

11.3.1. **Test case Name:** DUT sends alerts to sys admin

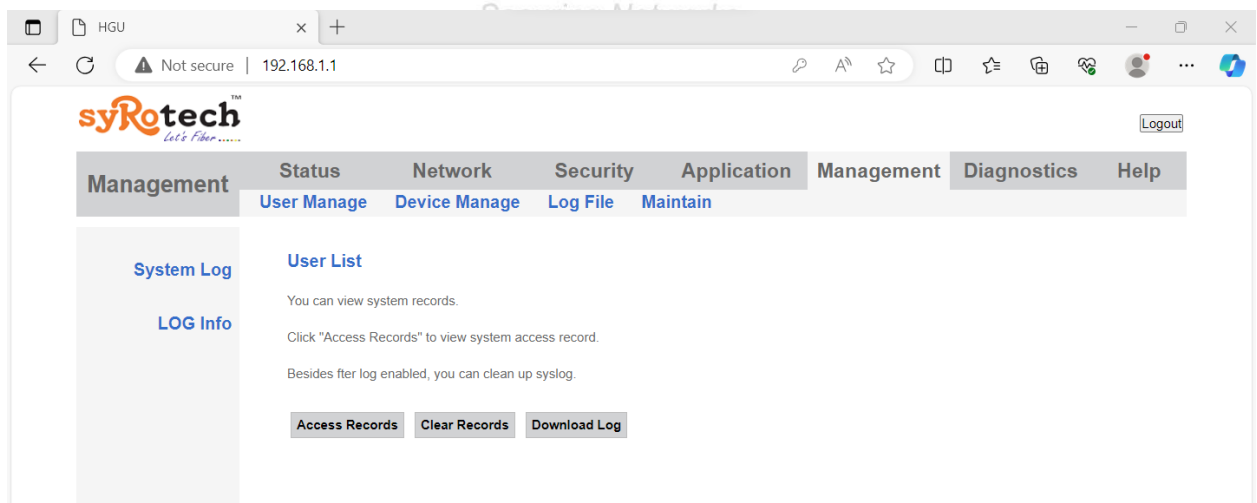
11.3.2. **Test Case Description:** To verify that the DUT is triggering alarm when logs storage reaches to threshold.

11.3.3. Execution Steps:

- i. The tester accesses the DUT via web browser and navigate to management >> logs files.



- ii. Tester looks for the option to configure alarms and alerts for sys admin or network admin.



11.3.4. **Test Observation:** DUT is not having any option to configure the alerts and alarms when logs are full and it's not generating any alarm or alert.

11.3.5. **Evidence Provided:** Screenshots of logs files and log configuration

12. Test Results:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Forwarding of the security logs to external secure system		
2	Storing the logs locally with sufficient memory		
3	DUT sends alerts to sys admin		



2.6.1 TSTP for Evaluation of Cryptographic Based Secure Communication with connecting entities

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.6.1
--	--------------------------	-----------------

Applicant Name: **Tejas**

Application Number: **GE-BE-1103240001**

DUT Details: ONT

DUT Software Version:2.3.4.50B

Digest Hash of OS: Hash of DUT OS is required

Digest Hash of Configuration: Hash of DUT configuration is required

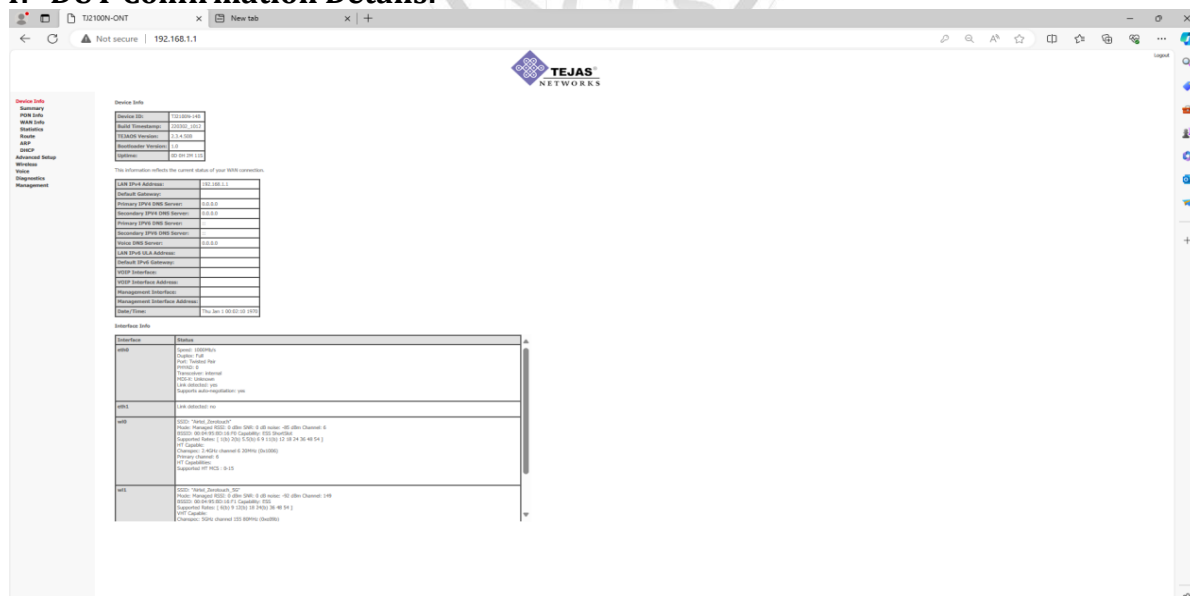
Applicable ITSAR: ONT ITSAR403012311

ITSAR Version No: 1.0.1

OEM Supplied Document list: NA

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No &Name>**2.6.1: Cryptographic Based Secure Communication with connecting entities
3. **Requirement Description:** ONU/ONT shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

4. DUT Confirmation Details:



5. DUT Configuration:

- i.** Configure the DUT for the supported management protocols
- ii.** Configure the DUT for control plane communication with any other connected entity (eg: OLT)

6. **Pre-Condition:** OEM shall provide detail of cryptographic algorithms used by DUT for communication between the CPE and connected entities.

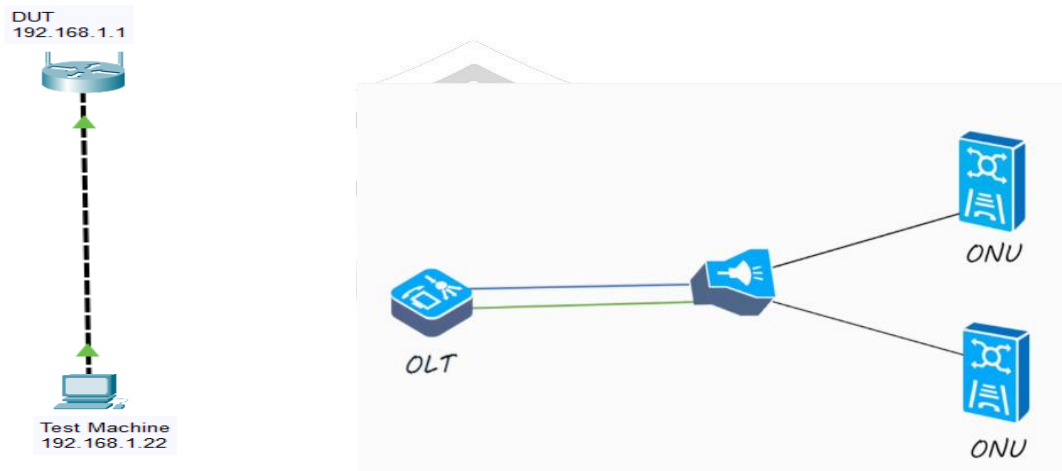
7. **Test Objective:** To verify that the DUT communicates with connected entities with secure ciphers in accordance to crypto control ITSAR

8. Test Plan

8.1 Number of Test Scenarios:

- 8.1.1 OEM documentation review
- 8.1.2 Secure communication verification
- 8.1.3 Control plane communication verification
- 8.1.4 /+

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: Wireshark

9. **Expected Results for Pass:** DUT communicates with connected entities with secure ciphers in accordance to crypto control ITSAR

10. **Expected Format of Evidence:** Screenshots

11. Test Execution:

- i. Review the OEM documentation to check for the supported connected entities and the protocol with which it communicates with
- ii. Attempt to connect with each entity and capture the same on Wireshark
- iii. Analyze the packets and verify the ciphers used in the communication

11.1 Test Case Number: 01

11.1.1 **Test case Name:** Review the OEM documentation.

11.1.2 **Test Case Description:** Check the OEM document describing the secure communication services/protocols supported on the DUT, details of Crypto modules used, Cryptographic protocols and algorithms, command to verify the related configuration in the DUT.

11.1.3 **Execution Steps:**

- i. Review the OEM documentation to check for the supported connected entities and the protocol with which it communicates with
- ii. Attempt to connect with each entity and capture the same on wireshark

11.1.4 Test Observations: Check the OEM document describing the secure communication services/protocols supported on the DUT, details of Crypto modules used, Cryptographic protocols and algorithms, command to verify the related configuration in the DUT.

11.1.5 Evidence Provided: -NA-

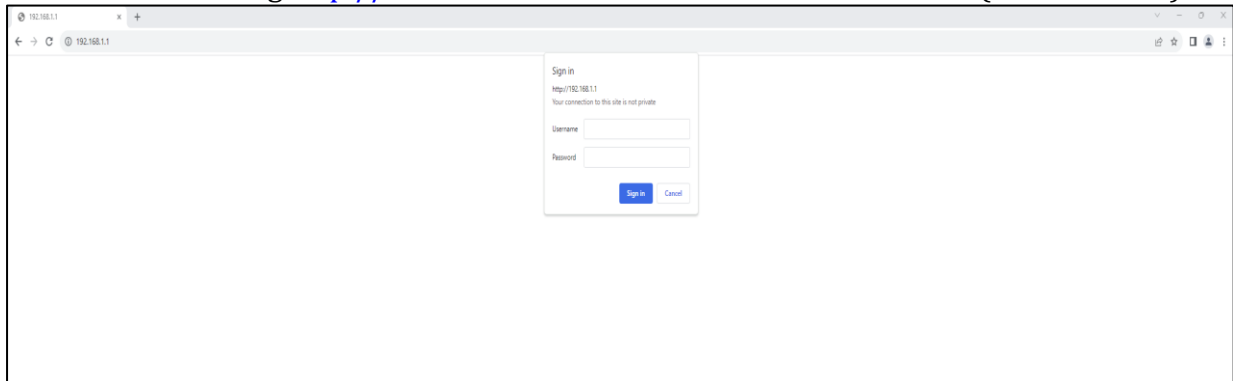
11.2 Test Case Number: 02

11.2.1 Test case Name: Secure cipher communication (1)

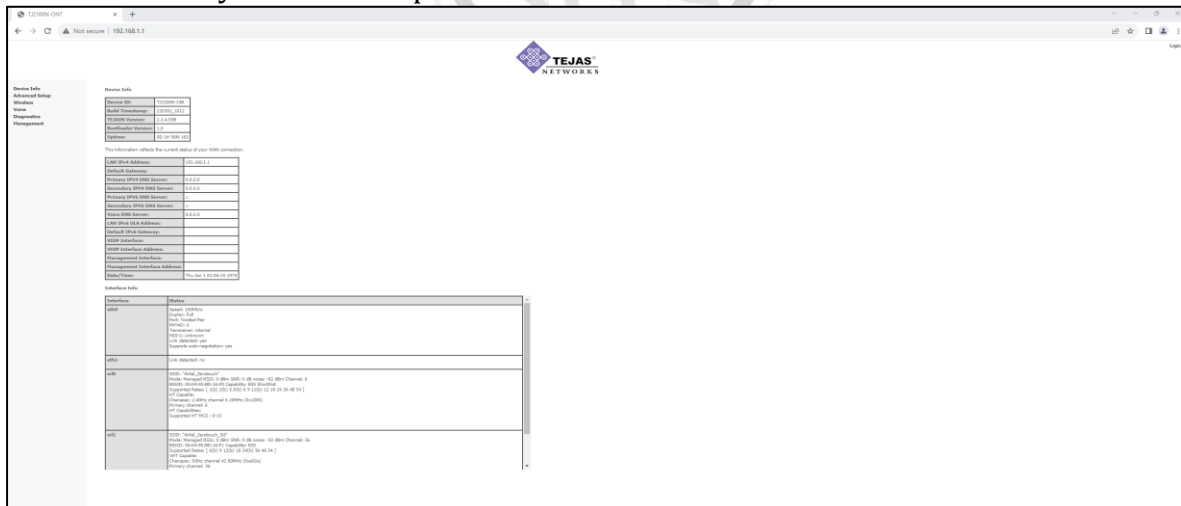
11.2.2 Test Case Description: The Tester shall check the DUT specifications and the cryptographic protocols it uses for communication.

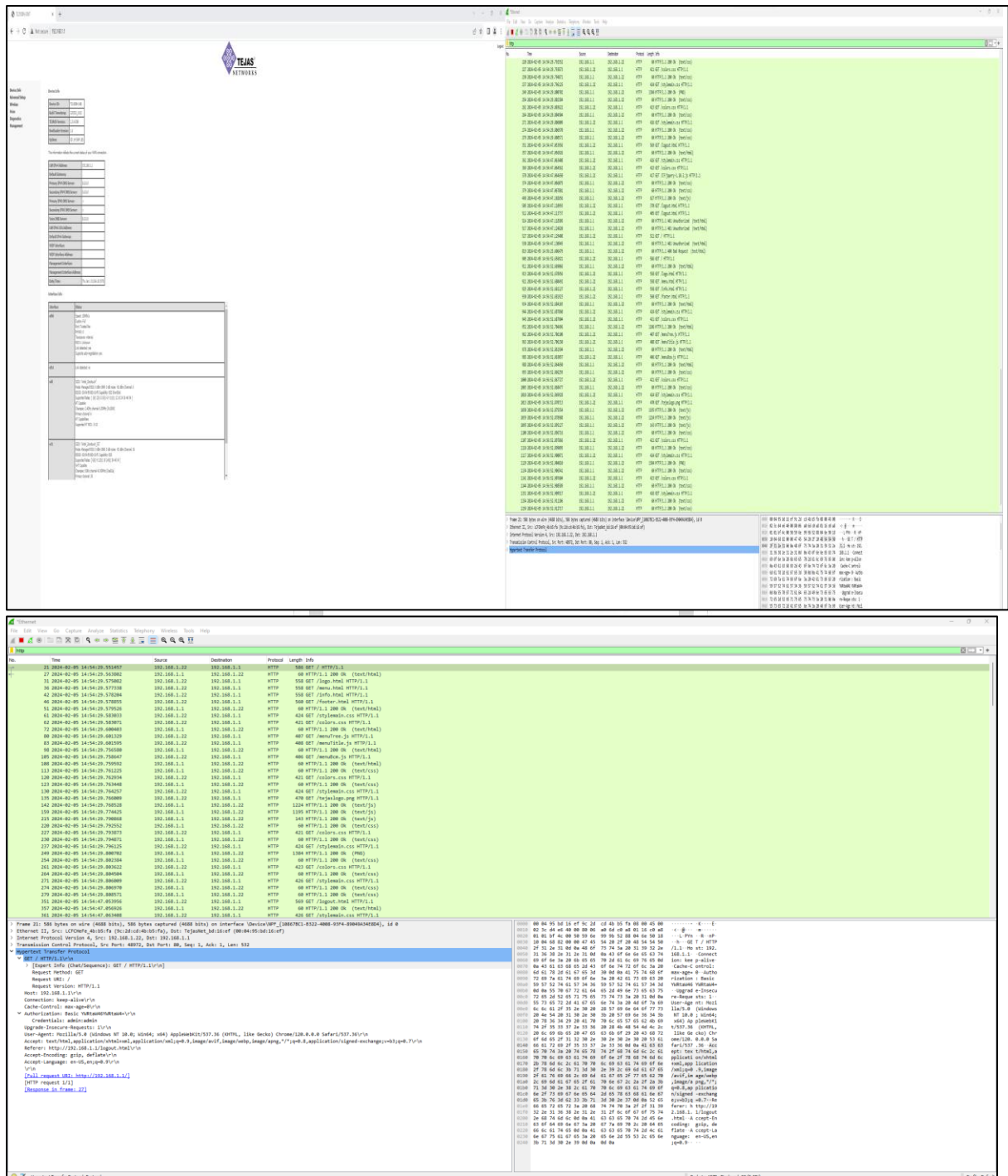
11.2.3 Execution Steps: DUT only support HTTP for communication.

- i. The Tester connects the DUT through LAN port and access HTTP using following <http://192.168.1.1> in browser of the test machine (192.168.1.22).



- ii. The Tester captured traffic between DUT and test machine in Wireshark to verify the secure ciphers used in the communication





a. Testssl

- i. The Tester install testssl from this url <https://github.com/drwetter/testssl.sh.git> on Kali Linux (test machine1) to verify ciphers on DUT.
- ii. The Tester used this command `./testssl.sh 192.168.1.1` and observed that DUT is not supporting any cipher.
- iii. The Tester observed that DUT did not use any ciphers for secure communication


```

(kali@kali):~/testssl.sh
$ ./testssl.sh 192.168.1.1:80

#####
testssl.sh      3.2rc3 from https://testssl.sh/dev/
(1a9a486 2023-11-10 19:41:08)

This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/

#####

Using "OpenSSL 1.0.2-bad (1.0.2k-dev)" [~183 ciphers]
on Kali: "/bin/openssl.Linux.x86_64"
(built: "Sep 14:03:44 2022", platform: "linux-x86_64")

Start 2024-02-05 02:41:05      --> 192.168.1.1:80 (192.168.1.1) <--

rDNS (192.168.1.1):      --

192.168.1.1:80 doesn't seem to be a TLS/SSL enabled server
The results might look ok but they could be nonsense. Really proceed ? ("yes" to continue) --> yes
Service detected:      Couldn't determine what's running on port 80, assuming no HTTP service => skipping all HTTP checks

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    not offered
TLS 1.3    not offered

You should not proceed as no protocol was detected. If you still really really want to, say "YES" --> YES

NPN/SPDY   not offered
ALPN/HTTP2 not offered

Testing cipher categories

NULL ciphers (no encryption)      not offered (OK)
Anonymous NULL ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)      not offered (OK)
LOW: 64 bit + DES, RC2,4, MD5 (w/o export) not offered (OK)
Triple DES Ciphers / IDEA         not offered
Obsoleted CBC ciphers (AES, ARIA etc.) not offered
Strong encryption (AEAD ciphers) with no FS      not offered
Forward Secrecy strong encryption (AEAD ciphers) not offered

Testing server's cipher preferences

Handshake error/Hexcode  Cipher Suite Name (OpenSSL)      KeyExch.  Encryption  Bits      Cipher Suite Name (IANA/RFC)

SSLv2
-
SSLv3
-
TLSv1
-
TLSv1.1
-
TLSv1.2
-
TLSv1.3
-

Has server cipher order?      unable to determine

```

```

Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES, RC4

No ciphers supporting Forward Secrecy (FS) offered

Testing server defaults (Server Hello)

TLS extensions (standard)      (none)
Session Ticket RFC 5077 hint   no -- no lifetime advertised
SSL Session ID support         no      Tickets no, ID: no
Session Resumption              no
TLS clock skew                  SSLv3 through TLS 1.2 didn't return a timestamp
Client Authentication           none

Client problem: No server certificate could be retrieved. Thus we can't continue with "server defaults".

Testing vulnerabilities

Heartbleed (CVE-2014-0160)      not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)             not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment. (applicable only for HTTPS)
ROBOT                            Server does not support any cipher suites that use RSA key transport
Secure Renegotiation (RFC 5746) OpenSSL handshake didn't succeed
Secure Client-Initiated Renegotiation not vulnerable (OK)
CRIME, TLS (CVE-2012-4929)       test failed (couldn't connect)
POODLE_SSL (CVE-2014-3566)       not vulnerable (OK), no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)    No fallback possible (OK), no protocol below TLS 1.2 offered
SWEET32 (CVE-2016-2183, CVE-2016-6329) not vulnerable (OK)
FREAK (CVE-2015-0284)            not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703) not vulnerable on this host and port (OK)
LOGJAM (CVE-2015-4000), experimental no RSA certificate, thus certificate can't be used with SSLv2 elsewhere
BEAST (CVE-2011-3389)            not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
LUCKY13 (CVE-2013-0169), experimental not vulnerable (OK), no SSL3 or TLS1
Winshock (CVE-2014-6321), experimental not vulnerable (OK) - no HTTP or RDP
RC4 (CVE-2013-2566, CVE-2015-2808) no RC4 ciphers detected (OK)

Could not determine the protocol, only simulating generic clients.

Running client simulations via sockets

Browser      Protocol  Cipher Suite Name (OpenSSL)      Forward Secrecy

Android 6.0      No connection
Android 7.0 (native) No connection
Android 8.1 (native) No connection
Android 9.0 (native) No connection
Android 10.0 (native) No connection
Android 11 (native) No connection
Android 12 (native) No connection
Chrome 79 (Win 10) No connection
Chrome 101 (Win 10) No connection
Firefox 66 (Win 8.1/10) No connection
Firefox 100 (Win 10) No connection
IE 6 XP         No connection
IE 8 Win 7      No connection
IE 8 XP         No connection
IE 11 Win 7     No connection
IE 11 Win 8.1   No connection
IE 11 Win Phone 8.1 No connection
IE 11 Win 10    No connection
Edge 15 Win 10  No connection
Edge 101 Win 10 21H2 No connection
Safari 12.1 (iOS 12.2) No connection
Safari 13.0 (macOS 10.14.6) No connection
Safari 15.4 (macOS 12.3.1) No connection
Java 7u25        No connection
Java 8u161       No connection
Java 11.0.2 (OpenJDK) No connection
Java 17.0.3 (OpenJDK) No connection
go 1.17.8        No connection
LibreSSL 2.8.3 (Apple) No connection

```

```

OpenSSL 1.0.2e                No connection
OpenSSL 1.1.0l (Debian)      No connection
OpenSSL 1.1.1d (Debian)      No connection
OpenSSL 3.0.3 (git)          No connection
Apple Mail (16.0)            No connection
Thunderbird (91.9)           No connection

Rating (experimental)
Rating specs (not complete)   SSL Labs's 'SSL Server Rating Guide' (version 2009g from 2020-01-30)
Specification documentation   https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted)    100 (30)
Key Exchange (weighted)       100 (30)
Cipher Strength (weighted)     60 (24)
Final Score                   84
Overall Grade                  C
Grade cap reasons              Grade capped to C. TLS 1.2 or TLS 1.3 are not offered
                              Grade capped to B. Forward Secrecy (FS) is not supported

Done 2024-02-05 04:01:38 [4836s] —> 192.168.1.1:80 (192.168.1.1) <—

(kali@kali)~[~/testssl.sh]

```

iv. The Tester observed the communication between Web client and Web server is not protected using industry standard secured communication protocols such as TLS/HTTPS.

11.2.4 Test Observation: Tester verified no secure communication mechanism between the Network product and the connected entities. Not using industry standard and NIST recommended cryptographic protocols.

11.2.5 Evidence Provided: Screenshots are attached above

11.3 Test Case Number: 03

11.3.1 Test case Name: Secure ciphers to be used (2)

11.3.2 Test Case Description: The Tester shall capture the communication between the DUT and OLT to check for secure ciphers

- **Note :** Due to unavailability of OLT the following executions steps have been given on generalized manner for reference purpose

11.3.3 Execution Steps:

- Trigger the communication between ONT and OLT and simultaneously capture the same on wireshark.
- Expected control plane communication : OMCI (ONT Management and Control Interface)

11.3.4 Test Observations: NA

11.3.5 Evidence Provided: NA

12) Test Case Result:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the OEM documentation		
2	Secure ciphers used 1		
3	Secure ciphers to be used 2		

2.6.2 TSTP for Evaluation of Cryptographic Module Security Assurance

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR ITSAR403012311	No:	Clause no:2.6.2
---	-------------------------	-----	-----------------

Applicant Name: Tejas

Application Number: GE-BE-1103240001

DUT Details: ONT

DUT Software Version:2.3.4.50B

Digest Hash of OS: Hash of DUT OS is required

Digest Hash of Configuration: Hash of DUT configuration is required

Applicable ITSAR: ONT ITSAR403012311

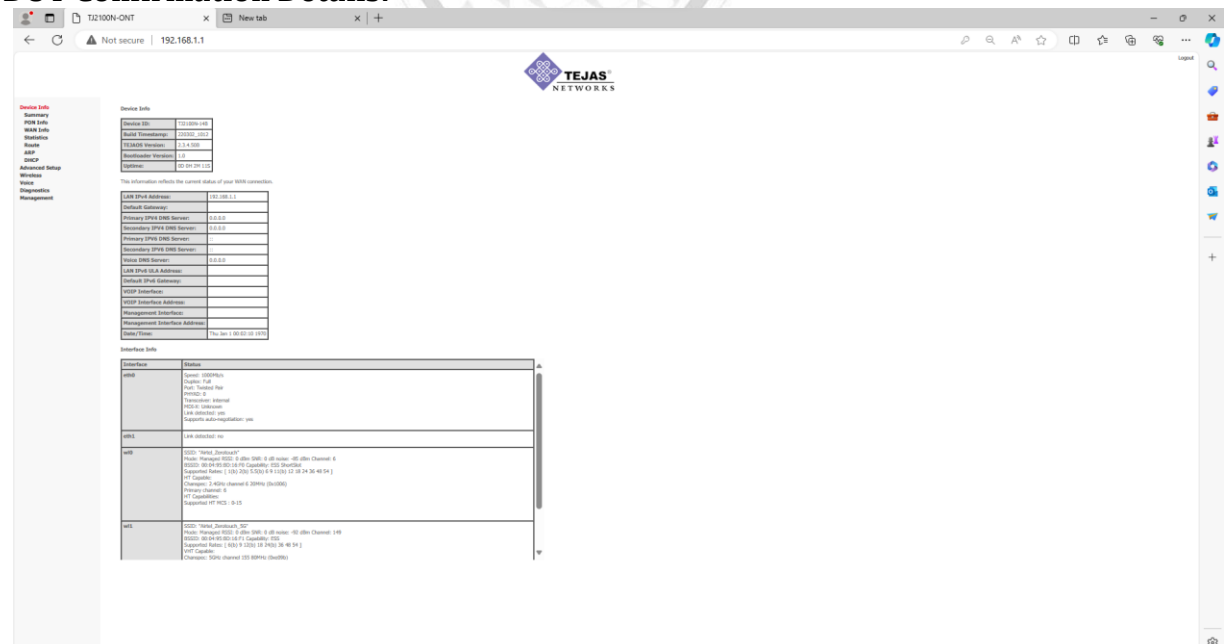
ITSAR Version No: 1.0.1

OEM Supplied Document list: NA

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No &Name>**1.6.2: Cryptographic Based Secure Communication on WiFi Access
3. **Requirement Description:** An undertaking is to be submitted by the vendor mentioning that “Cryptographic module embedded inside the ONU/ONT (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.”

Vendor shall submit cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.

6. Pre-Condition: OEM shall provide the cryptographic Module testing document and the detailed self / Lab test report along with test results

7. Test Objective: - To review the undertaking provided by the OEM

8. Test Plan

8.1 The Tester shall review the undertaking provided by the vendor as below.

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: NA

8.4 Test Execution Steps: Review the OEM undertaking

9. Expected Results for pass: The submitted undertaking is as per the ONT ITSAR

10. Expected Format of Evidence: *Securing Networks*

11. Test Execution

11.1 Test Case Number: 01

11.1.1 Test case Name: Review the undertaking provided by the vendor

11.1.2 Test Case Description: Review the undertaking provided by the vendor

11.1.3 Execution Steps:

- i. The Tester shall review the undertaking provided by the vendor as below: Cryptographic module embedded inside the Network product (which may be in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality are designed and implemented in compliance with FIPS 140-2 standards for different levels of security.
- ii. The Tester searched cryptographic module mentioned on OEM website so find below. However, no undertaking is available form OEM.

11.1.4 Test Observation: OEM undertaking required

11.1.5 Evidence Provided: -NA-

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	REMARKS
1	Review the undertaking provided by the vendor		



2.6.3 TSTP for Evaluation of Cryptographic Algorithms implementation Security Assurance

Optical Network Terminal (ONT)-PON
family Broadband Equipment ITSAR

ITSAR No: ITSAR403012311

Clause no:6.1.3

TSTP Document ID: **GE-BE-1103240001 v001**

DUT Details: **ONT**

DUT Software Version: **2.3.4.50B**

Digest Hash of OS: **Hash of DUT OS is required**

Digest Hash of Configuration: **Hash of DUT configuration is required**

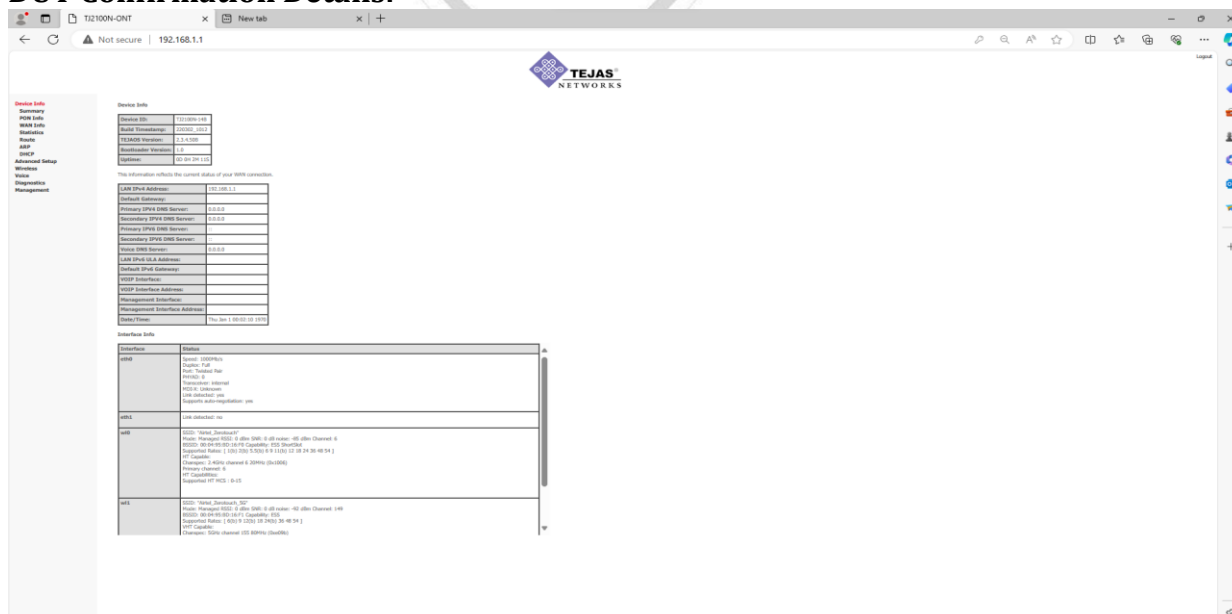
Applicable ITSAR: **ONT ITSAR403012311**

ITSAR Version No: **1.0.1**

OEM Supplied Document list: **NA**

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No & Name>** 2.6.3: Cryptographic Algorithm Implementation Security Assurance
3. **Requirement Description:** An undertaking is to be submitted by the vendor mentioning that "Cryptographic algorithms embedded in the crypto module of ONU/ONT shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm)."
Vendor shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results for scrutiny.

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.

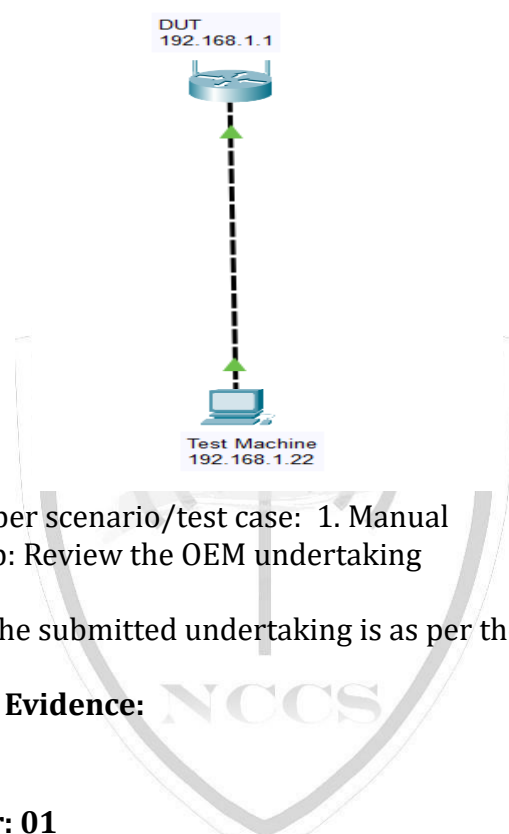
6. **Pre-Condition:** The vendor shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report

7. **Test Objective/ Purpose:** To review the undertaking provided by the OEM

8. Test Plan

8.1 Review the undertaking provided by the vendor.

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: 1. Manual

8.4 Test Execution Step: Review the OEM undertaking

9. **Expected Results:** The submitted undertaking is as per the ONT ITSAR

10. **Expected Format of Evidence:**

11 Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test case Name:** Review the undertaking provided by the vendor

11.1.2 **Test Case Description:** Review the undertaking provided by the vendor

11.1.3 **Execution Steps:** The Tester shall review the undertaking that is provided by the vendor as below: An undertaking shall be provided by the vendor as below: Cryptographic algorithms embedded in the crypto module of Network product are implemented in compliance with respective FIPS standards (for the specific crypto algorithm).

11.1.4 **Test Observation:** OEM undertaking required

11.1.5 **Evidence Provided:** -NA-

12 Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the undertaking provided by the vendor		

OEM undertaking required

2.6.4 TSTP for Evaluation of Protecting data and information – Confidential System Internal Data

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.6.4
--	--------------------------	-----------------

DUT Details: **ONT**

DUT Software Version: **2.3.4.50B**

Digest Hash of OS: Hash of DUT OS is required

Digest Hash of Configuration: **Hash of DUT configuration is required**

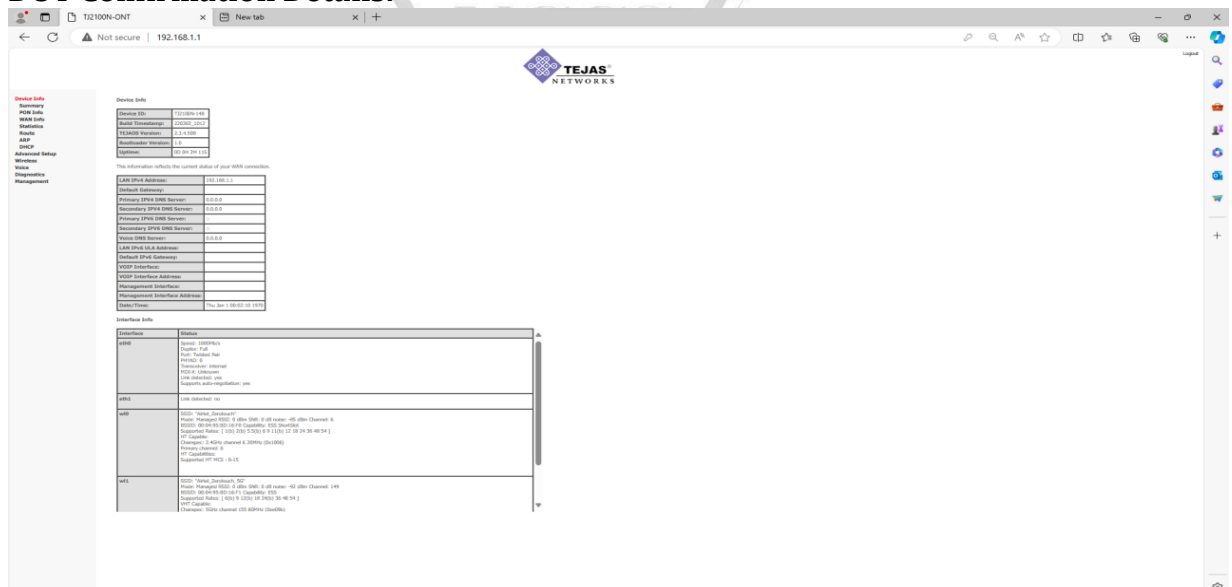
Applicable ITSAR: **ONT ITSAR403012311**

ITSAR Version No: **1.0.1**

OEM Supplied Document list: NA

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No &Name>** 1.6.4: Protecting data and information – Confidential System Internal Data
3. **<Requirement Description:>** When ONU/ONT is in normal operational mode (i.e., not in maintenance mode PINs, Cryptographic Keys, passwords, cookies) there shall be no system function that reveals confidential system internal data in the clear to users and administrators
Access to maintenance mode shall be restricted only to authorized privileged user.

4. DUT Confirmation Details:



5. **DUT Configuration:** Check if the DUT can be configured for normal operation mode and maintenance mode

6. Pre-Condition:

- i. The OEM shall provide documentation describing how confidential system internal information that could possibly be revealed in clear text is handled by system functions.
- ii. OEM shall provide a list of all system functions in the ONT, information on how to enable and execute them should be provided as a part of the vendor's documentation.

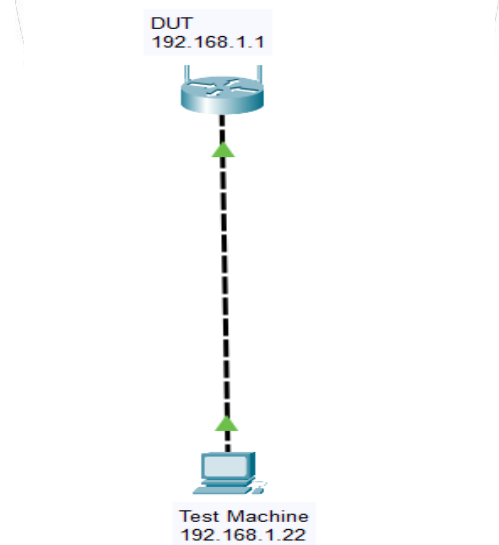
7. **Test Objective:** To verify that the DUT doesn't include a system function that exposes sensitive data in clear text

8. Test Plan

8.1 Test Cases:

- 8.1.1 Review the documentation provided by the vendor describing how confidential system internal information is handled by system functions.
- 8.1.2 The Tester shall connect DUT locally using command line interface or web interface and see the running configuration details, user details, error messages, logging messages, alarms, export mechanism.
- 8.1.3 The Tester shall check if the maintenance mode (if supported) is only accessed by authorized user

8.2 Test-bed setup Diagram:



8.3 **Test tool required per scenario/test case:** CMI/GUI Interface

8.4 Test Execution Steps

- i. Verify the normal operational and the maintenance mode feature present in the DUT from the OEM documentation
- ii. Verify the possible sensitive data at the directories and check if its visible in clear text
- iii. If maintenance mode supported by the DUT check if its only operated by the authorized mode

9. **Expected Results for Pass:** To verify that the DUT doesn't include a system function that exposes sensitive data in clear text

10. **Expected Format of Evidence:** - Screenshots

11. **Test Execution:**

11.1 **Test Case Number:** 01

11.1.1 **Test case Name:** OEM documentation for sensitive data

11.1.2 **Test Case Description:** Review the documentation provided by the vendor describing how confidential system internal information is handled by system functions.

11.1.3 **Execution Steps:** Review the OEM documentation to check for the sensitive data present at the possible directories (may also require shell access)

11.1.4 **Test Observation:** NA

11.1.5 **Evidence Provided:** -NA-

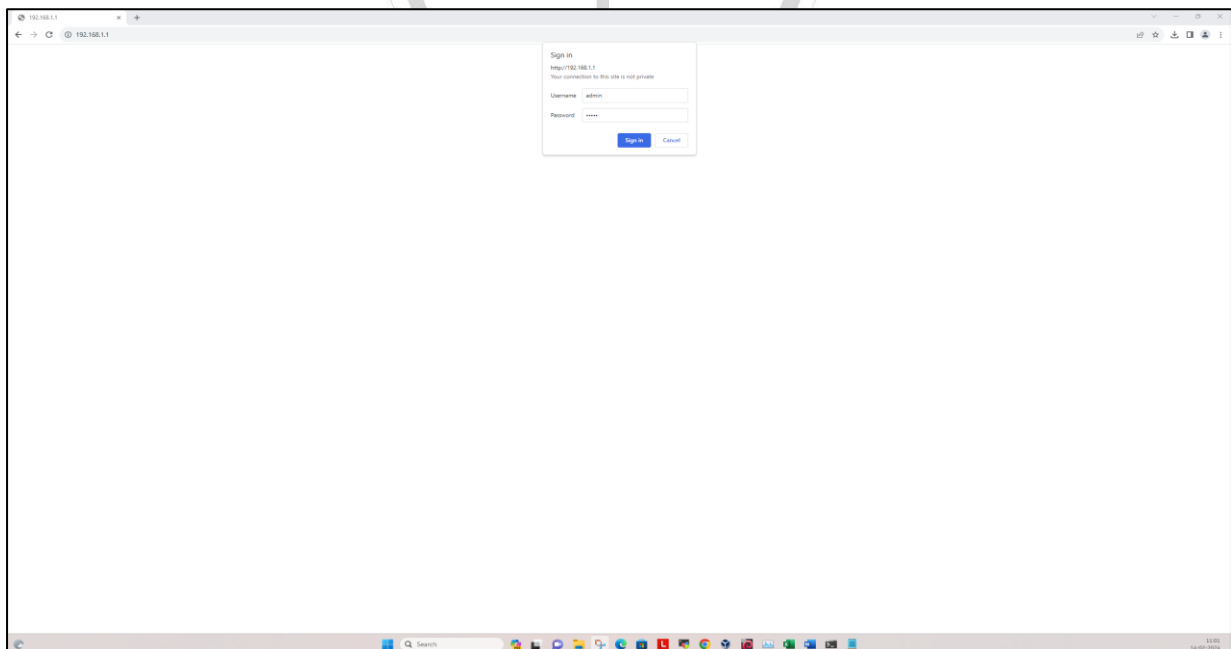
11.2 **Test Case Number:** 02

11.2.1 **Test case Name:** Sensitive data check

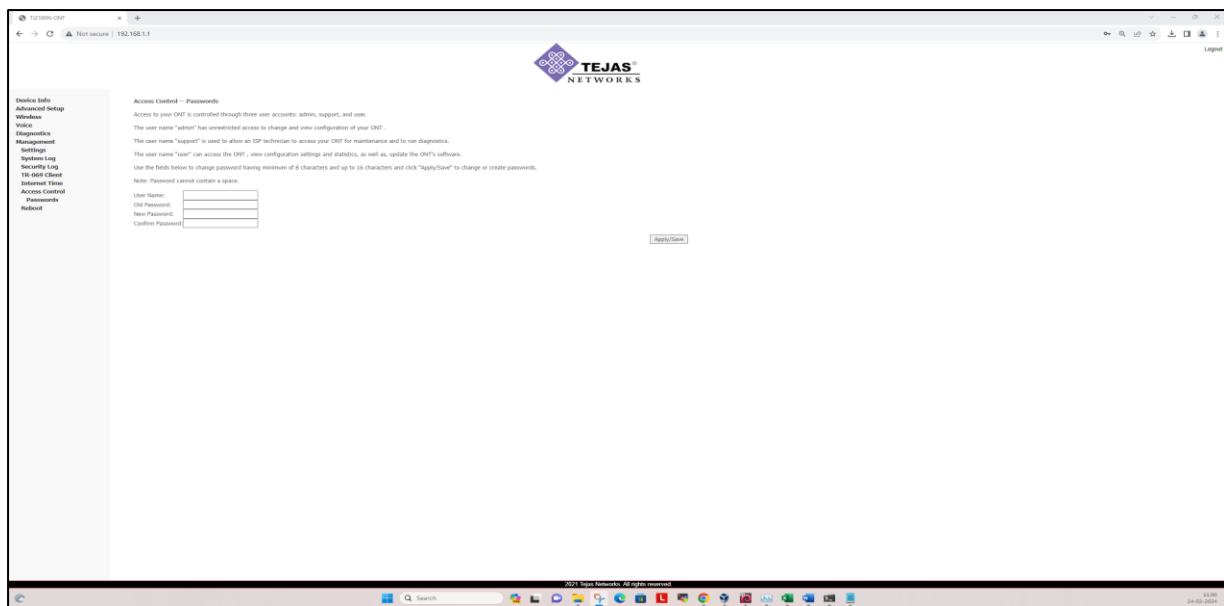
11.2.2 **Test Case Description:** The Tester shall connect DUT locally using command line interface or web interface and see the running configuration details, user details, error messages, logging messages, alarms, export mechanism.

11.2.3 **Execution Steps:**

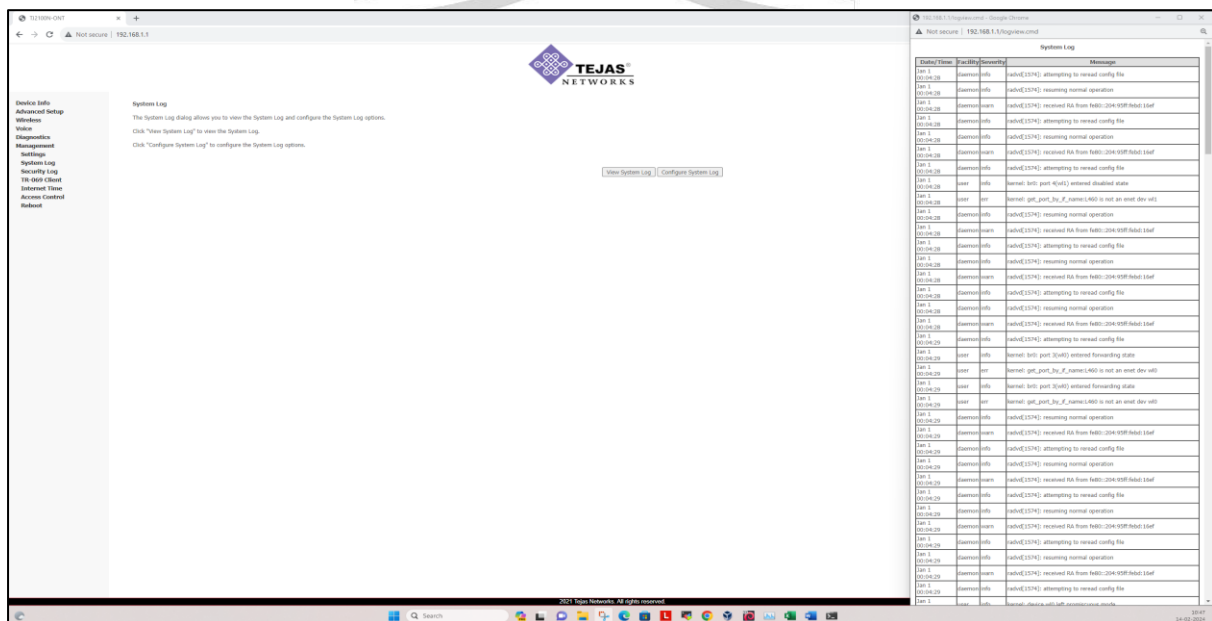
- i. Tester login DUT (192.168.1.1) via web interface using username and password from test machine (192.168.1.22).



- ii. The Tester Click Device info > summary for view configuration details of DUT.



- v. The Tester Click on management > system log for view logging messages details of DUT.



11.2.4 Test Observation: The Tester concludes no confidential system internal data revealed in the clear by each system function.

11.2.5 Evidence Provided: Screenshots are attached above

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM documentation for sensitive data		
2	Sensitive data check		

2.6.5 TSTP For Protecting data and information in storage

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.6.5
---	--------------------------	-----------------

DUT Details: **ONT**

DUT Software Version:**2.3.4.50B**

Digest Hash of OS: **Hash of DUT OS is required**

Digest Hash of Configuration: **Hash of DUT configuration is required**

Applicable ITSAR: **ONT ITSAR403012311**

ITSAR Version No: **1.0.1**

OEM Supplied Document list: **NA**

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No &Name>** 2.6.5: Protecting data and information in storage
3. **Requirement Description:** For Sensitive (eg PINs, cryptographic keys, password, cookies) data in storage (persistent or temporary), read access rights shall be restricted. Files of ONU/ONT system that are needed for the functionality shall be protected against manipulation strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only with appropriate nonrepudiation controls.

In addition, the following rules apply for:

- (i) Systems that need access to identification and authentication data in the clear/readable form e.g. in order to perform an activity/operation, such systems shall not store this data in the clear/readable form , but scramble or encrypt it by implementation-specific means.
- (ii) Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.
- (iii) Stored files: Shall be protected against manipulation strictly using the NCCS approved secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3;

4. DUT Confirmation Details:

Username of the Account	Password of the Account	Group	Privileges
admin	Digisol@321(Default)	Administrator	Admin – Highest Privilege
user	user	Normal user	Low Privilege
admin	admin123	Administrator	Admin – Highest Privilege
e8ftp	e8ftp	FTP user	FTP level privilege

12. Wireless Access Credentials:

SSID	Password	Frequency	Security
DIGISOL_5G	12345678	5GHz	WPA2-Personal
DIGISOL_2.4G	12345678	2.4GHz	WPA2-Personal

13. DUT Interface Information:

Interfaces	No. of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
GUI	-	Man-Machine Interface (MMI)	-

5. DUT Configuration:

i. SSH is enabled.

Service-Name	LAN	WAN	Port	Remote Host
Telnet	☐	☐	23	
Ftp	☒	☒	21	
Http	☒	☐	80	
HTTPS	☒	☐	443	
Secure Shell(Ssh)	☒	☒	22	
Tftp	☐	☐		
Ping	☒	☐		

ii. DUT is pre-configured with **BOA** as a webserver and its version 0.93.15.

```
C:\Users\KshitijaMhatre>curl http://192.168.1.1 --insecure -I
HTTP/1.0 302 Moved Temporarily
Date: Thu, 01 Jan 1970 02:14:12 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Location: /admin/login.asp
```

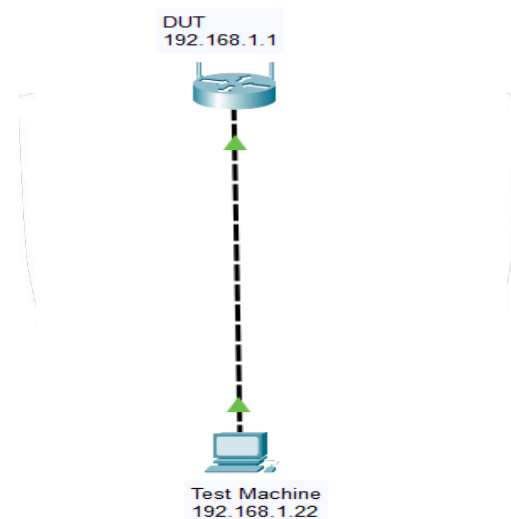
6. **Pre-Condition:** OEM shall provide detail of sensitive data in (persistent or temporary) and where it is stored and who all have access to read/ write.
7. **Test Objective/ Purpose:** To verify that the DUT stores the sensitive information in encrypted/hashed format

8. Test Plan

8.1 Number of Test Scenarios:

- 8.1.1 To verify that sensitive data in (persistent or temporary) storage read access rights shall be restricted.
- 8.1.2 The tester shall verify the unauthorized manipulation of the sensitive data is not possible.
- 8.1.3 The Tester shall check if sensitive data is encrypted or hashed in accordance to crypto control ITSAR

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: CLI/GUI Interface

8.4 Test Execution step:

- The tester accesses the DUT remotely and navigates to the directory of the sensitive data (in accordance to OEM documents)
- The tester shall check if read access is restricted
- The tester shall also attempt to manipulate the sensitive files
- If the sensitive files are encrypted or hashed the tester shall the used ciphers

9. **Expected Results:** DUT stores the sensitive data in encrypted format or hashed format which cannot be manipulated

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test case Name:** Read access rights restricted

11.1.2 **Test Case Description:** The tester shall check if read access rights of the sensitive files are restricted

11.1.3 Execution Steps:

- i. Open PuTTY application, provide the hostname as 192.168.1.1, port as 22, connection type as SSH and click on open. For authentication, provide the username as **admin** and password as **admin123**.

- ii. To check the read access of sensitive data in (persistent or temporary) storage, execute the following command – as shown in figure 4.1.6.1.

Enterlinuxshell

ls -la /var/tmp

- iii. To check the read permissions of the sensitive data like password, execute the below command – as shown in figure 4.1.6.1.

ls -la /etc/passwd

```
192.168.1.1 - PuTTY
login as: admin
admin@192.168.1.1's password:
>enterlinuxshell
# ls -la /var/tmp
drwxrwxr-x 2 admin 0 0 Jan 1 05:49 .
drwxr-xr-x 14 admin 0 0 Jan 1 05:30 ..
-rw-r--r-- 1 admin 0 107 Jan 1 05:49 .ash_history
-rw-r--r-- 1 admin 0 13 Jan 1 05:30 authinfo
-rw-r--r-- 1 admin 0 10 Jan 1 05:30 bosa_tips
-rw-r--r-- 1 admin 0 8 Jan 1 05:30 bosa_ver
-rw-r--r-- 1 admin 0 13 Jan 1 05:30 chip_type
-rw-r--r-- 1 admin 0 0 Jan 1 05:30 ft.conf
-rw-r--r-- 1 admin 0 74 Jan 1 05:49 hosts
-rw-r--r-- 1 admin 0 2 Jan 1 05:30 max_size_of_tcpdump_fil
s
---X----- 1 admin 0 84 Jan 1 05:30 pmap_deconfig
prwxr-xr-x 1 admin 0 0 Jan 1 05:30 ppp_serv_fifo
-rw-r--r-- 1 admin 0 13 Jan 1 05:30 prihwver
srwxr-xr-x 1 admin 0 0 Jan 1 05:30 upnpdm_action.sock
-rw-r--r-- 1 admin 0 1 Jan 1 05:30 voipstatus
-rw-r--r-- 1 admin 0 11 Jan 1 05:30 weblock_ver
-rw-r--r-- 1 admin 0 271 Jan 1 05:30 wscd_config.old
# ls -la /etc/passwd
lrwxrwxrwx 1 admin 0 11 Apr 3 2024 /etc/passwd -> /var/passwd
```

Figure no. 4.1.6.1: Check read permission of sensitive files

11.1.4 Test Observation: Normal users are restricted from accessing the Linux shell, and their privileges differ from those of admin users. Only **admin** users have read and write access to sensitive information.

```
192.168.1.1 - PuTTY
login as: user 1
user@192.168.1.1's password:
>
>enterlinuxshell 2
command error!

config          Configure system
exit            Exit command line interface
help           Help information
reboot         Reboot system
show           Show system information

>
login as: admin 3
admin@192.168.1.1's password:
>
>enterlinuxshell 4
# ls -l /var/passwd
-rw-r--r-- 1 admin 0 235 Jan 1 05:39 /var/passwd 5
```

11.1.5 Evidence Provided: Screenshots above

11.2 Test Case Number: 02

11.2.1 Test case Name: Manipulation protected

11.2.2 Test Case Description: The tester shall attempt to manipulate the sensitive files

11.2.3 Execution Steps:

- i. To check the write access of sensitive data in storage, execute the following command – as shown in figure
 - enterlinuxshell
 - cd /etc
 - cat passwd
 - cat >> passwd
 - enter “Hiiii”
 - cat passwd

```

>
>enterlinuxshell
# cd /etc
# pwd
/etc
#
  
```

Figure CLI access of DUT.

```

# cat passwd
admin:$1$wKGuF19A9A7dNAvGYdWC51:0:0::/tmp:/bin/cli
nobody:x:0:0::/tmp:/dev/null
admin:$1$CoERg7ynjYLSj2j4glJ34.:0:0::/tmp:/bin/cli
user:$1$ex9cQFo.PV11eSLXJFZuj.:1:0::/tmp:/dev/null
#
#
#
#
# cat >> passwd
Hiiiiii
# cat passwd
admin:$1$wKGuF19A9A7dNAvGYdWC51:0:0::/tmp:/bin/cli
nobody:x:0:0::/tmp:/dev/null
admin:$1$CoERg7ynjYLSj2j4glJ34.:0:0::/tmp:/bin/cli
user:$1$ex9cQFo.PV11eSLXJFZuj.:1:0::/tmp:/dev/null
Hiiiiii
#
  
```

Figure no. Check write permission of sensitive files.

11.2.4 Test Observations: It was observed that passwd files (that’s needed for the functionality of ONT) allows manipulation by the user.

11.3 Test Case Number: 03

11.3.1 Test case Name: Encrypted or Hashed sensitive files

11.3.2 Test Case Description: The tester shall verify the ciphers used in encrypting or hashing the sensitive files

11.3.3 Execution Steps

- i. To check if hashing is used to protect sensitive data, execute the following command – as shown in figure 4.3.6.1. and 4.3.6.2

- enterlinuxshell
- cd /etc
- cat passwd

```
>
>enterlinuxshell
# cd /etc
# pwd
/etc
#
```

Figure CLI access of DUT.

```
# cat passwd
admin:$1$$wKGuF19A9A7dNAvGYdWC51:0:0::/tmp:/bin/cli
nobody:x:0:0::/tmp:/dev/null
admin:$1$$CoERg7ynjYLsj2j4glJ34.:0:0::/tmp:/bin/cli
user:$1$$ex9cQFo.PV11eSLXJFZuj.:1:0::/tmp:/dev/null
#
```

Figure Check the hashing used for password

- Compare the hash found with cryptographic control of ITSAR.

11.3.4 Test Observation:

- The hashing used is MD5 as the hash begins with \$1\$ which is not as per Prescribed Cryptographic Control.
- (The tester may also confirm from the OEM for the supported ciphers by the ONT to encrypt or hash the sensitive data)

11.3.5 Evidence Provided:

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Read access rights restricted		
2	Manipulation protected		
3	Encrypted or Hashed sensitive files		

2.6.6 TSTP Report for Protection against Copy of Data

Optical Network Terminal (ONT)-PON
family Broadband Equipment ITSAR

ITSAR No: ITSAR403012311

Clause no:2.6.6

DUT Details: **ONT**

DUT Software Version: **2.3.4.50B**

Digest Hash of OS: **Hash of DUT OS is required**

Digest Hash of Configuration: **Hash of DUT configuration is required**

Applicable ITSAR: **ONT ITSAR403012311**

ITSAR Version No: **1.0.1**

OEM Supplied Document list: **NA**

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No &Name>** 2.6.6: Protection against copy of data
3. **Requirement Description:** Without authentication, ONU/ONT shall not create a copy of data in use or data in transit. Protective measures shall exist against use of available system functions/software residing in ONU/ONT to create copy of data for illegal transmission. The software functions, components in the ONU/ONT for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

4. DUT Confirmation Details:

DIGISOLLogout

Status

StatusNetworkSecurityApplicationManagementDiagnosticsHelp

Device InfoWAN InfoUser InfoVoip InfoRemote Manage Info

Device Basic Info

Device Info

Device model	DG-GR8821AC
Device SN	123451CEF03376DE2
Hardware Version	V4.2
Firmware Version	V2.1.08-230602
PON S/N	GPON00376DE2





14. DUT Interface Information:

Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
GUI	-	Man-Machine Interface (MMI)	-

5. **DUT Configuration:** There is no additional configuration required for this test case.
6. **Pre-Condition:** OEM shall provide detail of available system functions / software (ex. FTP, TFTP, NFS etc.) residing in ONT to create copy of data for illegal transmission.
7. **Test Objective / Purpose:** To verify that DUT doesn't allow unauthorized copying of data in use and transit
8. **Test Plan:**
 - 8.1 **Test Cases:**
 - 8.1.1 Copy of data in use
 - 8.1.2 Copy of data in transit
 - 8.2 **Test Bed Diagram:**



8.3 Test tool required per scenario/test case: CLI/GUI Interface

8.4 Test Execution

- i. The Tester shall review OEM documentation for the supported system functions used for copying of data and check if copying of data in use is possible without authentication
- ii. The Tester shall transfer data from ONT to another connected entity and check if data in transit been encrypted

9. Expected Results:

- i. DUT has protection measure against copying of data (by asking for authentication or only restricting it to authorized users only)
- ii. DUT shall check if copying of data is possible for data in transfer

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

Securing Networks

11.1.1 Test case Name: The Tester checks copying of data in use

11.1.2 Test Case Description: The Tester shall check if copy of data is possible for data in use

11.1.3 Execution Steps:

- i. The Tester shall review OEM documentation for the supported system functions used for copying of data and check if copying of data in use is possible without authentication
- ii. The tester checks if system functions for copying of data is possible without authentication
- iii. The tester can also check if copying of data is permitted to authorized users only

11.1.4 Test **Observation:** The Tester observed that there is no such system function present in the DUT

11.1.5 **Evidence Provided: screenshots**

11.2 Test Case Number: 02

11.2.1 Test case Name: Copying of data in transfer.

11.2.2 Test Case Description The tester checks if system functions for copying of data in transfer is possible without authentication

11.2.3 Execution Steps:

- i. Setup the FTP service in the DUT as mentioned in precondition.
- ii. Open the FTP client and provide the details to establish connection as below:
 - Host: 192.168.1.1
 - Username: e8ftp
 - Password: e8ftp
 - Port:21
- iii. Click on 'Quickconnect' to establish the connection.
- iv. Upload file 'authinfo' file from the DUT (Remote site) to the client (Local site) by dragging the file from remote site to local site – as shown in figure 4.1.6.1.

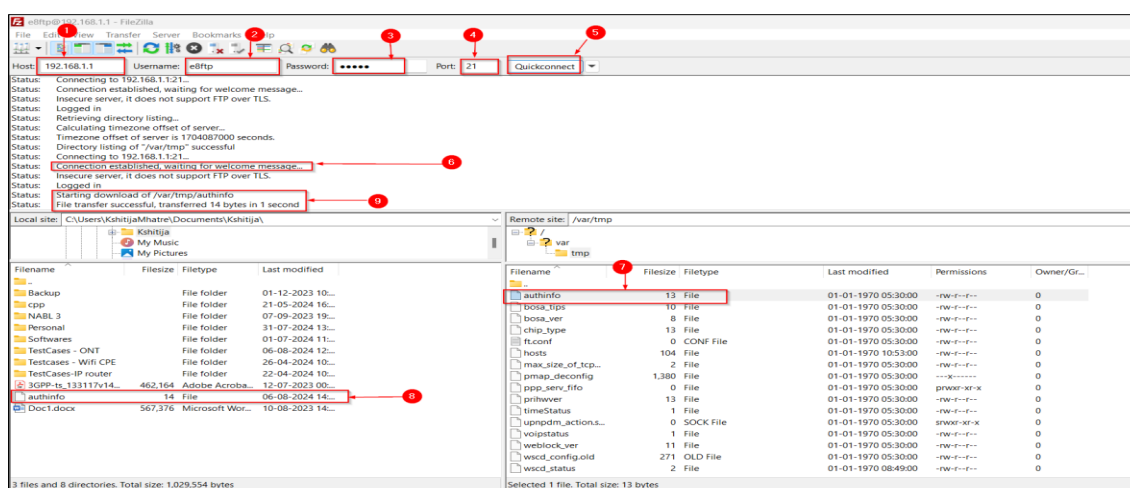
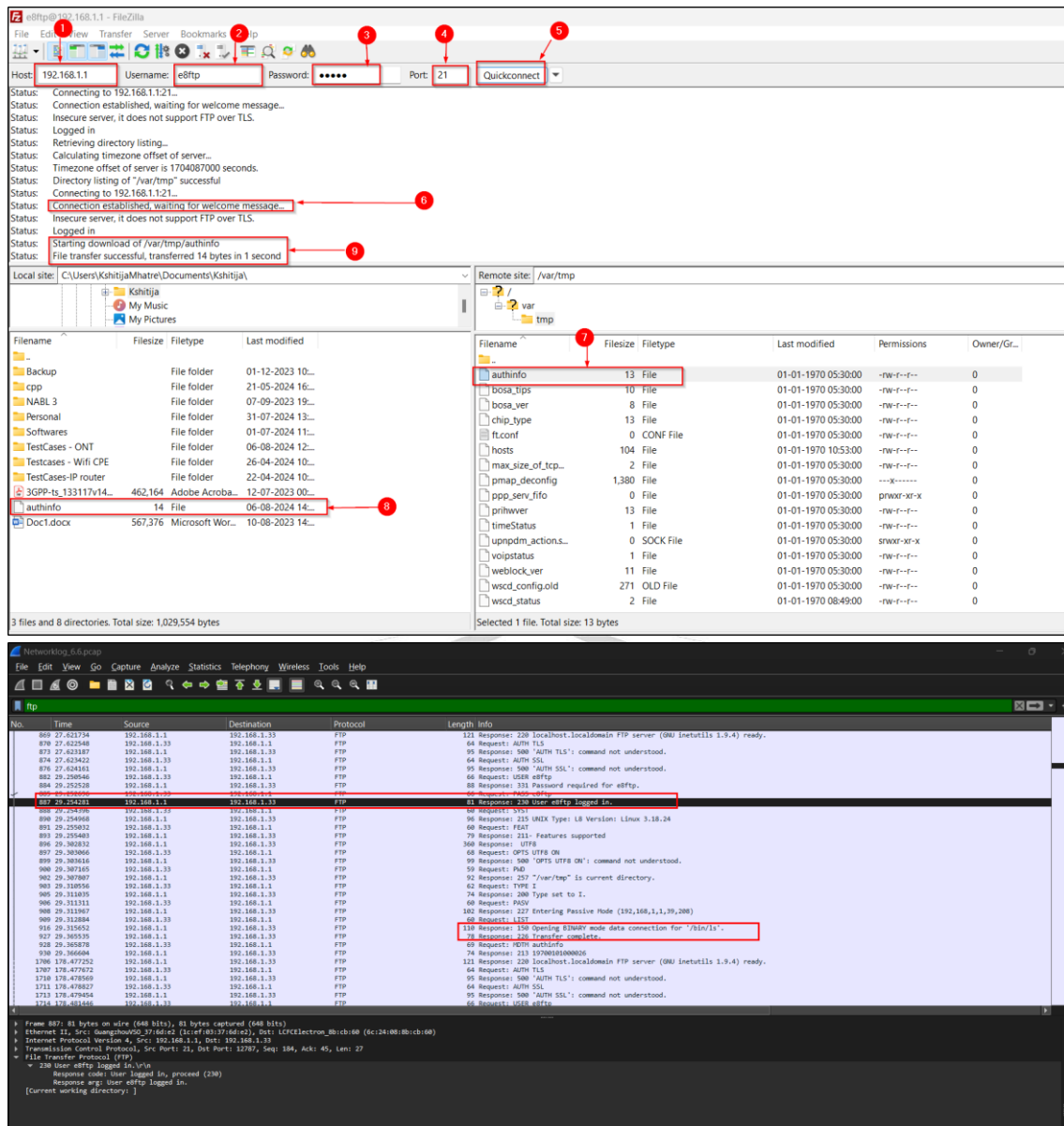


Figure Checking copy of data over ftp transfer.

- Check if a copy of the file 'authinfo' is created at the local site (192.168.1.33) or at the DUT (192.168.1.1)

11.2.4 Test Observation:

- i. Transfer of data does not create a copy of the data on the server, nor does it create copy on the client side.
- ii. The DUT also asks for authentication before the transfer of data.



11.2.5 Evidence Provided: Screenshots above

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	The Tester checks copying of data in use		
2	Copying of data in transfer		

2.6.7 TSTP Report for Protection against Data Exfiltration - Overt Channel

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR

ITSAR No: ITSAR403012311

Clause no:2.6.7

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

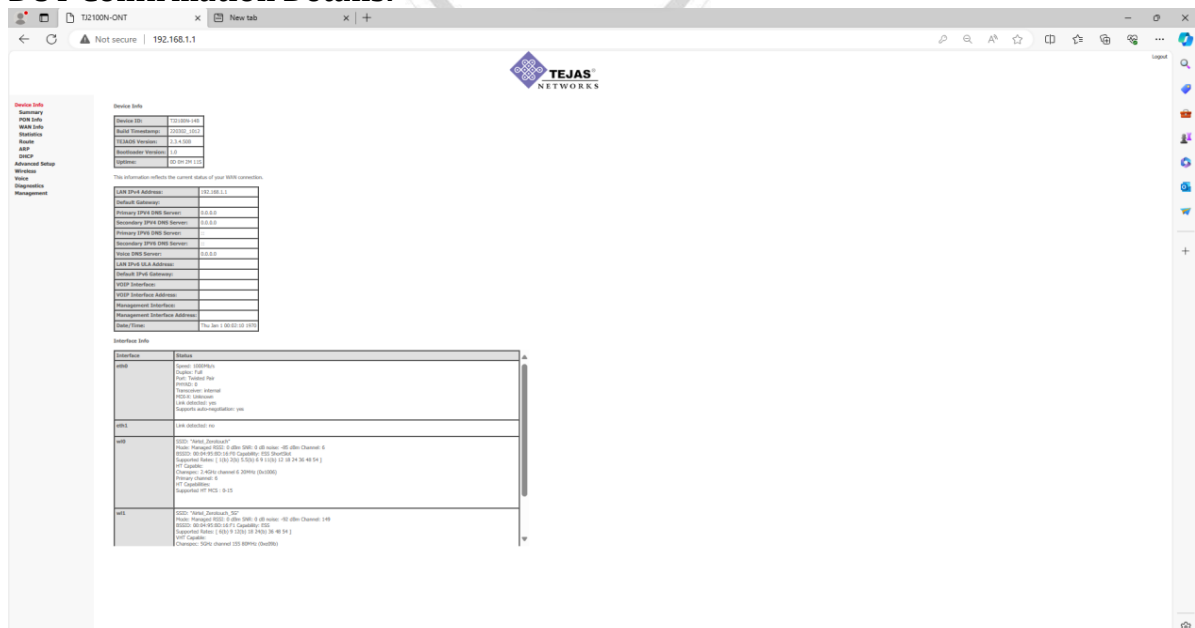
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No &Name>** 2.6.7: Protection against Data Exfiltration – Overt Channel
3. **Requirement Description:** ONU/ONT shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound overt channels such as, HTTPS IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network product. Session logs shall be generated for establishment of any session initiated by either user or ONU/ONT.

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.

6. **Precondition:** OEM to provide the documentation describing the supported overt outbound protocols
7. **Test Objective:** To verify that DUT's overt channels cannot be used for data exfiltration

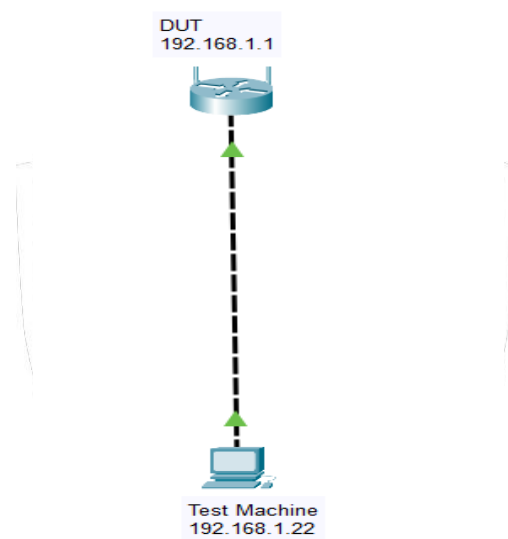
8. Test Plan

8.1 Test Cases:

8.1.1 The Tester shall review the document from OEM explaining the mechanism implemented to meet the clause and the default configuration.

8.1.2 The Tester shall check if any of the services is used for Outbound channel.

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: CLI/GUI Interface

8.4 Test Execution Steps

- i. The Tester shall review the OEM documentation for the supported outbound overt channels
- ii. The Tester shall verify the protection mechanism implemented for the establishment of outbound overt channel
- iii. The Tester shall verify the presence of monitoring logs for established outbound overt channel

9. Expected Results for Pass: DUT's overt channels cannot be used for data exfiltration

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 **Test case Name:** OEM document review for outbound overt channel

11.1.2 **Test Case Description:** OEM shall provide detail of mechanisms used to prevent data exfiltration attacks for theft of data in use / data in transit.

11.1.3 **Execution Steps:**

- i. The Tester shall review the OEM documentation for the supported outbound overt channels and verify its existence
- ii. The Tester may use any port scanning tool (eg: nmap) for its verification

11.1.4 Test Observation:

11.1.5 Evidence Provided:-NA-

11.2 Test Case Number: 02

11.2.1 Test case Name: Protection for outbound overt channel establishment

11.2.2 Test Case Description: The Tester shall check if any of the services is used for Outbound channel has protection mechanism

11.2.3 Execution Steps:

- i. The tester shall review the OEM documentation if any protection feature is present for the usage of outbound overt channel
- ii. The tester shall verify by establishing connection with any connected entity and check if its only possible for authorized users only
- iii. The tester shall check if any authentication is asked before the establishment of outbound overt channel.

11.2.4 Test Observation:

11.2.5 Evidence Provided: -NA-

11.3 Test Case Number: 03

11.3.1 Test case Name: Monitoring log system

11.3.2 Test Case Description: To Verify the Session logs must be generated for all user and ONU/ONT initiated session.

11.3.3 Execution Steps:

- i. Verify that which outbound services present on the DUT.
- ii. Try to initiate the session by using any of this outbound service FTP, HTTP, HTTPS IM, P2P supported by DUT.
- iii. Verify that DUT generated session log if any of the outbound service such as FTP, HTTP, HTTPS IM, P2P initiate by DUT.

11.3.4 Test Observation

11.3.5 Evidence Provided: -NA-

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM document review for outbound overt channel		
2	Protection for outbound overt channel establishment		
3	Monitoring log system		

2.6.8 TSTP Report for Protection against Data Exfiltration - Covert Channel

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR

ITSAR No: ITSAR403012311

Clause no:2.6.8

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 1.6: Data Protection
2. **<Security Requirement No &Name >** 2.6.8: Protection against Data Exfiltration – Covert Channel
3. **Requirement Description:** NE shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network Product.
Session logs shall be generated for establishment of any session initiated by either user or ONU/ONT.

4. DUT Confirmation Details:

The screenshot displays the TEJAS NETWORKS management interface for a device at IP 192.168.1.1. The interface is divided into several sections:

- Device Info:**
 - Device ID: 123456789
 - Build Version: 1.0.0.0
 - Hardware Version: 1.0.0.0
 - Software Version: 1.0.0.0
 - Uptime: 00:01:24.123
- WAN Info:**
 - WAN IP Address: 192.168.1.1
 - Default Gateway: 192.168.1.1
 - Primary DNS Server: 8.8.8.8
 - Secondary DNS Server: 8.8.4.4
 - Primary IPv6 DNS Server: 2001::1
 - Secondary IPv6 DNS Server: 2001::2
 - WAN IPsec Status: Disabled
 - WAN IPsec SA Address: 192.168.1.1
 - Default IPsec Gateway: 192.168.1.1
 - IPsec Tunnel Name: 192.168.1.1
 - IPsec Tunnel Address: 192.168.1.1
 - Management Interface: 192.168.1.1
 - Device Time: Thu Jan 1 00:00:00 2020
- Interface Info:**
 - eth0:** Status: Up, Type: Ethernet, MAC: 00:00:00:00:00:00, IP: 192.168.1.1, MTU: 1500, Speed: 100Mbps, Duplex: Full, Link Status: Up, Link Speed: 100Mbps, Link Duplex: Full, Link Mode: Auto.
 - eth1:** Status: Up, Type: Ethernet, MAC: 00:00:00:00:00:00, IP: 192.168.1.2, MTU: 1500, Speed: 100Mbps, Duplex: Full, Link Status: Up, Link Speed: 100Mbps, Link Duplex: Full, Link Mode: Auto.
 - eth2:** Status: Up, Type: Ethernet, MAC: 00:00:00:00:00:00, IP: 192.168.1.3, MTU: 1500, Speed: 100Mbps, Duplex: Full, Link Status: Up, Link Speed: 100Mbps, Link Duplex: Full, Link Mode: Auto.
 - eth3:** Status: Up, Type: Ethernet, MAC: 00:00:00:00:00:00, IP: 192.168.1.4, MTU: 1500, Speed: 100Mbps, Duplex: Full, Link Status: Up, Link Speed: 100Mbps, Link Duplex: Full, Link Mode: Auto.

5. **DUT Configuration:** OEM shall provide details on what mechanisms are used to prevent data exfiltration attacks for theft of data in use/data in transit and Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS

Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation, etc. are to be forbidden. if they are initiated by CPE and how to monitor anomalous channels.

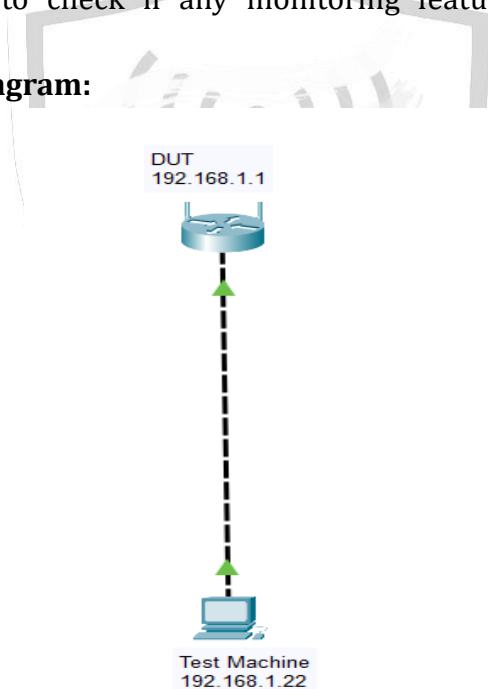
6. **Precondition:** OEM shall provide details what mechanisms used to prevent data exfiltration attacks for theft of data in use / data in transit and Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden. if they are initiated by CPE and how to monitoring anomalous channels.
7. **Test Objective:** To check DUT's protection against establishment of covert channel for data exfiltration

8. Test Plan

8.1 Test Cases:

- 8.1.1 Test Scenario to review the OEM documentation and check if the mentioned covert channels are used as overt channels
- 8.1.2 Test Scenario to check for the establishment of covert channel
- 8.1.3 Test Scenario to check if any monitoring feature exists for any channel establishment

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: CLI/GUI Interface

8.4 Test Execution

- i. The Tester shall review the OEM documentation to check if any covert channels can be figured out
- ii. The Tester shall attempt to establish covert channels from DUT to other connected entity
- iii. The Tester shall check for any monitoring features present in DUT upon establishment of any channel

9. **Expected Result for pass:** The DUT should have protection measures against establishment of covert channel

10. **Expected Format of Evidence:** screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1.**Test Case Name:** Review the OEM documentation

11.1.2.**Test Case Description:** The Tester shall check if any of the services are used for the Outbound covert channel.

11.1.3.**Execution Steps:** The Tester shall review the OEM documentation for the mentioned overt channels and figure out the possible covert channels

11.1.4.**Test Observation:** The Tester explored the DUT and didn't find any outbound covert channels such as FTP, HTTPS IM, P2P, Email, etc. other than HTTP. HTTP channel is used for the management/configuration of DUT.

11.1.5.**Evidence Provided:** -NA-

11.2 Test Case Number: 02

11.2.1. **Test Case Name:** Covert channel establishment

11.2.2. **Test Case Description:** The Tester shall attempt to establish the covert channels from DUT to any other connected entity

11.2.3. Execution Steps

- i. The Tester shall attempt to establish covert channel Dns tunnel
- ii. Attempt to connect the WIFI CPE to a testing machine via ethernet and capture the same on Wireshark filter the packets captured on port 53 and inspect the packet traces. Check if any dns tunnel query is found in the traces (looking for unusual characteristics like frequent, short queries with seemingly random domain names, large numbers of subdomains within a single domain, or unusual query types, which could indicate data being encoded within the DNS requests)
- iii. If the DUT supports the tool "iodine" or "dnscat2", these tools can be used to establish dns tunnel (Similarly the tester can check for the establishment of other covert channels from DUT using relevant commands)

11.2.4. Test Observation: -NA-

11.2.5. Evidence Provided: -NA-

11.3 Test Case Number: 03

11.3.1 **Test Case Name:** Monitoring feature in DUT

11.3.2 **Test Case Description:** The Tester shall check for any monitoring features present in DUT upon establishment of any channel

11.3.3 Execution Steps:

- i. The Tester shall attempt to establish of a channel (covert or overt)
- ii. The Tester shall check if the DUT logs the establishment of the channel

11.3.4 **Test Observations:** -NA-

11.3.5 **Evidence provided:** -NA-

12. Test Case Results:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Review the OEM documentation		
2.	Establishment of covert channels		
3.	Monitoring of establishment		



Section 7: Network Services

2.7.1 TSTP for Evaluation of Traffic Separation

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.7.1
--	--------------------------	-----------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 7: Network Services

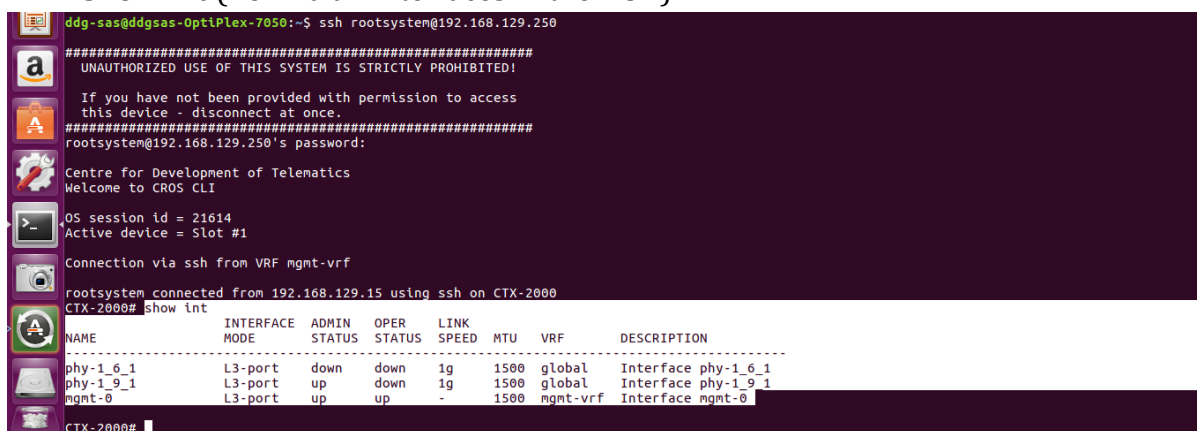
2. <Security Requirement No & Name > 1.7.1 Traffic Separation

3. <Requirement Description: > ONU/ONT shall support physical and/or logical separation of Operation & Maintenance traffic and control plane traffic. See RFC 3871 [3] for further information.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.5.1].

4. DUT Confirmation Details:

- Use the command line interface to get details of the machine on which test is conducted.
- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info
Command used: **do show int** (To find all interfaces in the DUT)
show int (To find all interfaces in the DUT)



```
ddg-sas@ddgsas-OptiPlex-7050:~$ ssh rootsystem@192.168.129.250
#####
UNAUTHORIZED USE OF THIS SYSTEM IS STRICTLY PROHIBITED!
#####
If you have not been provided with permission to access
this device - disconnect at once.
#####
rootsystem@192.168.129.250's password:
Centre for Development of Telenatics
Welcome to CROS CLI
OS session id = 21614
Active device = Slot #1
Connection via ssh from VRF mgmt-vrf
rootsystem connected from 192.168.129.15 using ssh on CTX-2000
CTX-2000# show int
NAME          INTERFACE ADMIN  OPER  LINK  MTU  VRF      DESCRIPTION
MODE          STATUS STATUS SPEED
-----
phy-1_6_1     L3-port  down  down  1g    1500 global Interface phy-1_6_1
phy-1_9_1     L3-port  up    down  1g    1500 global Interface phy-1_9_1
mgmt-0        L3-port  up    up    -     1500 mgmt-vrf Interface mgmt-0
CTX-2000#
```

Command used: **show version** (To get Application No/Version No & Kernel Info)


```

CTX-2000#
CTX-2000#
CTX-2000#
CTX-2000#
CTX-2000# show version
Release summary of active image

Host           : CTX-2000
Uptime         : up 1 week, 6 days, 22 hours, 25 minutes
System MAC     : 00:24:88:a0:41:00

Model          : CTX-2000-32Q-AC
Serial Num     : 1122600012
Software Version : CROS-H-1.1.1
Build          : 1140 (base:6196) (Tue Nov 22 14:16:48 IST 2022)
SDK Version    : SX-SDK ETH 4.5.2028, SX-API 1.0.0, SXD 2.00 , ISSU 101

Bootloader     : (GRUB) 2.02~beta3-5+deb9u2
Platform Version : ONIE 2020.11-5.3.0005-115200
Kernel Version : git-b799d9558a Wed Apr 27 11:02:30 UTC 2022

CTX-2000#
CTX-2000#

```

5. DUT Configuration:

- i. Tester should configure the DUT interfaces to support O&M and Control plane traffic separately.
- ii. IP address of Management interface: x.x.x.x
- iii. IP address of Data interface: x.x.x.x

6. Preconditions

- i. The network product has at least two separate physical or logical interfaces.
- ii. OEM should provide details about interface configuration.

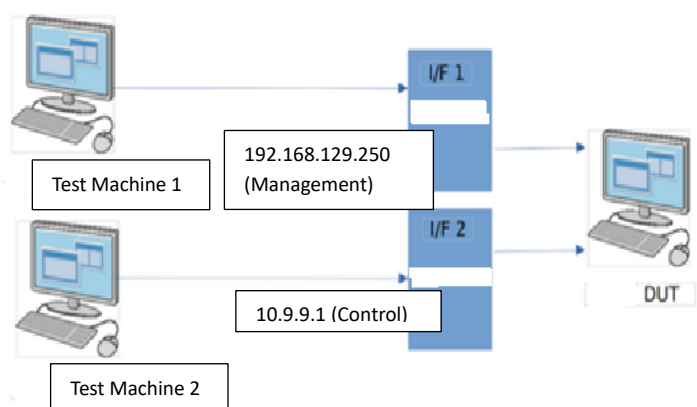
7. Test Objective: DUT shall support physical or logical separation of O&M and Control Plane traffic.

8. Test Plan:

8.1 Number of Test Scenarios: 01

8.1.1 Test Scenario for physical or logical traffic Separation

8.2 Test Setup Diagram:



13.1.21.

8.3 Tools Used: Command line interface of DUT, Ping

8.4 Test Execution Steps

- i. Test Machine 1 and Test Machine 2 will try to send the ICMP messages to system over separate interfaces.
- ii. DUT should allow the traffic to separately handle at the two interfaces.
- iii. Test Machine 1 will be sending the traffic to DUT over interface I/F 1
- iv. Test Machine will be sending the traffic of icmp messages to DUT over interface with ip address I/F 2

9. Expected Results for Pass:

- i. The ping messages for the Test Machine 1 will be successfully transmitted without any loss when sent to the interface 1 of the DUT. But the ping messages fail to reach interface 2 of the DUT.
- ii. The ping messages for the Test Machine 2 will be successfully transmitted without any loss when sent to the interface 2 of the DUT. But the ping messages fail to reach interface 1 of the DUT.
- iii. This is because the traffic is separated by DUT to different domains for handling the icmp messages from different Test Machine.

10. **Expected Format of Evidence:** Evidence in the form of the screenshot of the command line can be submitted.

11. Test Execution:

11.1 **Test Case Name:** TC_TRAFFIC_SEPARATION

11.2 **Test Case Description:** The DUT should support the physical or logical separation of traffic belonging to different network domains.

11.3 **Execution Steps:**

- i. Case 1 – Physical separation of O&M and Control Traffic.: Below screenshots shows DUT has separate interface for O&M traffic and separate for data plane traffic.



15. Figure: Console and Management Interface of DuT

- ii. Case 2 – Logical Separation of O&M and Control plane Traffic.

16. Tester will ping the DUT using command line of the Test Machine 1

17. ping 192.168.129.250

18. Tester will ping the DUT using command line of the Test Machine 2

19. ping 10.9.9.1
20. Tester will ping the DUT using the command line of Test Machine 1 but this time at the other interface
21. ping 10.9.9.1

```

ddg-sas@ddgsas-OptiPlex-7050: ~
ddg-sas@ddgsas-OptiPlex-7050:~$ ping 10.9.9.1
PING 10.9.9.1 (10.9.9.1) 56(84) bytes of data.
From 192.168.129.9 icmp_seq=1 Destination Host Unreachable
From 192.168.129.9 icmp_seq=2 Destination Host Unreachable
From 192.168.129.9 icmp_seq=3 Destination Host Unreachable
^C
--- 10.9.9.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2037ms
ddg-sas@ddgsas-OptiPlex-7050:~$

```

22. Tester will ping the DUT using the command line of Test Machine 2 but this time at the other interface.
23. Ping 192.168.129.250

```

ddg-sas@ddgsas-OptiPlex-7050: ~
ddg-sas@ddgsas-OptiPlex-7050:~$ ping 192.168.129.250
PING 192.168.129.250 (192.168.129.250) 56(84) bytes of data.
^C
--- 192.168.129.250 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2052ms
ddg-sas@ddgsas-OptiPlex-7050:~$

```

11.4 Test Observations:

- i. The ping messages for the Test Machine 1 will be successfully transmitted without any loss when sent to the interface 1 of the DUT. But the ping messages fail to reach the interface 2 of the DUT.
- ii. The ping messages for the Test Machine 2 will be successfully transmitted without any loss when sent to the interface 2 of the DUT. But the ping messages fail to reach the interface 1 of the DUT.
- iii. This is because the traffic is separated by DUT to different domains for handling the ICMP messages from different Test Machines.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_ TRAFFIC_SEPARATION		

2.7.2 TSTP Evaluation for Traffic Filtering – Network Level Requirement

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.7.2
--	--------------------------	-----------------

<DUT Details: > **SyroTech**

<DUT Software Version:> **V 3.2.02-231205**

<Digest Hash of OS>

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 7: Network Services

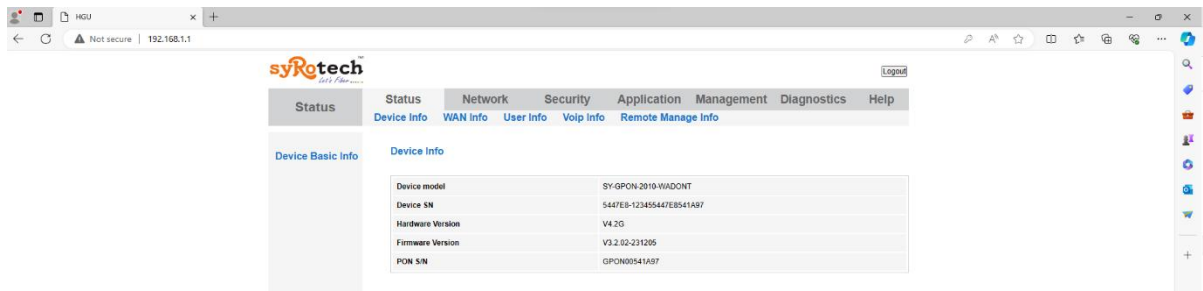
2. **<Security Requirement No & Name >** 2.7.2 Traffic Filtering – Network Level Requirement

3. **<Requirement Description: >** ONT/ONU shall provide a mechanism to filter incoming IP packets on any IP interface. In particular the Network product shall provide a mechanism:

- i. To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.
- ii. To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
 - Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
 - Accept: the matching message is accepted.
 - Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
- iii. To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.
- iv. To filter on the basis of the value(s) of any portion of the protocol header.
- v. To reset the accounting.
- vi. The Network product shall provide a mechanism to disable/enable each defined rule.

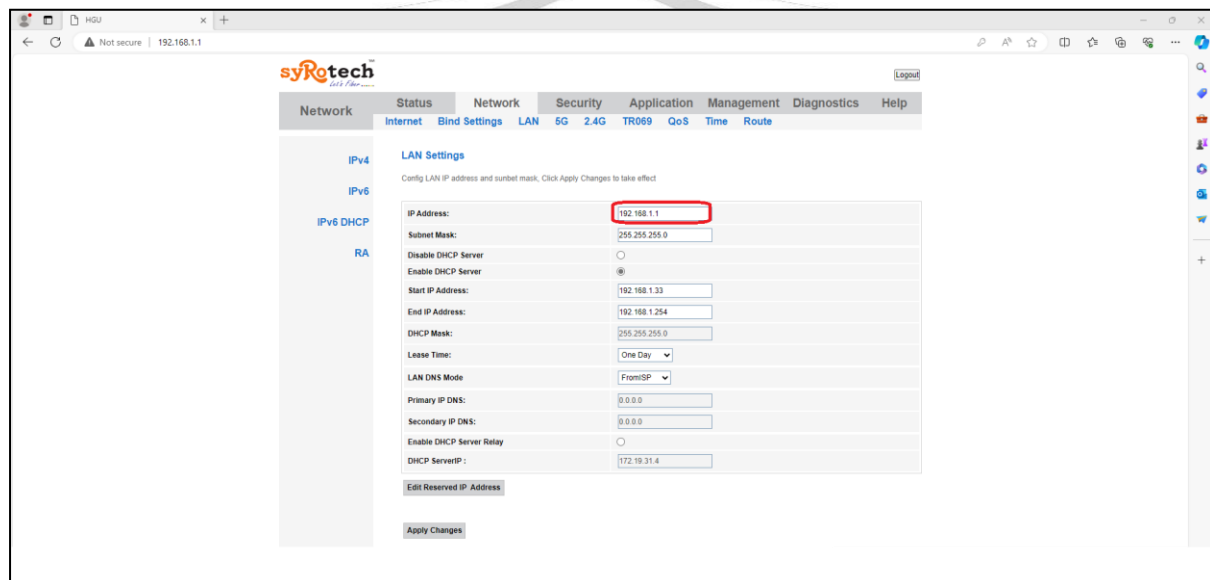
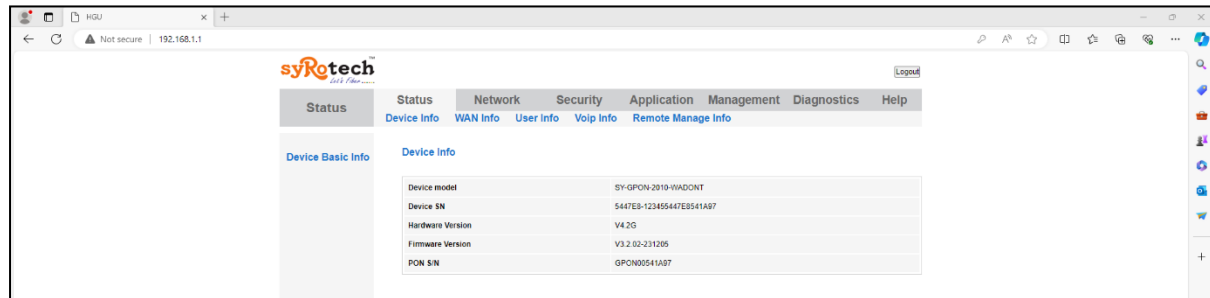
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. section 4.2.6.2.1]

4. **DUT Confirmation Details:**



5. DUT Configuration:

Below screenshot is IP address of DUT:



Below Screenshot is IP address of DUT Test Machine:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\GRL MAS> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:db8::2
    Link-local IPv6 Address . . . . . : fe80::f15:48d0:ec20:8580%5
    IPv4 Address. . . . . : 192.168.1.22
    Subnet Mask . . . . . : 255.255.255.0
    IPv4 Address. . . . . : 192.168.3.1
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 2001:db8::1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::828b:589b:918f:89ec%15
    IPv4 Address. . . . . : 192.168.1.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f620:5e07:cb37:86aa%4
    IPv4 Address. . . . . : 192.168.100.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e92b:1eeb:17bc:293a%25
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1042:cb42:a604:410e%20
    IPv4 Address. . . . . : 169.254.19.174
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 6:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::be98:ec2f:d4cc:6198%2
    IPv4 Address. . . . . : 192.168.169.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Additionally, to ensure the connectivity between the DUT and the test machine, a ping test is conducted. This test verifies the ability to test machine to communicate with the DUT over the Ethernet connection by sending ICMP echo requests and receiving ICMP echo replies. A successful ping indicates that the network connection is established and functioning properly, enabling further testing and data transfer between the DUT and the test machine.

```
PS C:\Users\GRL MAS> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\GRL MAS>
```

6. Preconditions

- i. The DUT has packet filtering enabled.
- ii. The DUT should have at least 2 different logical or physical ports and each port is connected to a host.

iii. OEM should submit document about filtering features available in DUT.

7. Test Objective: To check that DUT shall provide a mechanism:

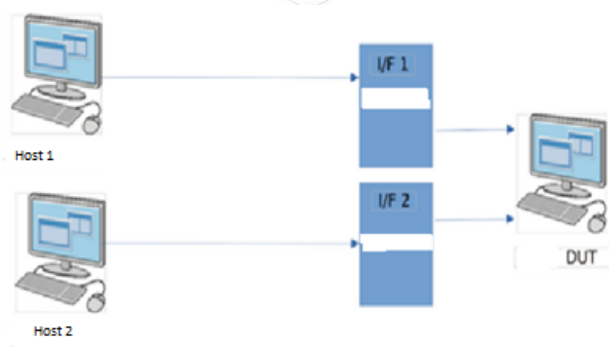
- i. To filter incoming IP packets on any IP interface at Network Layer and Transport Layer Of the stack ISO/OSI.
- ii. To allow specific actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
 - a. Discard/Drop: the matching message is discarded, no subsequent rules are applied and no answer is sent back.
 - b. Accept: the matching message is accepted.
 - c. Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
- iii. To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.
- iv. To filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.
- v. To reset the accounting.
- vi. The DUT shall provide a mechanism to disable/enable each defined rule.

8. Test Plan:

8.1 Number of test scenario:

- 8.1.1 Packet filtering for HOST 1
- 8.1.2 Packet filtering for HOST2.
- 8.1.3 Enable/Disable logging
- 8.1.4 Port Filtering
- 8.1.5 To enable or disable filter.
- 8.1.6 To reset the counter
- 8.1.7 Packet Filtering account.

8.2 Test Setup Diagram:



8.3 Tools Used: Command line interface, IP tables

8.4 Test Execution Steps

- i. Firstly, the network should be established as such in which DUT is the Server and 2 Hosts (For simulation purposes we have taken 2 Hosts/Clients) are connected to the Server.
- ii. Obtain the IP Address of the DUT and the Hosts.

iii. Configure the Rules in the DUT for Packet Filtering as follows.

Name	Ip Address	Rules
(HOST1)	172.20.0.4	ACCEPT ICMP echo messages
(HOST2)	172.20.0.3	DROP ICMP echo messages
(SERVER/DUT)	172.20.0.2	-

iv. In case iptables is implemented then below command should be used in command line of DUT for accepting the icmp echo messages from HOST 1.

v. iptables **-A INPUT -p icmp --icmp-type 8 -s <HOST1 ip Address> -j ACCEPT**

vi. In case iptable is implemented then below command should be used in command line of DUT for dropping the icmp echo messages from HOST 2.

vii. iptables **-A INPUT -p icmp --icmp-type 8 -s <HOST2 ip Address> -j DROP**

viii. The tester configures the Network Product to only allow ICMP traffic from host 1.
(Check if option is available at network level)

ix. The tester initiates ping traffic from host 1.

x. The tester initiates ping traffic from host 2.

9. **Expected Results for Pass:** Host 1 will receive a 'ping' answer back, but host 2 will not.

10. **Expected Format of Evidence:** Log files and screen shots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. **Test Case Name:** TC1_PACKET_FILTERING_HOST1

11.1.2. **Test Case Description:** As per the Rules mentioned in the table, DUT should respond to ICMP messages sent from HOST 1.

11.1.3. Execution Steps:

- Check that precondition is already satisfied by the DUT.
- Use the command line of the HOST1 to ping the DUT.
- Use the following command.
- ping -I <HOST1 IP Address> <DUT IP Address>**
- Capture the response on the HOST1 for the above command.

11.1.4. Test Observations:

- Case 1: DUT's response is positive for the HOST1's icmp messages (PASS CASE)
Below image can be used as a reference that HOST1 is getting positive response from DUT to ICMP messages sent.


```

root@6f47349eede5:/# ping -I 172.20.0.4 172.20.0.2
PING 172.20.0.2 (172.20.0.2) from 172.20.0.4 : 56(84) bytes of data.
64 bytes from 172.20.0.2: icmp_seq=1 ttl=64 time=0.135 ms
64 bytes from 172.20.0.2: icmp_seq=2 ttl=64 time=0.138 ms
64 bytes from 172.20.0.2: icmp_seq=3 ttl=64 time=0.128 ms
64 bytes from 172.20.0.2: icmp_seq=4 ttl=64 time=0.118 ms
64 bytes from 172.20.0.2: icmp_seq=5 ttl=64 time=0.138 ms
64 bytes from 172.20.0.2: icmp_seq=6 ttl=64 time=0.130 ms
64 bytes from 172.20.0.2: icmp_seq=7 ttl=64 time=0.137 ms
64 bytes from 172.20.0.2: icmp_seq=8 ttl=64 time=0.103 ms
64 bytes from 172.20.0.2: icmp_seq=9 ttl=64 time=0.136 ms
64 bytes from 172.20.0.2: icmp_seq=10 ttl=64 time=0.147 ms
64 bytes from 172.20.0.2: icmp_seq=11 ttl=64 time=0.104 ms
64 bytes from 172.20.0.2: icmp_seq=12 ttl=64 time=0.146 ms
64 bytes from 172.20.0.2: icmp_seq=13 ttl=64 time=0.139 ms
64 bytes from 172.20.0.2: icmp_seq=14 ttl=64 time=0.148 ms
64 bytes from 172.20.0.2: icmp_seq=15 ttl=64 time=0.128 ms
64 bytes from 172.20.0.2: icmp_seq=16 ttl=64 time=0.129 ms
^C
--- 172.20.0.2 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15356ms
rtt min/avg/max/mdev = 0.103/0.131/0.148/0.013 ms
root@6f47349eede5:/#

```

Figure : Packet lost

- ii. **Case 2:** DUT is not responding to icmp echo messages by HOST1(FAIL CASE)
Below image can be used as a reference that HOST1 is getting no response from DUT to ICMP messages sent.

```

root@6f47349eede5:/# ping -I 172.20.0.4 172.20.0.2
PING 172.20.0.2 (172.20.0.2) from 172.20.0.4 : 56(84) bytes of data.
^C
--- 172.20.0.2 ping statistics ---
16 packets transmitted, 0 received, 100% packet loss, time 15360ms
root@6f47349eede5:/#

```

Figure : 100% Packet lost

11.2 Test Case Number: 02

11.2.1. Test Case Name: TC2_PACKET_FILTERING_HOST2

11.2.2. **Test Case Description:** As per the Rules mentioned in the table, DUT should not respond to ICMP messages sent from HOST2.

11.2.3. Execution Steps: *Securing Networks*

- Check that precondition is already satisfied by the DUT.
- Use the command line of the HOST2 to ping the DUT.
- Use the following command
- ping -I <HOST2 IP Address> <DUT IP Address>**
- Capture the response on the HOST2 for the above command.

11.2.4. Test Observations:

- i. **Case 1:** DUT is not responding to ICMP echo messages by HOST2 (PASS CASE)
Below image can be used as a reference that HOST1 is getting no response from DUT to icmp messages sent.

```

root@edf2b545e90f:/# ping -I 172.20.0.3 172.20.0.2
PING 172.20.0.2 (172.20.0.2) from 172.20.0.3 : 56(84) bytes of data.
^C
--- 172.20.0.2 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11243ms
root@edf2b545e90f:/# █

```

Figure : 100% Packet Loss

- ii. **Case 2:** DUT's response is positive for the HOST2's ICMP messages (FAIL CASE)
Below image can be used as a reference that HOST2 is getting positive response from DUT to icmp messages sent.

```

root@edf2b545e90f:/# ping -I 172.20.0.3 172.20.0.2
PING 172.20.0.2 (172.20.0.2) from 172.20.0.3 : 56(84) bytes of data.
64 bytes from 172.20.0.2: icmp_seq=1 ttl=64 time=0.141 ms
64 bytes from 172.20.0.2: icmp_seq=2 ttl=64 time=0.149 ms
64 bytes from 172.20.0.2: icmp_seq=3 ttl=64 time=0.164 ms
64 bytes from 172.20.0.2: icmp_seq=4 ttl=64 time=0.154 ms
64 bytes from 172.20.0.2: icmp_seq=5 ttl=64 time=0.152 ms
64 bytes from 172.20.0.2: icmp_seq=6 ttl=64 time=0.151 ms
^C
--- 172.20.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5121ms
rtt min/avg/max/mdev = 0.141/0.151/0.164/0.006 ms
root@edf2b545e90f:/# █

```

Figure : No Packet Loss

11.3 Test Case Number: 03

11.3.1. Test Case Name: TC3_ENABLE_LOGGING

11.3.2. Test Case Description: DUT should have a functionality to enable or disable logging for each filter.

11.3.3. Execution Steps:

- i. Check that the precondition is already satisfied by the DUT.
- ii. Drop all incoming packets and enable logging for it. A sample script is added below.

NOTE: Following commands are OEM dependent

Clear existing rules

sudo iptables -F

Set default policies to DROP

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

Allow loopback traffic

sudo iptables -A INPUT -i lo -j ACCEPT

Allow established connections

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Log and drop all other incoming packets

sudo iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: " --log-level 4

sudo iptables -A INPUT -j DROP

Log and drop all forwarded packets

```
sudo iptables -A FORWARD -j LOG --log-prefix "IPTables-Dropped: " --log-level 4
sudo iptables -A FORWARD -j DROP
```

Then the DUT is pinged from another source

11.3.4. Test Observations:

- i. **CASE 1:** The desired rule which we intend to log gets logged (PASS CASE)

Command : sudo tail -n 20 /var/log/syslog | grep "IPTables-Dropped"

```
Jul 31 09:37:42 naan20-pc kernel: [241707.425111] IPTables-Dropped: IN=ens18 OUT=
= MAC=bc:24:11:06:53:c3:4a:d9:c0:2b:e7:c9:08:00 SRC=192.168.100.1 DST=192.168.10
0.15 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=43157 DF PROTO=ICMP TYPE=8 CODE=0 ID=31
898 SEQ=3
Jul 31 09:37:43 naan20-pc kernel: [241708.449143] IPTables-Dropped: IN=ens18 OUT=
= MAC=bc:24:11:06:53:c3:4a:d9:c0:2b:e7:c9:08:00 SRC=192.168.100.1 DST=192.168.10
0.15 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=43191 DF PROTO=ICMP TYPE=8 CODE=0 ID=31
898 SEQ=4
Jul 31 09:37:44 naan20-pc kernel: [241709.473070] IPTables-Dropped: IN=ens18 OUT=
= MAC=bc:24:11:06:53:c3:4a:d9:c0:2b:e7:c9:08:00 SRC=192.168.100.1 DST=192.168.10
0.15 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=43582 DF PROTO=ICMP TYPE=8 CODE=0 ID=31
898 SEQ=5
Jul 31 09:37:44 naan20-pc kernel: [241709.477728] IPTables-Dropped: IN=ens18 OUT=
= MAC= SRC=192.168.100.15 DST=224.0.0.251 LEN=73 TOS=0x00 PREC=0x00 TTL=255 ID=2
5053 DF PROTO=UDP SPT=5353 DPT=5353 LEN=53
Jul 31 09:37:45 naan20-pc kernel: [241710.496961] IPTables-Dropped: IN=ens18 OUT=
```

This is happening because the ping fails

```
root@acer2:~# ping 192.168.100.15
PING 192.168.100.15 (192.168.100.15) 56(84) bytes of data.
```

- ii. **CASE 2:** The desired rule which we intend to log is not logged (FAIL CASE)

11.4 Test Case Number: 04

11.4.1 Test Case Name: TC4_PORT_FILTERING

11.4.2 Test Case Description: DUT should have a functionality to filter on the basis of the value(s) of source IP, destination IP and port addresses of protocol header.

11.4.3 Execution Steps:

- i. Check that the precondition is already satisfied by the DUT.
- ii. First only allow a specific IP to reach the DUT on a particular port and check that DUT is reachable on that particular port.
- iii. Next disallow an IP and a particular port and next check that DUT CANNOT be reached by that IP and on that port.
- iv. Sample script to be run on DUT and Testing machine is attached below. Actual script should be provided by the OEM.

IP_TABLES CONFIGURE SCRIPT - TO BE RUN ON DUT

```
#!/bin/bash
# Define variables
ALLOWED_SRC_IP="192.168.137.15" # Allowed source IP
DISALLOWED_SRC_IP="192.168.137.157" # Disallowed source IP
PROXMOX_IP="192.168.137.96" # IP of DUT
ALLOWED_PORT="23" # Allowed port (e.g., random)
```

DISALLOWED_PORT="22" # Disallowed port (e.g., SSH)
#When wanting to test allowed change allowed to 22 and disallowed to random number
#When wanting to test disallowed, change disallowed to 22 and allowed to random number
 # Clear existing iptables rules
 echo "Flushing existing iptables rules..."
 sudo iptables -F
 # Set default policies to DROP
 echo "Setting default policies to DROP..."
 sudo iptables -P INPUT DROP
 sudo iptables -P FORWARD DROP
 sudo iptables -P OUTPUT ACCEPT
 # Allow loopback traffic
 echo "Allowing loopback traffic..."
 sudo iptables -A INPUT -i lo -j ACCEPT
 # Allow established connections
 echo "Allowing established connections..."
 sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED, RELATED -j ACCEPT
 # Allow incoming traffic from the allowed source IP
 echo "Allowing traffic from source IP: \$ALLOWED_SRC_IP"
 sudo iptables -A INPUT -s \$ALLOWED_SRC_IP -j ACCEPT
 # Allow incoming traffic to the Proxmox host on the allowed port
 echo "Allowing traffic to Proxmox IP \$PROXMOX_IP on port \$ALLOWED_PORT"
 sudo iptables -A INPUT -d \$PROXMOX_IP -p tcp --dport \$ALLOWED_PORT -j ACCEPT
 # Log and drop all incoming traffic to a specific disallowed port
 echo "Dropping traffic to Proxmox IP \$PROXMOX_IP on port \$DISALLOWED_PORT"
 sudo iptables -A INPUT -d \$PROXMOX_IP -p tcp --dport \$DISALLOWED_PORT -j LOG
 --log-prefix "IPTables-Dropped: " --log-level 4
 sudo iptables -A INPUT -d \$PROXMOX_IP -p tcp --dport \$DISALLOWED_PORT -j DROP
 # Log and drop all other incoming packets
 echo "Logging and dropping all other incoming packets..."
 sudo iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: " --log-level 4
 sudo iptables -A INPUT -j DROP
 echo "iptables rules configured successfully."

```

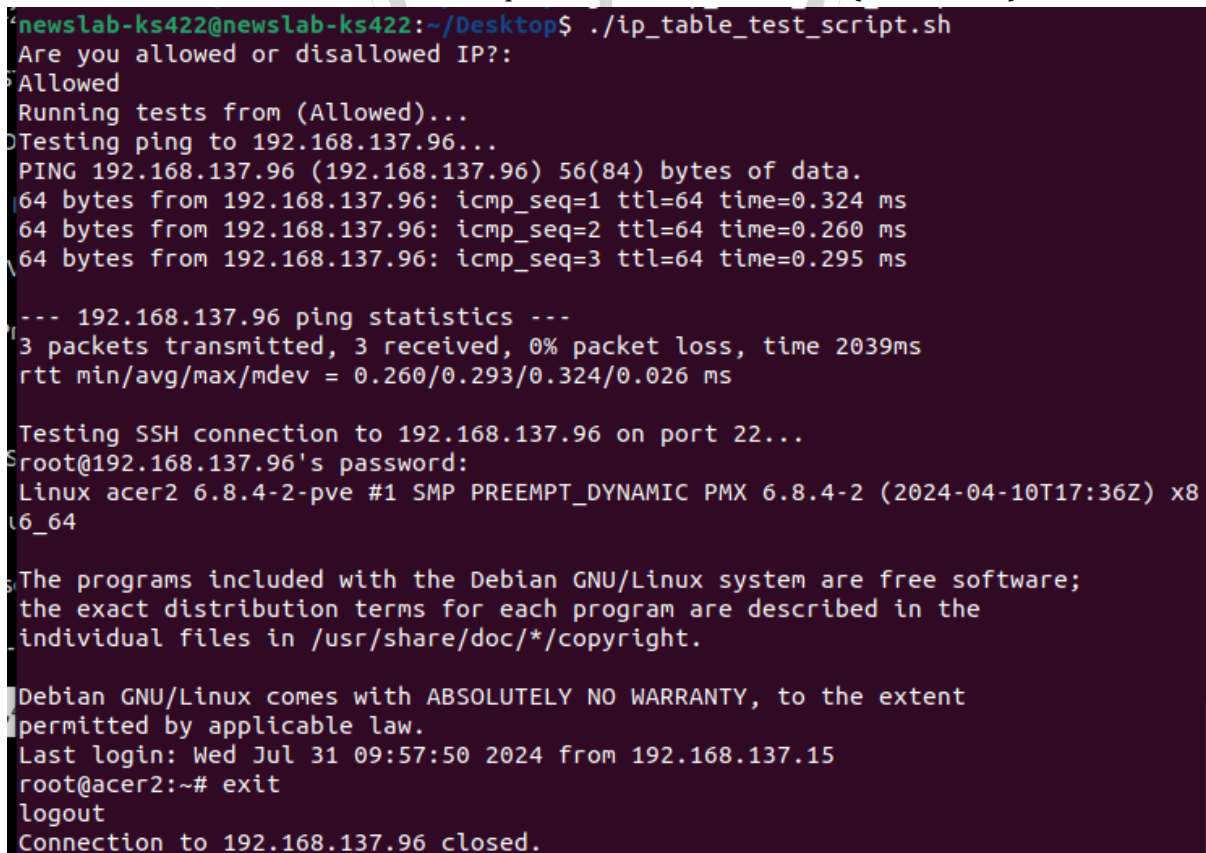
root@acer2:~# ./ip_table_bash.sh
Flushing existing iptables rules...
Setting default policies to DROP...
Allowing loopback traffic...
Allowing established connections...
Allowing traffic from source IP: 192.168.137.15
Allowing traffic to Proxmox IP 192.168.137.96 on port 22
Dropping traffic to Proxmox IP 192.168.137.96 on port 22
Logging and dropping all other incoming packets...
iptables rules configured successfully.
  
```


TESTING SCRIPT TO BE RUN ON TEST MACHINE

```
#!/bin/bash
# Define variables
PROXMOX_IP="192.168.137.96" # IP of Proxmox host
PORT="22" # Allowed/Disallowed port
echo "Are you allowed or disallowed IP?"
read name
# Function to test ping
test_ping()
{echo "Testing ping to $PROXMOX_IP..." ping -c 3 $PROXMOX_IP echo ""}
# Function to test SSH (allowed port)
test_ssh()
{echo "Testing SSH connection to $PROXMOX_IP on port $PORT..." ssh -o Connect
Timeout=5 -p $PORT root@$PROXMOX_IP || echo "SSH connection failed." echo ""}
# Execute tests
echo "Running tests from ($name) ..."
test_ping
Test_ssh
```

11.4.4 Test Observations:

- i. **CASE 1:** The allowed IP and port is able to reach DUT (PASS CASE)



```
news1ab-ks422@news1ab-ks422:~/Desktop$ ./ip_table_test_script.sh
Are you allowed or disallowed IP?:
Allowed
Running tests from (Allowed)...
Testing ping to 192.168.137.96...
PING 192.168.137.96 (192.168.137.96) 56(84) bytes of data.
64 bytes from 192.168.137.96: icmp_seq=1 ttl=64 time=0.324 ms
64 bytes from 192.168.137.96: icmp_seq=2 ttl=64 time=0.260 ms
64 bytes from 192.168.137.96: icmp_seq=3 ttl=64 time=0.295 ms

--- 192.168.137.96 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.260/0.293/0.324/0.026 ms

Testing SSH connection to 192.168.137.96 on port 22...
root@192.168.137.96's password:
Linux acer2 6.8.4-2-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.4-2 (2024-04-10T17:36Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 31 09:57:50 2024 from 192.168.137.15
root@acer2:~# exit
logout
Connection to 192.168.137.96 closed.
```

- ii. **CASE 2:** The DISALLOWED IP and port is unable to reach DUT (PASS CASE)

```
ph@pop-os:~$ ./ip_table_test.sh
Are you allowed or disallowed IP?:
Disallowed
Running tests from (Disallowed)...
Testing ping to 192.168.137.96...
PING 192.168.137.96 (192.168.137.96) 56(84) bytes of data.

--- 192.168.137.96 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2038ms

Testing SSH connection to 192.168.137.96 on port 22...
ssh: connect to host 192.168.137.96 port 22: Connection timed out
SSH connection failed.

ph@pop-os:~$
```

- iii. **CASE 3:** Any other case apart from above (FAIL CASE)

11.5 Test Case Number: 05

11.5.1. Test Case Name: TC5_ENABLE/DISABLE_FILTERING

11.5.2. Test Case Description:

- i. DUT should have a functionality to enable or disable each filter.
- ii. DUT should disable the desired rule for the corresponding filter.

11.5.3. Execution Steps:

- i. Check that the precondition is already satisfied by the DUT.
- ii. Use the command line of the HOST2 to ping the DUT.
- iii. Use the following command **iptables -L**
- iv. The list of rules will be shown in the command line shown below:

```
i.
root@4c0cc631b92b:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           icmp echo-request
ACCEPT     icmp -- ausf.test_net         anywhere              icmp echo-request
DROP       icmp -- udm.test_net          anywhere              icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

- v. use the below command to delete 2nd rule.
iptables -D INPUT -p icmp --icmp-type 8 -s 172.20.0.4 -j DROP
- vi. use the below command to see the rules listed in iptables and capture the result.
iptables -L

11.5.4. Test Observations:

- i. **CASE 1:** The desired rule which we intend to delete gets deleted (PASS CASE)
See that the second rule got deleted from the table of rules

```

root@4c0cc631b92b:/# iptables -D INPUT -p icmp --icmp-type 8 -s 172.20.0.4 -j DROP
root@4c0cc631b92b:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            icmp echo-request
ACCEPT     icmp -- ausf.test_net         anywhere               icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@4c0cc631b92b:/# █

```

- ii. **CASE 2:** The desired rule which we intend to delete is not deleted (FAIL CASE)

11.6 Test Case Number: 06

11.6.1 Test Case Name: TC6_FILTERING_COUNTER_RESET

11.6.2 Test Case Description: DUT should have a functionality to reset the counter available to count the data packet received under each rule.

11.6.3 Execution Steps:

- i. Check that precondition is already satisfied by the DUT.
- ii. Use the command below to see the current counter value for each filter in DUT.

iptables -vL

- iii. The output like this will be displayed as per the below figure.

```

root@4c0cc631b92b:/# iptables -vL
Chain INPUT (policy ACCEPT 4 packets, 397 bytes)
pkts bytes target     prot opt in     out    source                destination            icmp echo-request
 15 1260 ACCEPT     icmp -- any    any    ausf.test_net         anywhere               icmp echo-request
  8  672 DROP      icmp -- any    any    udm.test_net         anywhere               icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source                destination

Chain OUTPUT (policy ACCEPT 13 packets, 1153 bytes)
pkts bytes target     prot opt in     out    source                destination

```

- iv. Use the command below to set the counters to zero. **iptables -Z**
- v. Use the command below to see the current counter value for each filter in DUT and capture the result displayed in the command line. **iptables -vL**

11.6.4 Test Observations:

- i. **CASE 1:** The counters for each rule is set to zero after the above command is run (PASS CASE) Please see the below screen shot for Reference.

```

root@4c0cc631b92b:/# iptables -Z
root@4c0cc631b92b:/# iptables -vL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source                destination            icmp echo-request
  0  0 ACCEPT     icmp -- any    any    ausf.test_net         anywhere               icmp echo-request
  0  0 DROP      icmp -- any    any    udm.test_net         anywhere               icmp echo-request

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source                destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source                destination
root@4c0cc631b92b:/# █

```

Figure : All the Counters for the Filter Rules are set to Zero

- ii. **CASE 2:** The counter for each rule is not set to zero after the above command is run (FAIL CASE)

11.7 Test Case Number: 07

11.7.1 Test Case Name: TC7_PACKET_FILTERING_ACCOUNT

11.7.2 Test Case Description: DUT should have a functionality to ensure the matching message is accounted for i.e. a counter for the rule is incremented.

11.7.3 Execution Steps:

- i. Check that the precondition is already satisfied by the DUT.
- ii. The tester should use the command below to set up rules to log and count ICMP trafficking HOST 1.

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j LOG --log-prefix "PING REQUEST: "

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

- iii. Then From HOST2 ping HOST1.
- iv. In HOST1 check the iptables counter to see if the packets matching the rule were logged: *sudo iptables -L -v -n*
- v. Again, from HOST2 ping HOST1.
- vi. Again, in HOST1 check the counters to see if they have increased.

11.7.4 Test Observations: The counters have increased.

```

naan30@naa30-pc:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 178 packets, 41610 bytes)
 pkts bytes target    prot opt in     out     source                   destination
 5     420 ACCEPT    icmp  --  *      *       0.0.0.0/0                0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
Chain OUTPUT (policy ACCEPT 168 packets, 22592 bytes)
 pkts bytes target    prot opt in     out     source                   destination
naan30@naa30-pc:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 192 packets, 42772 bytes)
 pkts bytes target    prot opt in     out     source                   destination
10    840 ACCEPT    icmp  --  *      *       0.0.0.0/0                0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
Chain OUTPUT (policy ACCEPT 183 packets, 24602 bytes)
 pkts bytes target    prot opt in     out     source                   destination
naan30@naa30-pc:~$

newslab-ks422@newslab-ks422: ~
newslab-ks422@newslab-ks422: ~ 80x24
newslab-ks422@newslab-ks422:~$ ping 192.168.137.201
PING 192.168.137.201 (192.168.137.201) 56(84) bytes of data:
 64 bytes from 192.168.137.201: icmp_seq=1 ttl=64 time=0.587 ms
 64 bytes from 192.168.137.201: icmp_seq=2 ttl=64 time=0.544 ms
 64 bytes from 192.168.137.201: icmp_seq=3 ttl=64 time=0.456 ms
 64 bytes from 192.168.137.201: icmp_seq=4 ttl=64 time=0.514 ms
 64 bytes from 192.168.137.201: icmp_seq=5 ttl=64 time=0.548 ms
^C
--- 192.168.137.201 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4099ms
 rtt min/avg/max/mdev = 0.456/0.529/0.587/0.043 ms
newslab-ks422@newslab-ks422:~$ ping 192.168.137.201
PING 192.168.137.201 (192.168.137.201) 56(84) bytes of data:
 64 bytes from 192.168.137.201: icmp_seq=1 ttl=64 time=0.615 ms
 64 bytes from 192.168.137.201: icmp_seq=2 ttl=64 time=0.548 ms
 64 bytes from 192.168.137.201: icmp_seq=3 ttl=64 time=0.465 ms
 64 bytes from 192.168.137.201: icmp_seq=4 ttl=64 time=0.572 ms
 64 bytes from 192.168.137.201: icmp_seq=5 ttl=64 time=0.508 ms
^C
--- 192.168.137.201 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4092ms
 rtt min/avg/max/mdev = 0.465/0.541/0.615/0.051 ms

```

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL (Please see Note Below)
1	TC1_PACKET_FILTERING_HOST1	
2	TC2_PACKET_FILTERING_HOST2	
3	TC3_ENABLE/DISABLE_FILTERING	
4	TC4_FILTERING_COUNTER_RESET	
5	TC5_ENABLE/DISABLE_FILTERING	
6	TC6_FILTERING_COUNTER_RESET	
7	TC7_PACKET_FILTERING_ACCOUNT	
FINAL RESULT		

2.7.3 TSTP for Evaluation Traffic Protection –Anti-Spoofing

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no2.7.3
--	--------------------------	----------------

<DUT Details: > **SyroTech**

<DUT Software Version:> **V 3.2.02-231205**

<Digest Hash of OS>

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

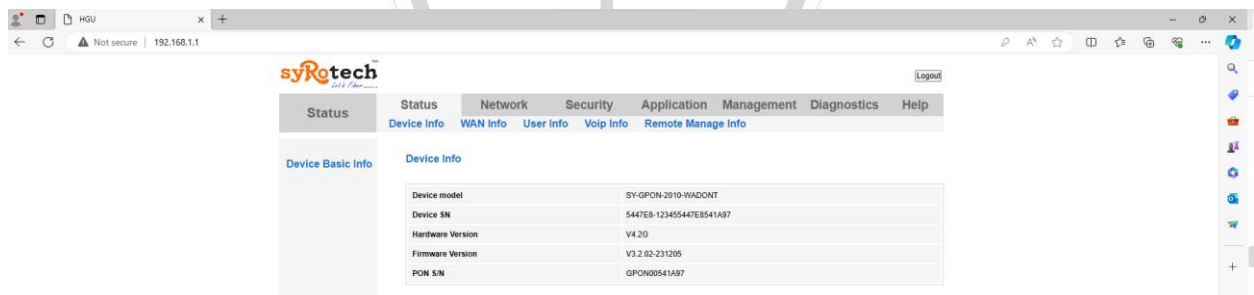
1. **ITSAR Section No & Name:** Section 7: Network Services

2. **Security Requirement No & Name:** 1.7.3: Traffic Protection –Anti-Spoofing

3. **Requirement Description:** ONT shall not process IP packets if their source address is not reachable via the incoming interface. This feature can be implemented in several ways like use of IPsec, TLS, "Reverse Path Filter" .

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. section 4.3.3.1.1]

4. DUT Confirmation Details:



5. DUT Configuration:

Below Screenshot is IP address of DUT Test Machine:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\GRL MAS> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:db8::2
    Link-local IPv6 Address . . . . . : fe80::f15:48d0:ec20:8580%5
    IPv4 Address. . . . . : 192.168.1.22
    Subnet Mask . . . . . : 255.255.255.0
    IPv4 Address. . . . . : 192.168.3.1
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 2001:db8::1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::828b:589b:918f:89ec%15
    IPv4 Address. . . . . : 192.168.1.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f620:5e07:cb37:86aa%4
    IPv4 Address. . . . . : 192.168.100.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e92b:1eeb:17bc:293a%25
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1042:cb42:a604:410e%20
    IPv4 Address. . . . . : 169.254.19.174
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 6:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::be98:ec2f:d4cc:6198%2
    IPv4 Address. . . . . : 192.168.169.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

Additionally, to ensure the connectivity between the DUT and the test machine, a ping test is conducted. This test verifies the ability to test machine to communicate with the DUT over the Ethernet connection by sending ICMP echo requests and receiving ICMP echo replies. A successful ping indicates that the network connection is established and functioning properly, enabling further testing and data transfer between the DUT and the test machine.

```
PS C:\Users\GRL MAS> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\GRL MAS>
```

6. Pre-Conditions:

A node N1 is available with:

- i. Two interfaces named respectively if1-n1 connected to the network product and if2-n1 to which the tester connects a tester machine
- ii. routing capabilities
- iii. if2-n1 has a static IP address (e.g. 192.168.3.1 belonging to the subnet 192.168.3.0/24).
- iv. A node N2 is available with:
- v. Two interfaces named respectively if1-n2 connected to the network product and if2-n2 to which the tester connects a tester machine
- vi. Routing capabilities. In particular N2 has a default route to if1-np subnet via if2-np (e.g. 192.168.2.1)
- vii. if2-n2 has a static IP address . This ip is the same as if2-n1 (e.g. 192.168.3.1 belonging to the subnet 192.168.3.0/24).
- viii. The network product has at least 2 enabled interfaces said if1-np and if2-np:
- ix. The interface if1-np is connected to interface if1-n1 of the node N1 on the subnet, e.g., 192.168.1.0/24.
- x. The interface if2-np is connected to interface if1-n2 of the node N2 on the subnet, e.g., 192.168.2.0/24.
- xi. The network product is configured with a static route for the subnet where if2-n1 is connected to (e.g. 192.168.3.0/24), so this subnet can be reached via if1-n1 through if1-np.
- xii. The vendor shall declare, in the documentation accompanying the network product, the supported anti-spoofing mechanism (e.g. RPF or similar function) and if it is enabled for all interfaces (e.g. `net.ipv4.conf.all.rp_filter = 1` and `net.ipv4.conf.default.rp_filter = 1` in the linux sysctl.conf file) or per interface bases.
- xiii. The vendor shall declare if the dropped packets can be logged and how to enable this logging.
- xiv. The tester has administrator privileges.
- xv. A tester machine is available and configured with:
- xvi. A static IP address belonging to the subnet where if2-n1 and if2-n2 are connected to (e.g. 192.168.3.2/24).
- xvii. A default gateway set to if2-n1 and if2-n2 IP Address (e.g. 192.168.3.1)
- xviii. A network traffic analyzer (e.g. tcpdump) on the network product is available

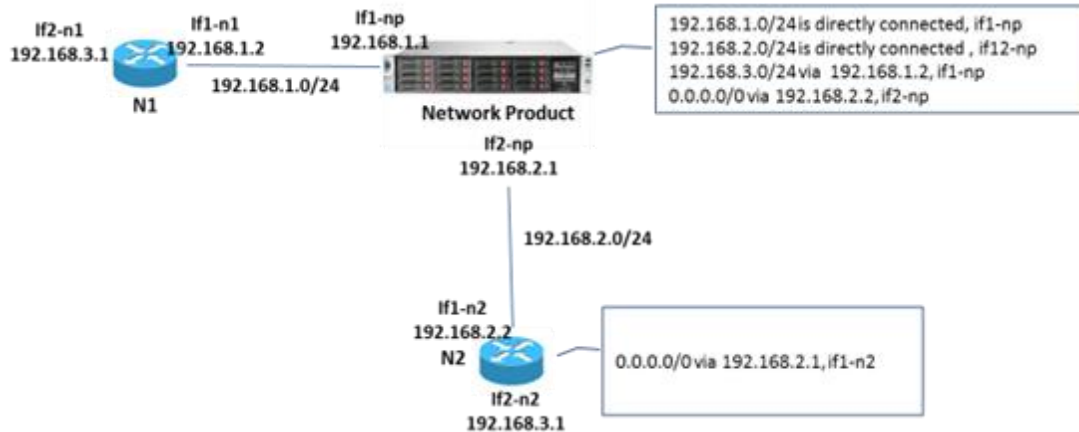
7. Test Objective: To test if the system shall not process IP Packets if their source address is not reachable via the incoming interface.

8. Test Plan:

8.1 Number of Test Scenarios: 1

8.1.1 Test to check that the system does not process IP Packets if their source address is not reachable via the incoming interface.

8.2 Testbed Diagram:



8.3 **Tools Used:** Command line , Hping3 ,Scapy

8.4 **Test Execution Steps:**

9. **Expected Results for Pass:** Host 1 will receive a 'ping' answer back, but host 2 will not.

10. **Expected Format of Evidence:** Log files and screen shots of test executions.

11. **Test Execution:**

11.1 Test Case 01

11.1.1. **Test Case Number:** 6.1

11.1.2. **Test case Name:** TC_IP_SPOOFING_MITIGATION

11.1.3. **Test Case Description:** Systems shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

11.1.4. **Execution Steps:** <REFER TO 3GPP>

- i. Tester should check the resources utilization before starting the spoofing.
- ii. Tester configures the spoofing tool and send the spoofed packets to the DUT. Here the tester is using the same ip to spoof the DUT

```
(kali㉿kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.67 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.82 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=2.49 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.68 ms
^C
— 192.168.1.1 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.439/1.818/2.486/0.355 ms

(kali㉿kali)-[~]
$ sudo hping3 --icmp --spoofer 192.168.1.1 192.168.1.1
```

- iii. Use the suitable command as per DUT to configure filtering on DUT

iv. Capture the response

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.23	192.168.1.1	ICMP	60	Echo (ping) request id=0x4125, seq=4096/16, ttl=64 (request in 3)
2	0.001864	192.168.1.1	192.168.1.23	ICMP	60	Echo (ping) reply id=0x4125, seq=4096/16, ttl=64 (reply in 1)
5	1.003494	192.168.1.23	192.168.1.1	ICMP	60	Echo (ping) request id=0x4125, seq=4352/17, ttl=64 (request in 4)
6	1.004922	192.168.1.1	192.168.1.23	ICMP	60	Echo (ping) reply id=0x4125, seq=4352/17, ttl=64 (reply in 5)
9	2.003441	192.168.1.23	192.168.1.1	ICMP	60	Echo (ping) request id=0x4125, seq=4608/18, ttl=64 (request in 18)
10	2.004354	192.168.1.1	192.168.1.23	ICMP	60	Echo (ping) reply id=0x4125, seq=4608/18, ttl=64 (reply in 9)
39	20.731594	10.0.0.1	192.168.1.1	TCP	60	1140 → 0 [RST] Seq=1 Win=512 Len=0
41	20.731556	10.0.0.1	192.168.1.1	TCP	60	1141 → 0 [RST] Seq=1 Win=512 Len=0
43	30.732520	10.0.0.1	192.168.1.1	TCP	60	1142 → 0 [RST] Seq=1 Win=512 Len=0
45	31.733286	10.0.0.1	192.168.1.1	TCP	60	1143 → 0 [RST] Seq=1 Win=512 Len=0
97	75.493890	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=0/0, ttl=64 (no response found)
99	77.493261	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=256/1, ttl=64 (no response found)
101	78.492723	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=512/2, ttl=64 (no response found)
103	79.493948	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=768/3, ttl=64 (no response found)
105	80.494565	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=1024/4, ttl=64 (no response found)
107	81.494893	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=1280/5, ttl=64 (no response found)
111	82.496215	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=1536/6, ttl=64 (no response found)
113	83.496904	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=1792/7, ttl=64 (no response found)
115	84.497175	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=2048/8, ttl=64 (no response found)
117	85.497790	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=2304/9, ttl=64 (no response found)
119	86.499181	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=2560/10, ttl=64 (no response found)
121	87.499728	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=2816/11, ttl=64 (no response found)
123	88.500798	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=3072/12, ttl=64 (no response found)
125	89.501713	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=3328/13, ttl=64 (no response found)
127	90.502368	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=3584/14, ttl=64 (no response found)
129	91.503759	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=3840/15, ttl=64 (no response found)
131	92.504191	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=4096/16, ttl=64 (no response found)
133	93.504428	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=4352/17, ttl=64 (no response found)
135	94.505436	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=4608/18, ttl=64 (no response found)
137	95.505908	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=4864/19, ttl=64 (no response found)
139	96.506908	192.168.1.1	192.168.1.1	ICMP	60	Echo (ping) request id=0x5328, seq=5120/20, ttl=64 (no response found)

11.1.5.Test Observation: The tester observed that the DUT is not responding to the spoofed packets, even if using the same ip and DUT is replying to the normal requests.

11.1.6.Evidence Provided: The screenshots of the Wireshark outcome are attached.

12. Test case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_IP_Packets_And_Incoming_Interface		

Section 8: Attack Prevention Mechanisms

2.8.1 TSTP For Network Level and application-level DDoS

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.8.1
--	--------------------------	-----------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 8 – Attack Prevention Mechanisms

2. **<Security Requirement No & Name >** 1.8.1 Network Level and application-level DDoS

3. **<Requirement Description: >** ONU/ONT shall have protection mechanism against network level and Application-level DDoS attacks. ONU/ONT shall provide security measures to deal with overload situations which may occur as a result of a denial-of-service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Any one or more of the following protective measures can be used, but not limited to the following.

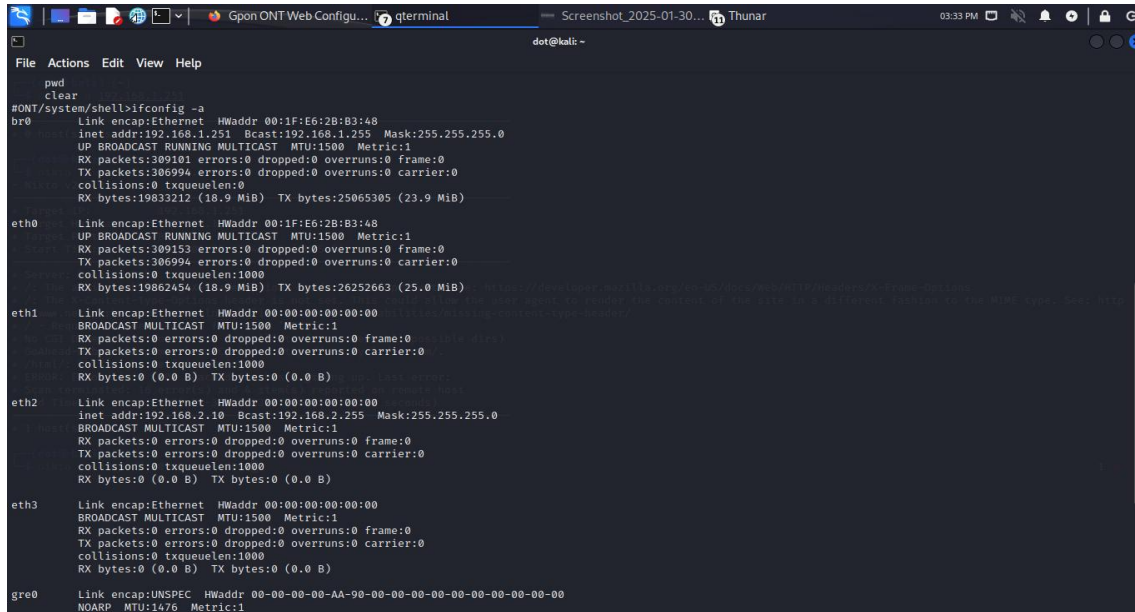
- i. Restricting of available RAM per application
- ii. Restricting of maximum sessions for a Web application
- iii. Defining the maximum size of a dataset
- iv. Restricting CPU resources per process
- v. Prioritizing processes
- vi. Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- vii. Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.3.1]

4. DUT Confirmation Details:

- i. Use the command line interface to get details of the machine on which test is conducted.
- ii. Use command to get Interfaces details

- iii. Use command to get Application No/Version No & Kernel Info
Command used: **ifconfig -a** (To find IP information and all interfaces)



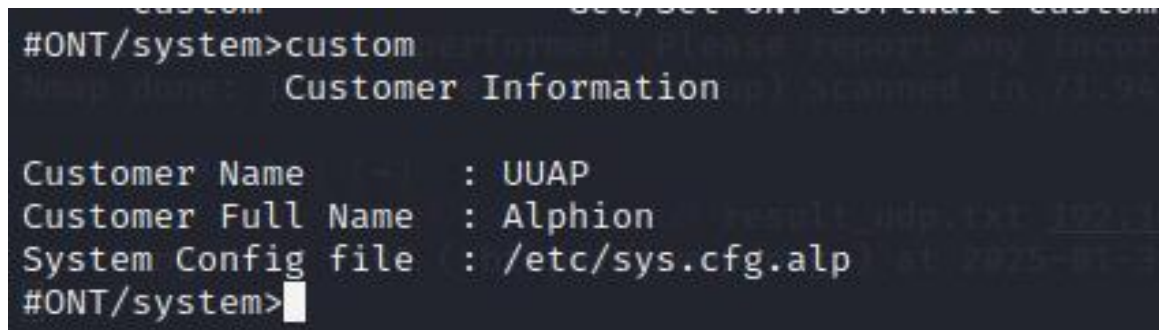
```
dot@kali: ~  
File Actions Edit View Help  
pwd  
clear  
#ONT/system/shell>ifconfig -a  
br0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:389101 errors:0 dropped:0 overruns:0 frame:0  
TX packets:386994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)  
  
eth0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:389153 errors:0 dropped:0 overruns:0 frame:0  
TX packets:386994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)  
  
eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
gre0: Link encap:UNSPEC HWaddr 00-00-00-00-AA-9A-00-00-00-00-00-00-00-00-00-00-00  
NOARP MTU:1476 Metric:1
```

The below screenshot shows the firmware version of the DUT



```
#ONT/system>ontver  
OntSwVer N: R2.0.9.6  
#ONT/system>
```

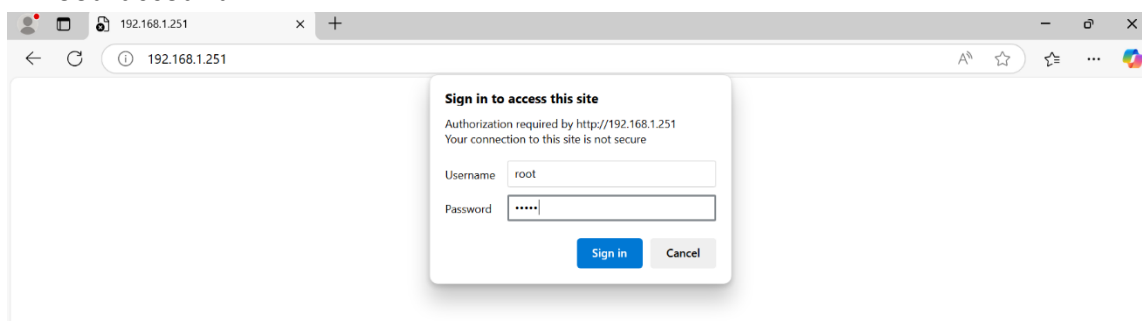
The below screenshot shows the information of the DUT



```
#ONT/system>custom  
Customer Information  
  
Customer Name : UUAP  
Customer Full Name : Alphion  
System Config file : /etc/sys.cfg.alp  
#ONT/system>
```

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



iii. Verify the DUT information through device info

The screenshot shows the 'GPON ONT' web configuration interface. The left sidebar has a menu with 'Status' (selected), 'Device Info', 'WAN Status', 'Network', 'Advanced', and 'Maintain'. The main content area is titled 'Status > Device Info' and 'Device Info'. It displays a table with the following information:

Equipment ID:	00142-00029-43
Hardware Version:	02
Software Version:	R2.0.9.6
Build Date:	2017-09-11
MAC Address	00-1F-E6-2B-B3-48
Current Time	2000-01-01 00:29:55

iv. Set the static IP address

The first screenshot shows the 'GPON ONT' web configuration interface with the 'Network > WAN' section selected. The 'WAN' tab is active. The 'Internet Connection Type' is set to 'Static IP'. The configuration fields are as follows:

Internet Connection Type	Static IP			
IP Address	168	2	10	
Subnet Mask	255	255	0	
Default Gateway	192	168	2	1
DNS Server 1	192	168	2	10
DNS Server 2	192	168	2	11

Buttons for 'Apply' and 'Refresh' are at the bottom right.

The second screenshot shows the 'GPON ONT' web configuration interface with the 'Status > WAN Status' section selected. The 'WAN Status' tab is active. It displays a table with the following information:

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

A 'Refresh' button is at the bottom right.

6. Preconditions:

- A document which provides a detailed technical description of the overload control mechanisms.
- Test results from a test execution phase of overload control mechanism testing.

7. Test Objective/ Purpose:

- Verify that the network product:
- has a detailed technical description of the overload control mechanisms used to deal with overload scenarios;
- has test results verifying the operation of the overload control mechanisms.

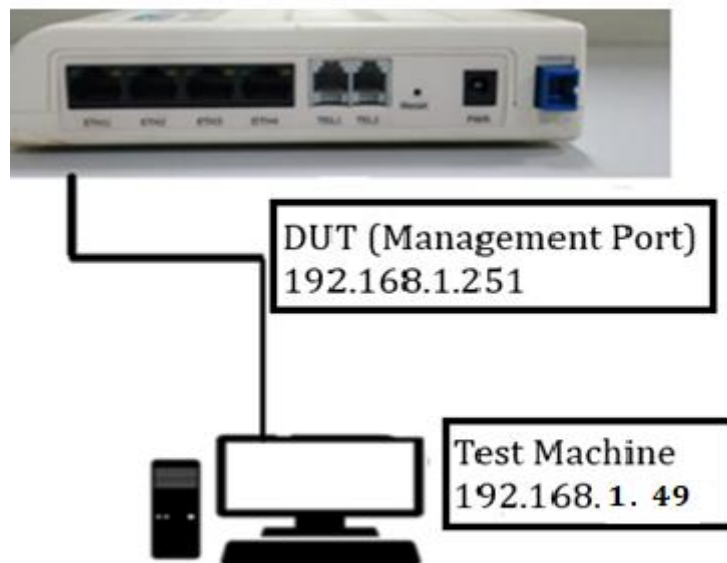
8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for Excessive Overload Protection due to Network Level DDOS Attack:

8.1.2 This test scenario stimulates Network Level DDOS attack due to which CPU and memory overload is caused, it then verifies whether the network product reacts in a controlled way during it or not. (Additional Test scenarios based on the OEM document) .

8.2 Test Bed Diagram:



8.3 Tools required: Command Line Interface, hping3.

8.4 Test Execution Step:

- a. The tester verifies that there is:
 - i. A technical description providing a high-level overview of the overload control design.
 - ii. An overview of the types of overload scenarios that the network product overload control mechanisms are expected to handle.
 - iii. An overview of the overload control thresholds that the network product uses to trigger overload control mechanisms.
 - iv. Description of the types of attacks that may cause an overload to the network product and how these are handled.
 - v. A description of how the network product discards or handles input during various overload situations including excessive overloads. i.e. where the overload is significantly greater than the thresholds where overload detection is triggered.
 - vi. A description of how the network product security functions operate and perform during overload.
 - vii. A description of how the network product shuts down or performs or takes other abatement or corrective actions during excessive overload conditions.

- b. The tester performs below steps:
 - i. Introduce a controlled DDOS scenario with predefined levels of load and traffic.
 - ii. Observe the Network Product's response and measure how it adjusts its resource allocation and prioritization to handle the increased load.
 - iii. Validate that the NF does not crash or suffer from critical failures due to the attack.
 - iv. Assess if the NF can dynamically adapt its behavior based on the severity of the attack.
 - v. Verify that the NF can smoothly recover and return to normal operation after the attack is removed.
- c. The tester verifies that the test results:
 - i. Contain details of the overload conditions used in the test execution that are consistent with the technical description document.
 - ii. Describe test procedures used to verify the overload control mechanisms.
 - iii. Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
 - iv. Contain details of the test set-up including the mechanisms for creating the overload. Where simulators and/or scripts are used to artificially create a load then details of these should also be included.

9. Expected Results:

- i. A technical description provides a high-level overview of the overload control design.
- ii. An overview of the types of overload scenarios and overload control thresholds that are considered.
- iii. Description on the types of attacks that may cause an overload to the system and how these are handled.
- iv. A description of how the network product discards or handles input during various overload situations.
- v. Describes if or how the network product security functions operate and perform during overload.
- vi. If parts of the system shutdown or take other abatement or corrective actions these should be described.

Note: If some of the items listed above are not applicable to a network product then, in those cases, it should be clarified by the vendor why these items are not applicable.

- a. The test results should:
 - i. Contain details of the overload conditions used in the test execution that are consistent with the technical description document.

- ii. Describe the test procedures used to verify the overload control mechanisms.
- iii. Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
- iv. Contain details of the test set-up including the mechanisms for creating the overload.

10. Expected Format of Evidence: Documentation showing each of the points in the results sections.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC1_NETWORK_LEVEL_DDOS

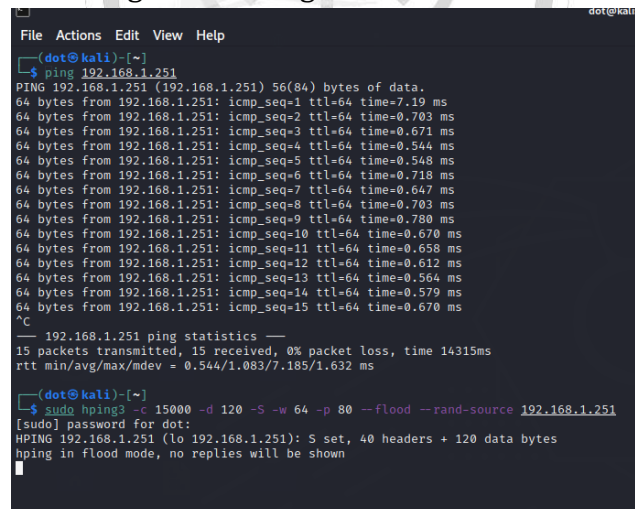
11.1.2. Test Case Description: Test needs to be conducted to verify that the Network Product can react to the Network Level DDOS in a controlled manner.

11.1.3. Execution Steps: Create an overload scenario, in this example we'll use 'hping3' to simulate high CPU and memory usage.

Run command: ***sudo hping3 -c 15000 -d 120 -S -w 64 -p <port-number> --flood --rand-source <ip-address>***

'hping3' will flood ping attack to the specified IP address.

This command will generate a significant load on both the CPU and memory.



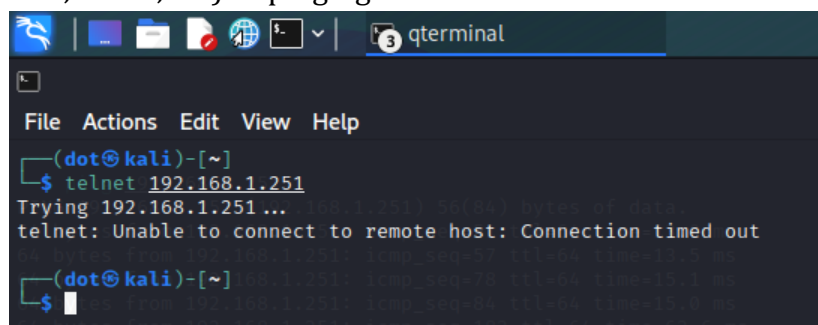
```

(dot@kali)-[~]
└─$ ping 192.168.1.251
PING 192.168.1.251 (192.168.1.251) 56(84) bytes of data:
64 bytes from 192.168.1.251: icmp_seq=1 ttl=64 time=7.19 ms
64 bytes from 192.168.1.251: icmp_seq=2 ttl=64 time=0.703 ms
64 bytes from 192.168.1.251: icmp_seq=3 ttl=64 time=0.671 ms
64 bytes from 192.168.1.251: icmp_seq=4 ttl=64 time=0.544 ms
64 bytes from 192.168.1.251: icmp_seq=5 ttl=64 time=0.548 ms
64 bytes from 192.168.1.251: icmp_seq=6 ttl=64 time=0.718 ms
64 bytes from 192.168.1.251: icmp_seq=7 ttl=64 time=0.647 ms
64 bytes from 192.168.1.251: icmp_seq=8 ttl=64 time=0.703 ms
64 bytes from 192.168.1.251: icmp_seq=9 ttl=64 time=0.780 ms
64 bytes from 192.168.1.251: icmp_seq=10 ttl=64 time=0.670 ms
64 bytes from 192.168.1.251: icmp_seq=11 ttl=64 time=0.658 ms
64 bytes from 192.168.1.251: icmp_seq=12 ttl=64 time=0.612 ms
64 bytes from 192.168.1.251: icmp_seq=13 ttl=64 time=0.564 ms
64 bytes from 192.168.1.251: icmp_seq=14 ttl=64 time=0.579 ms
64 bytes from 192.168.1.251: icmp_seq=15 ttl=64 time=0.670 ms
^C
— 192.168.1.251 ping statistics —
15 packets transmitted, 15 received, 0% packet loss, time 14315ms
rtt min/avg/max/mdev = 0.544/1.083/7.185/1.632 ms

(dot@kali)-[~]
└─$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.251
[sudo] password for dot:
HPING 192.168.1.251 (lo 192.168.1.251): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown

```

During the DoS attack tester try to access the DUT services such as remote login (eg - ssh, telnet, etc) or pinging the DUT.



```

(dot@kali)-[~]
└─$ telnet 192.168.1.251
Trying 192.168.1.251 ...
telnet: Unable to connect to remote host: Connection timed out

(dot@kali)-[~]
└─$ ping 192.168.1.251
PING 192.168.1.251 (192.168.1.251) 56(84) bytes of data:
64 bytes from 192.168.1.251: icmp_seq=1 ttl=64 time=15.1 ms
64 bytes from 192.168.1.251: icmp_seq=2 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=3 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=4 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=5 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=6 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=7 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=8 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=9 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=10 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=11 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=12 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=13 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=14 ttl=64 time=15.0 ms
64 bytes from 192.168.1.251: icmp_seq=15 ttl=64 time=15.0 ms
^C
— 192.168.1.251 ping statistics —
15 packets transmitted, 15 received, 0% packet loss, time 14315ms
rtt min/avg/max/mdev = 0.544/1.083/7.185/1.632 ms

```

Open a new terminal and run command: **top** (this command is OEM dependent)
While 'hping3' is running, 'top' will display the CPU and memory usage of the system. Observe how the CPU usage increases due to the workload.

```

File Actions Edit View Help

Mem: 32364K used, 11284K free, 0K shrd, 4752K buff, 12476K cached
CPU:  0% usr 2% sys 0% nice 96% idle 0% io 0% irq 0% softirq
Load average: 2.08 3.25 3.08

PID PPID USER STAT VSZ %MEM %CPU COMMAND
271 221 root S 4666 11% 2% /bin/MecMgr -p 20 -s 0
1977 1976 root R 1100 3% 1% top
221 1 root S 1796 4% 0% Ssp
439 271 root S 4666 11% 0% /bin/MecMgr -p 20 -s 0
440 439 root S 4666 11% 0% /bin/MecMgr -p 20 -s 0
260 259 root S < 3276 7% 0% /bin/VmrMgr -p 10 -s 0
258 221 root S < 3276 7% 0% /bin/VmrMgr -p 10 -s 0
499 259 root S < 3276 7% 0% /bin/VmrMgr -p 10 -s 0
259 258 root S < 3276 7% 0% /bin/VmrMgr -p 10 -s 0
491 259 root S < 3276 7% 0% /bin/VmrMgr -p 10 -s 0
512 259 root S < 3276 7% 0% /bin/VmrMgr -p 10 -s 0
262 221 root S 3108 7% 0% /bin/EthMgr -p 20 -s 0
270 269 root S 2912 7% 0% /bin/WebMgr -p 20 -s 0
264 221 root S 2912 7% 0% /bin/WebMgr -p 20 -s 0
269 264 root S 2912 7% 0% /bin/WebMgr -p 20 -s 0
255 221 root S 2908 7% 0% /bin/PonMgr -p 20 -s 0
453 255 root S 2908 7% 0% /bin/PonMgr -p 20 -s 0
454 453 root D < 2908 7% 0% /bin/PonMgr -p 20 -s 0
452 255 root D 2908 7% 0% /bin/PonMgr -p 20 -s 0
261 221 root S 2572 6% 0% /bin/IpPath -p 20 -s 0

```

and MEM% can be seen lesser which is

```

File Actions Edit View Help
Mem: 35436K used, 8212K free, 0K shrd, 4752K buff, 12476K cached
CPU:  2% usr  5% sys  0% nice  1% idle  0% io  2% irq 89% softirq
Load average: 4.96 3.75 3.26

```

PID	PPID	USER	STAT	VSZ	%MEM	%CPU	COMMAND
271	221	root	R	4660	11%	56%	/bin/MecMgr -p 20 -s 0
1977	1976	root	R	1100	3%	11%	top
226	225	root	S <	1808	4%	4%	/bin/TimerMgr -p 10 -s 0
498	5	root	SW<	0	0%	4%	[brdg_wkq/0]
499	259	root	S <	3276	7%	2%	/bin/VmrMgr -p 10 -s 0
260	259	root	S <	3276	7%	2%	/bin/VmrMgr -p 10 -s 0
2	1	root	RWN	0	0%	2%	[ksoftirqd/0]
494	5	root	SW<	0	0%	2%	[voip_isr/0]
179	5	root	SW<	0	0%	1%	[voshwtimer/0]
221	1	root	S	1796	4%	1%	Ssp
264	221	root	S	2912	7%	1%	/bin/WebMgr -p 20 -s 0
262	221	root	S	3108	7%	0%	/bin/EthMgr -p 20 -s 0
263	221	root	S	1940	4%	0%	/bin/HpnaMgr -p 20 -s 0
256	221	root	S	1900	4%	0%	/bin/NetMgr -p 20 -s 0
227	221	root	S	1764	4%	0%	/bin/LogMgr -p 20 -s 0
258	221	root	S <	3276	7%	0%	/bin/VmrMgr -p 10 -s 0
270	269	root	S	2912	7%	0%	/bin/WebMgr -p 20 -s 0
255	221	root	S	2908	7%	0%	/bin/PonMgr -p 20 -s 0
453	255	root	S	2908	7%	0%	/bin/PonMgr -p 20 -s 0

```

^[[A^[[A^[[A^[[A^[[A^[[A#ONT/system/shell> /bin/TimerMgr -p 10 -s 0

```

- i. Monitor the DUT performance, response times, and behavior during the overload simulation.
- ii. Validate that the network product reacts to the overload in a controlled manner and prioritizes critical tasks. (The expected behavior of the network product shall be provided in the OEM Documentation)

- iii. Observe how the network product's security functions operate and perform during the overload.
- iv. **Note:** While hping3 is primarily used for network-level attacks, it can also simulate **application-level attacks** by targeting specific application protocols (such as HTTP) and exploiting the behavior of the application.

11.2 Test Case Number: 02

11.2.1. Test Case Name: TC2_APPLICATION_LEVEL_DDOS

Use below command to launch application level HTTP attack:

```
sudo hping3 -S -p 80 --faster --url /index.html --flood --rand-source <target-ip>
```

Rest of the steps for monitoring are the same as Network Level Attacks.

11.2.2. Test Observation:

- i. **Case 1:** The network product reacts in a controlled way during overload (**Positive TestCase**) The network product demonstrates a controlled response to the simulated DDOS Attack. It prioritizes critical tasks, maintains essential functions, and keeps security functions operational during the overload scenario. Then the test case Passes.
- ii. **Case 2:** The network product reacts in an uncontrolled way during overload (**Negative TestCase**) If the network product exhibits unpredictable behavior, crashes, or fails to maintain its security functions during DDOS, it will be considered a failure.

11.2.3. **Evidence Provided:** Documentation showing each of the points in the results sections.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC1_NETWORK_LEVEL_DDOS		
2.	TC2_APPLICATION_LEVEL_DOS		

2.8.2 TSTP for Excessive Overload Protection

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.8.2
---	--------------------------	-----------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

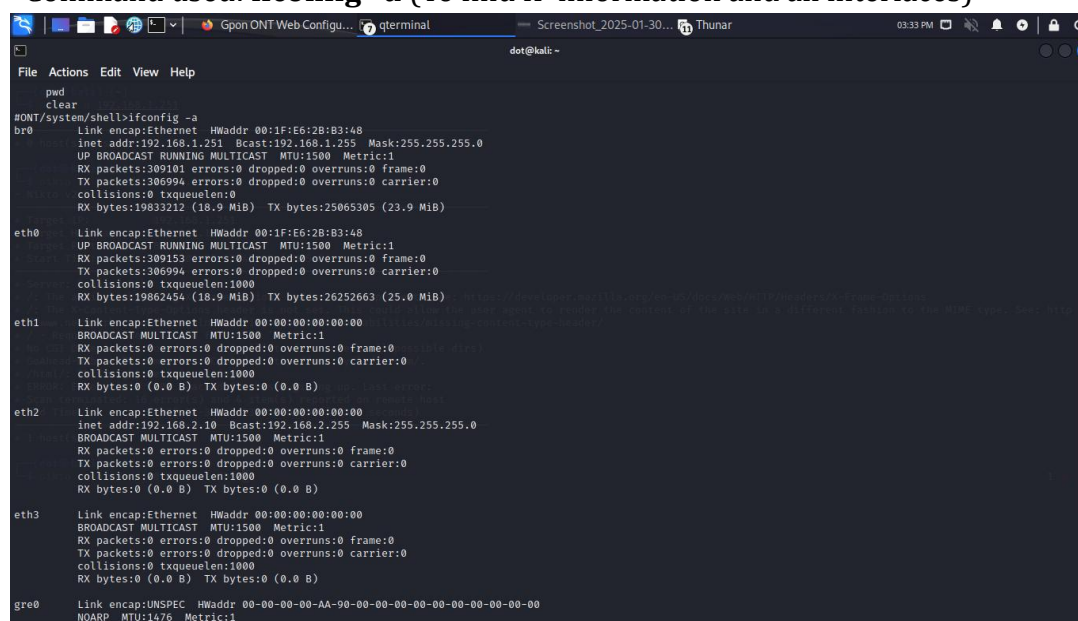
- i. <ITSAR Section No & Name> Section 8 – Attack Prevention Mechanisms
- ii. <Security Requirement No & Name > 1.8.2 Excessive Overload Protection
- iii. <Requirement Description: > The ONU/ONT may provide security measures to deal with overload situations which may occur during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.3.3]

iv. DUT Confirmation Details:

- i. Use the command line interface to get details of the machine on which test is conducted.
- ii. Use command to get Interfaces details
- iii. Use command to get Application No/Version No & Kernel Info

- Command used: **ifconfig -a** (To find IP information and all interfaces)



```
dot@kali:~$ ifconfig -a
br0: flags=4096<BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.251 netmask 255.255.255.0
    ether 00:1f:e6:28:b3:48
    RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
    TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)

eth0: flags=4096<BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.10 netmask 255.255.255.0
    ether 00:1f:e6:28:b3:48
    RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
    TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)

eth1: flags=4096<BROADCAST,MULTICAST> mtu 1500
    ether 00:00:00:00:00:00
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth2: flags=4096<BROADCAST,MULTICAST> mtu 1500
    inet 192.168.2.10 netmask 255.255.255.0
    ether 00:00:00:00:00:00
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth3: flags=4096<BROADCAST,MULTICAST> mtu 1500
    ether 00:00:00:00:00:00
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

gre0: flags=8010<LOOPBACK,UP,LOWER_UP> mtu 1476
    inet 127.0.0.1 netmask 255.255.255.0
    ether 00:00:00:00:00:00
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>
```

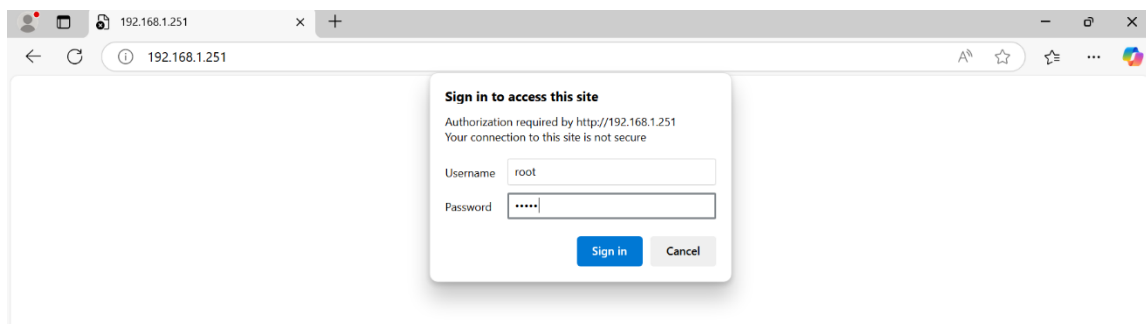
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

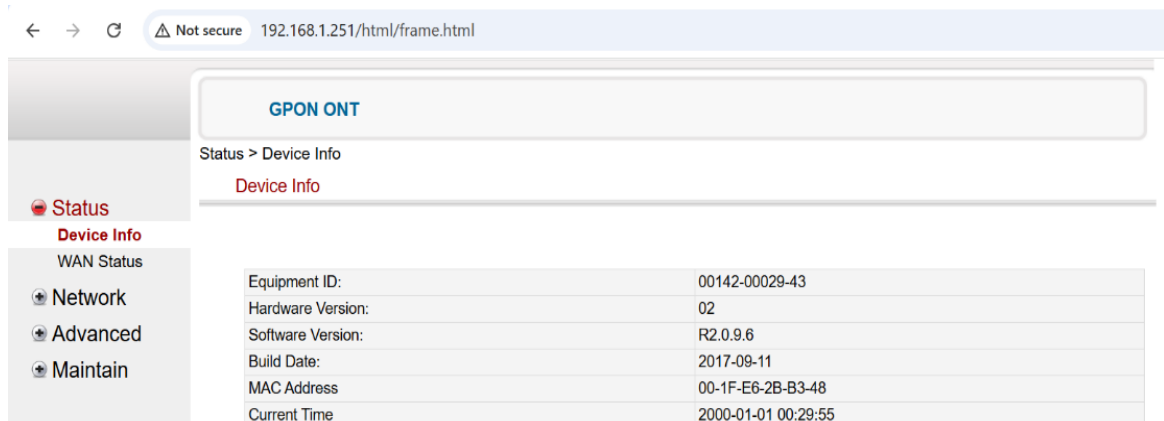
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

v. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address

GPON ONT Web Configuration - Network > WAN

Internet Connection Type: **Static IP**

IP Address	192	168	2	10
Subnet Mask	255	255	0	
Default Gateway	192	168	2	1
DNS Server 1	192	168	2	10
DNS Server 2	192	168	2	11

GPON ONT Web Configuration - Status > WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

vi. **Preconditions:**

- i. A document which provides a detailed technical description of the overload control mechanisms.
- ii. Test results from a test execution phase of overload control mechanism testing.

vii. **Test Objective/ Purpose:** Verify that the network product:

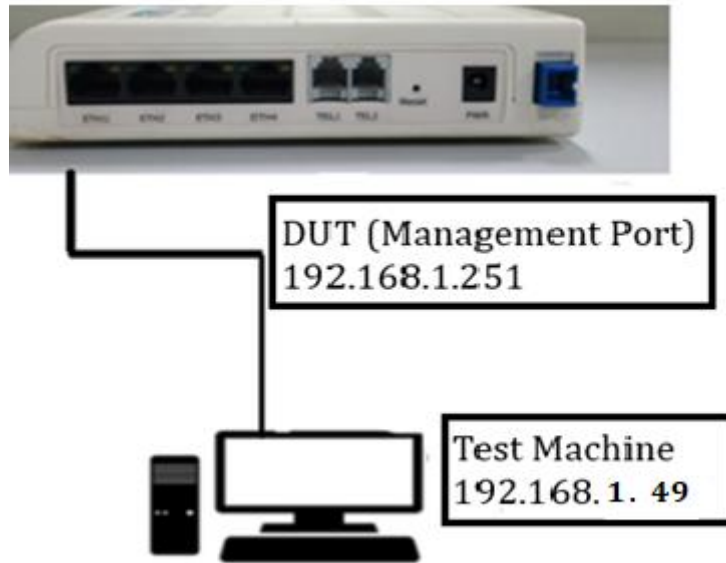
- i. has a detailed technical description of the overload control mechanisms used to deal with overload scenarios;
- ii. has test results verifying the operation of the overload control mechanisms.

viii. **Test Plan:**

8.1 **Number of Test Scenarios:**

8.1.1 **Test Scenario for Excessive Overload Protection due to CPU Overload:** This test scenario stimulates overload conditions in which CPU overload is performed and verifies whether the network product reacts in a controlled way during it. (Additional Test scenarios based on the OEM document)

8.2 **Test Bed Diagram:**



8.3 Tools required: Command Line Interface, hping3 and other tools for overload simulation based on documentation.

8.4 Test Execution Step:

A. The tester verifies that there is:

- i. A technical description providing a high-level overview of the overload control design.
- ii. An overview of the types of overload scenarios that the network product overload control mechanisms are expected to handle.
- iii. An overview of the overload control thresholds that the network product uses to trigger overload control mechanisms.
- iv. Description of the types of attacks that may cause an overload to the network product and how these are handled.
- v. A description of how the network product discards or handles input during various overload situations including excessive overloads. i.e. where the overload is significantly greater than the thresholds where overload detection is triggered.
- vi. A description of how the network product security functions operate and perform during overload.
- vii. A description of how the network product shuts down or performs or takes other abatement or corrective actions during excessive overload conditions.

B. The tester performs below steps:

- i. Introduce a controlled overload scenario with predefined levels of load and traffic.
- ii. Observe the Network Product's response and measure how it adjusts its resource allocation and prioritization to handle the increased load.
- iii. Validate that the DUT does not crash or suffer from critical failures due to the controlled overload.

- iv. Assess if the DUT can dynamically adapt its behaviour based on the severity of the overload situation.
- v. Verify that the DUT can smoothly recover and return to normal operation after the controlled overload is removed.

C. The tester verifies that the test results:

- i. Contain details of the overload conditions used in the test execution that are consistent with the technical description document.
- ii. Describe test procedures used to verify the overload control mechanisms.
- iii. Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
- iv. Contain details of the test set-up including the mechanisms for creating the overload. Where simulators and/or scripts are used to artificially create a load then details of these should also be included.

ix. **Expected Results:**

- i. A technical description provides a high-level overview of the overload control design.
 - ii. An overview of the types of overload scenarios and overload control thresholds that are considered.
 - iii. Description on the types of attacks that may cause an overload to the system and how these are handled.
 - iv. A description of how the network product discards or handles input during various overload situations.
 - v. Describes if or how the network product security functions operate and perform during overload.
 - vi. If parts of the system shutdown or take other abatement or corrective actions these should be described.
- **Note:** If some of the items listed above are not applicable to a network product then, in those cases, it should be clarified by the vendor why these items are not applicable.

a. The test results should:

- i. Contain details of the overload conditions used in the test execution that are consistent with the technical description document.
- ii. Describe the test procedures used to verify the overload control mechanisms.
- iii. Contain data which demonstrates/indicates that the overload control mechanisms described in the technical description document have been implemented.
- iv. Contain details of the test set-up including the mechanisms for creating the overload.

- x. **Expected Format of Evidence:** Documentation showing each of the points in the results sections.

xi. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC1_EXCESSIVE_OVERLOAD_PROTECTION

11.1.2. Test Case Description: Test needs to be conducted to verify that the Network Product can react to an overload situation in a controlled manner.

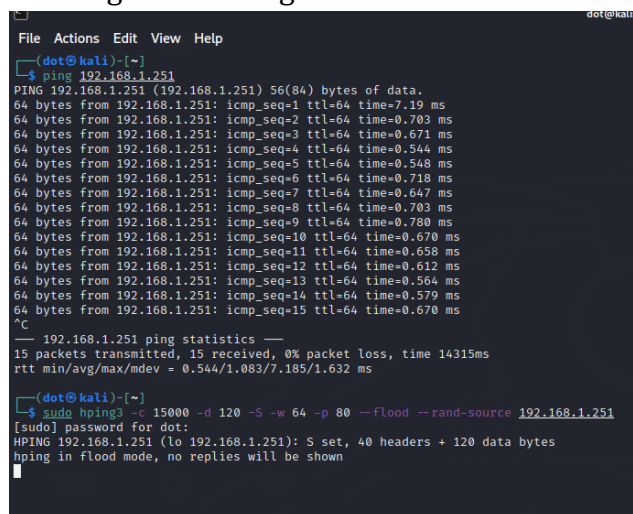
11.1.3. Execution Steps:

- Create an overload scenario, in this example we'll use 'hping3' to simulate high CPU and memory usage.

Run command:

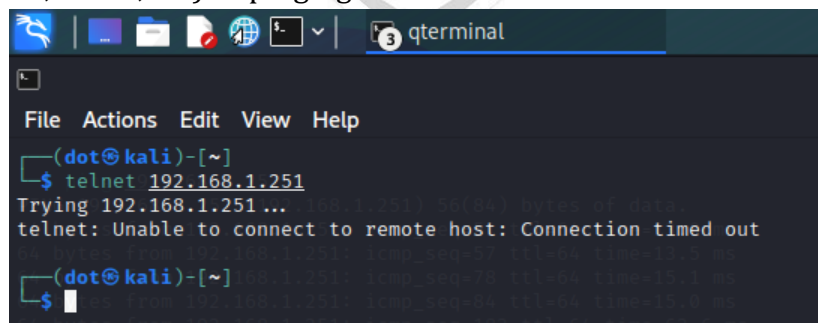
sudo hping3 -c 15000 -d 120 -S -w 64 -p <port-number> --flood --rand-source <ip-address>

'hping3' will flood ping attack to the specified IP address. This command will generate a significant load on both the CPU and memory.



```
File Actions Edit View Help
(dot@kali) [~]
$ ping 192.168.1.251
PING 192.168.1.251 (192.168.1.251) 56(84) bytes of data:
64 bytes from 192.168.1.251: icmp_seq=1 ttl=64 time=7.19 ms
64 bytes from 192.168.1.251: icmp_seq=2 ttl=64 time=0.703 ms
64 bytes from 192.168.1.251: icmp_seq=3 ttl=64 time=0.671 ms
64 bytes from 192.168.1.251: icmp_seq=4 ttl=64 time=0.544 ms
64 bytes from 192.168.1.251: icmp_seq=5 ttl=64 time=0.548 ms
64 bytes from 192.168.1.251: icmp_seq=6 ttl=64 time=0.718 ms
64 bytes from 192.168.1.251: icmp_seq=7 ttl=64 time=0.647 ms
64 bytes from 192.168.1.251: icmp_seq=8 ttl=64 time=0.703 ms
64 bytes from 192.168.1.251: icmp_seq=9 ttl=64 time=0.780 ms
64 bytes from 192.168.1.251: icmp_seq=10 ttl=64 time=0.670 ms
64 bytes from 192.168.1.251: icmp_seq=11 ttl=64 time=0.658 ms
64 bytes from 192.168.1.251: icmp_seq=12 ttl=64 time=0.612 ms
64 bytes from 192.168.1.251: icmp_seq=13 ttl=64 time=0.564 ms
64 bytes from 192.168.1.251: icmp_seq=14 ttl=64 time=0.579 ms
64 bytes from 192.168.1.251: icmp_seq=15 ttl=64 time=0.670 ms
^C
  192.168.1.251 ping statistics ---
  15 packets transmitted, 15 received, 0% packet loss, time 14315ms
 rtt min/avg/max/mdev = 0.544/1.083/7.185/1.632 ms
(dot@kali) [~]
$ sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.251
[sudo] password for dot:
HPING 192.168.1.251 (lo 192.168.1.251): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

During the DoS attack tester try to access the DUT services such as remote login (eg - ssh, telnet, etc) or pinging the DUT.



```
File Actions Edit View Help
(dot@kali) [~]
$ telnet 192.168.1.251
Trying 192.168.1.251 ...
telnet: Unable to connect to remote host: Connection timed out
(dot@kali) [~]
$
```

- During the overload simulation, we'll use 'top' to monitor the system's CPU and memory usage in real-time.
- Open a new terminal and run command: **top**
This will display the CPU and memory usage of the system. Observe how the CPU usage increases due to the workload.

Before Attack:

```

File Actions Edit View Help
Mem: 32364K used, 11284K free, 0K shrd, 4752K buff, 12476K cached
CPU:  0% usr  2% sys  0% nice 96% idle  0% io  0% irq  0% softirq
Load average: 2.08 3.25 3.08
  PID  PPID  USER      STAT  VSZ  %MEM  %CPU  COMMAND
  271   221  root       S      4660  11%   2%   /bin/MecMgr -p 20 -s 0
 1977  1976  root       R      1100   3%   1%   top
  221    1  root       S      1796   4%   0%   Ssp
  439   271  root       S      4660  11%   0%   /bin/MecMgr -p 20 -s 0
  440   439  root       S      4660  11%   0%   /bin/MecMgr -p 20 -s 0
  260   259  root       S <    3276   7%   0%   /bin/VmrMgr -p 10 -s 0
  258   221  root       S <    3276   7%   0%   /bin/VmrMgr -p 10 -s 0
  499   259  root       S <    3276   7%   0%   /bin/VmrMgr -p 10 -s 0
  259   258  root       S <    3276   7%   0%   /bin/VmrMgr -p 10 -s 0
  491   259  root       S <    3276   7%   0%   /bin/VmrMgr -p 10 -s 0
  512   259  root       S <    3276   7%   0%   /bin/VmrMgr -p 10 -s 0
  262   221  root       S      3108   7%   0%   /bin/EthMgr -p 20 -s 0
  270   269  root       S      2912   7%   0%   /bin/WebMgr -p 20 -s 0
  264   221  root       S      2912   7%   0%   /bin/WebMgr -p 20 -s 0
  269   264  root       S      2912   7%   0%   /bin/WebMgr -p 20 -s 0
  255   221  root       S      2908   7%   0%   /bin/PonMgr -p 20 -s 0
  453   255  root       S      2908   7%   0%   /bin/PonMgr -p 20 -s 0
  454   453  root       D <    2908   7%   0%   /bin/PonMgr -p 20 -s 0
  452   255  root       D      2908   7%   0%   /bin/PonMgr -p 20 -s 0
  261   221  root       S      2572   6%   0%   /bin/IpPath -p 20 -s 0

```

here CPU% and MEM% can be seen lesser which increases post the attack is launched.

After Attack:

```

File Actions Edit View Help
Mem: 35436K used, 8212K free, 0K shrd, 4752K buff, 12476K cached
CPU:  2% usr  5% sys  0% nice  1% idle  0% io  2% irq 89% softirq
Load average: 4.96 3.75 3.26
  PID  PPID  USER      STAT  VSZ  %MEM  %CPU  COMMAND
  271   221  root       R      4660  11%  56%   /bin/MecMgr -p 20 -s 0
 1977  1976  root       R      1100   3%  11%   top
  226   225  root       S <    1808   4%   4%   /bin/TimerMgr -p 10 -s 0
  498    5  root       SW<      0   0%   4%   [brdg_wkq/0]
  499   259  root       S <    3276   7%   2%   /bin/VmrMgr -p 10 -s 0
  260   259  root       S <    3276   7%   2%   /bin/VmrMgr -p 10 -s 0
    2    1  root       RWN      0   0%   2%   [ksoftirqd/0]
  494    5  root       SW<      0   0%   2%   [voip_isr/0]
  179    5  root       SW<      0   0%   1%   [voshwtimer/0]
  221    1  root       S      1796   4%   1%   Ssp
  264   221  root       S      2912   7%   1%   /bin/WebMgr -p 20 -s 0
  262   221  root       S      3108   7%   0%   /bin/EthMgr -p 20 -s 0
  263   221  root       S      1940   4%   0%   /bin/HpnaMgr -p 20 -s 0
  256   221  root       S      1900   4%   0%   /bin/NetMgr -p 20 -s 0
  227   221  root       S      1764   4%   0%   /bin/LogMgr -p 20 -s 0
  258   221  root       S <    3276   7%   0%   /bin/VmrMgr -p 10 -s 0
  270   269  root       S      2912   7%   0%   /bin/WebMgr -p 20 -s 0
  255   221  root       S      2908   7%   0%   /bin/PonMgr -p 20 -s 0
  453   255  root       S      2908   7%   0%   /bin/PonMgr -p 20 -s 0
^[[A^[[A^[[A^[[A^[[A^[[A#ONT/system/shell$ bin/TimerMgr -p 10 -s 0

```

- iv. Monitor the network product's performance, response times, and behavior during the overload simulation.
- v. Validate that the network product reacts to the overload in a controlled manner and prioritizes critical tasks. (The expected behavior of the network product shall be provided in the OEM Documentation)
- vi. Observe how the network product's security functions operate and perform during the overload.

11.1.4. Test Observation:

- i. **Case 1:** The network product reacts in a controlled way during overload (**Positive Test Case**) The network product demonstrates a controlled response to the simulated overload. It prioritizes critical tasks, maintains essential functions, and keeps security functions operational during the overload scenario. Then the test case Passes.

- ii. **Case 2:** The network product reacts in an uncontrolled way during overload
(**Negative Test Case**) If the network product exhibits unpredictable behavior, crashes, or fails to maintain its security functions during overload, it will be considered a failure.

11.1.5. **Evidence Provided:** Documentation showing each of the points in the results sections.

xii. **Test Case Result:**

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC1_EXCESSIVE_OVERLOAD_PROTECTION		



Section 9: Vulnerability Testing Requirements

2.9.1 TSTP for Evaluation of Fuzzing – Network and Application Level

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.9.1
--	--------------------------	-----------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 9: Vulnerability Testing Requirements

2. <Security Requirement No & Name > 2.9.1 Fuzzing – Network and Application Level

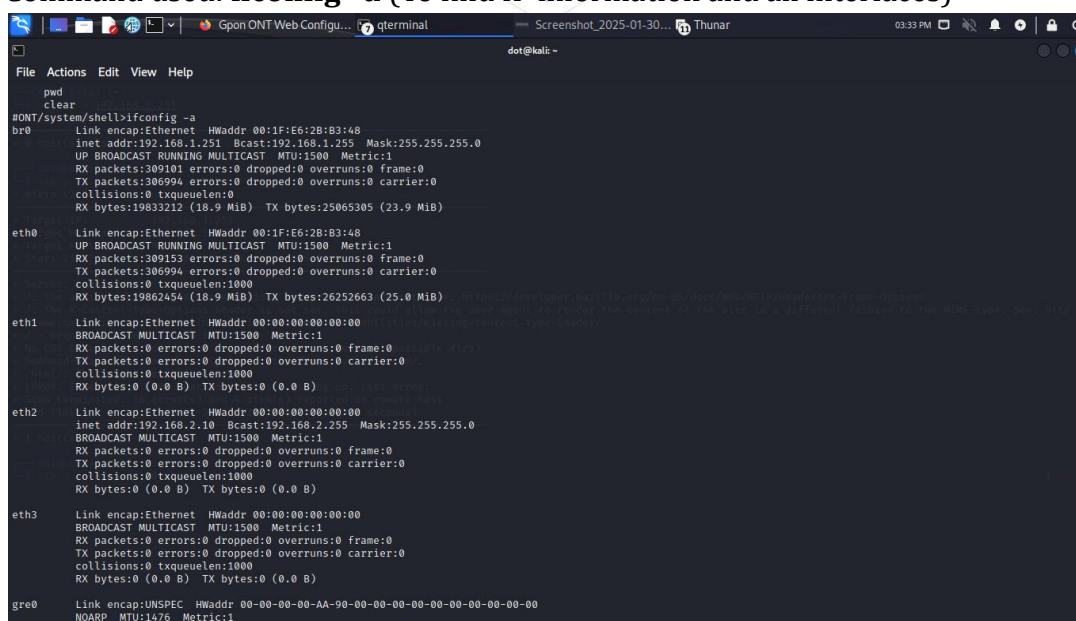
3. <Requirement Description: > It shall be ensured that externally reachable services of ONU/ONT are reasonably robust when receiving unexpected input.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. section 4.4.4]

4. DUT Confirmation Details:

- Use the command line interface to get details of the machine on which test is conducted.
- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info

Command used: **ifconfig -a** (To find IP information and all interfaces)



```
File Actions Edit View Help
dot@kali: ~
pwd
clear
#ONT/system/shell>ifconfig -a
br0:
    Link encap:Ethernet  HWaddr 00:1F:E6:2B:B3:48
    inet addr:192.168.1.251  Bcast:192.168.1.255  Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
    TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0:
    Link encap:Ethernet  HWaddr 00:1F:E6:2B:B3:48
    BROADCAST MULTICAST  MTU:1500  Metric:1
    RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
    TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1:
    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
    BROADCAST MULTICAST  MTU:1500  Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2:
    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
    inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
    BROADCAST MULTICAST  MTU:1500  Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3:
    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
    BROADCAST MULTICAST  MTU:1500  Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0:
    Link encap:UNSPEC  HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
    NOARP  MTU:1476  Metric:1
```

The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>
```

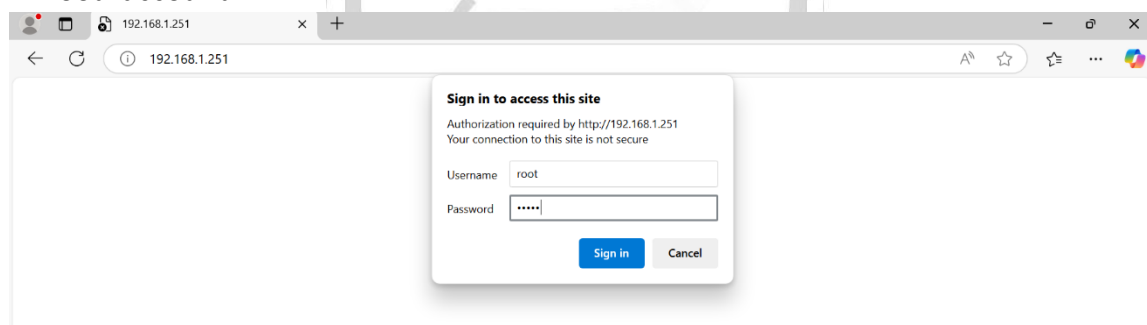
The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

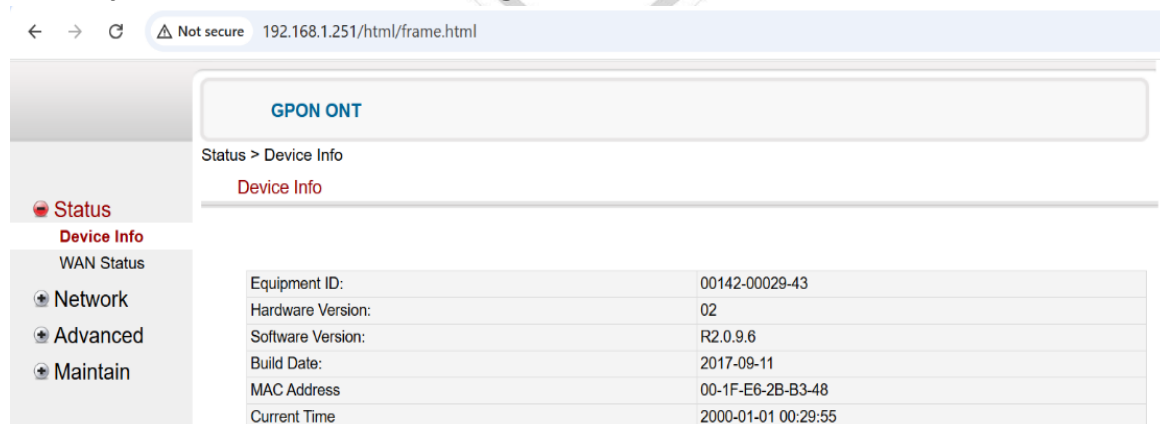
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

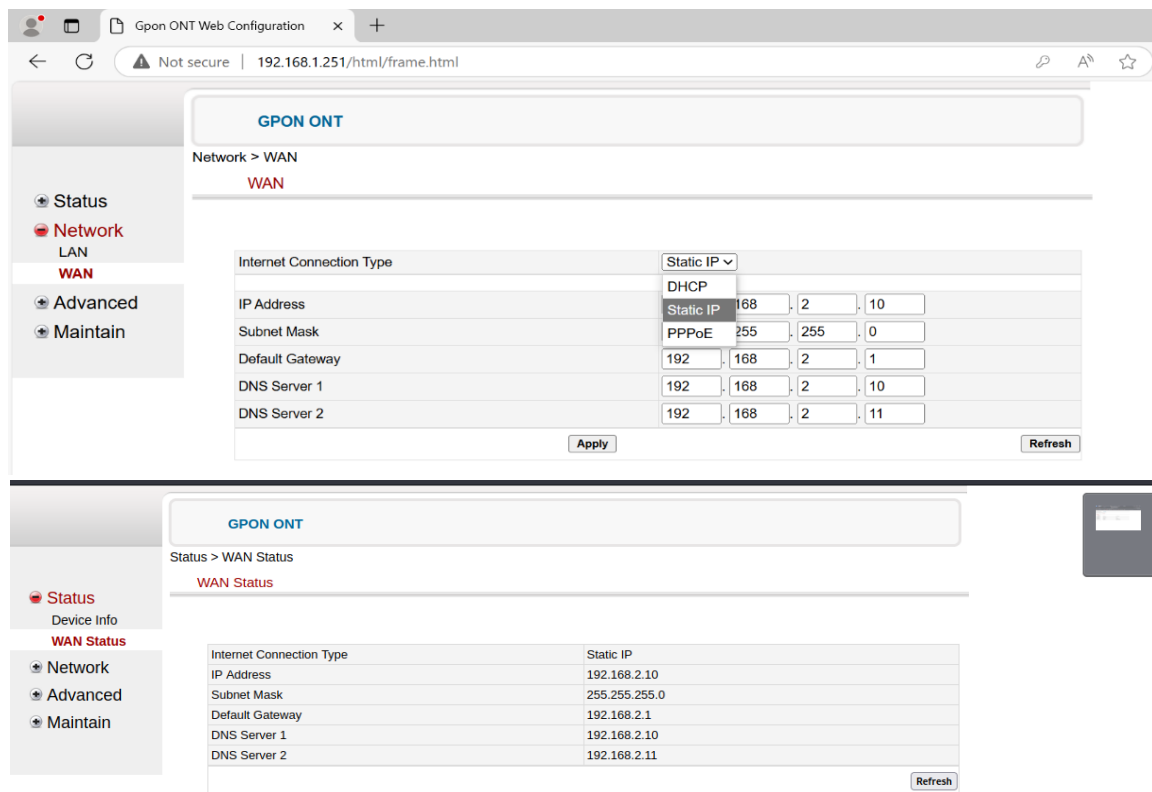
- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address



6. Preconditions

- i. The tester has the privileges to log in the network product and to access all system resources (e.g. log files)
- ii. A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:
 - a. all interfaces providing IP-based protocols;
 - b. the available transport layer protocols on these interfaces;
 - c. their open ports and associated services;
 - d. and a free-form description of their purposes.
- iii. NOTE: This list is to be validated as part of the port scanning activity.
- iv. The robustness and fuzzing tools that are selected for this test shall utilize state-of-the-art technology to identify input which causes the Network Product to behave in an unspecified, undocumented, or unexpected manner.
- v. Fuzz testing tools are a highly sophisticated technology and adaptation to the individual protocols in question is needed to be effective. Therefore, there is a lack of available effective fuzz testing tools available especially for protocols proprietary to the Telco industry. Taking into account note 4 of TR 33.916's clause 7.2.4, test labs shall acquire fuzz testing tools for those protocols where commercially feasible.
- vi. It needs to be taken into account that fuzz testing tools might show drastic differences in terms of effectiveness.
- vii. The accredited test lab is expected to have sufficient expertise to recognize the level of effectiveness of the available tools.

7. Test Objective: To verify that the network product provides externally reachable services which are robust against unexpected input.

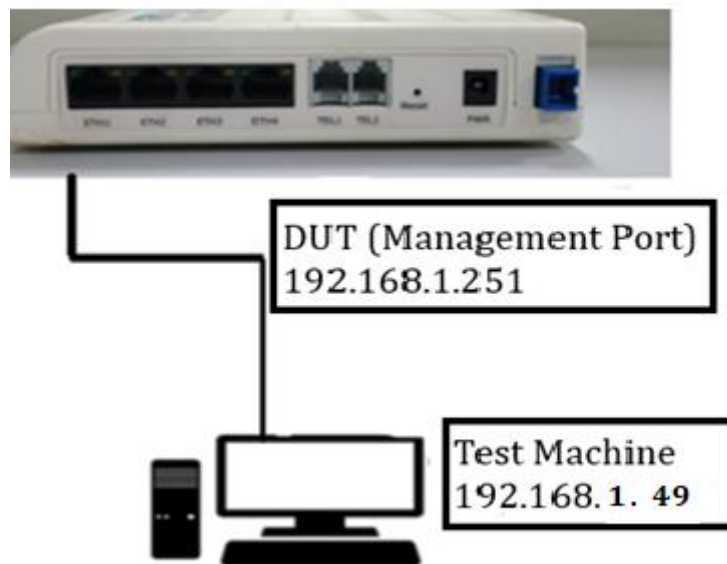
8. Test Plan

8.1. Number of Test Scenarios

8.1.1. Test Scenario for Fuzzing for Application Layer

8.1.2. Test Scenario for Fuzzing for Network Layer

8.2. Test Bed Diagram



8.3. Tools Required: Fuzzing Tool (Defensics by Synopsys was used in our case)

8.4. Test Execution Steps:

The accredited evaluator's test lab is required to execute the following steps:

- i. Execution of available effective fuzzing tools against the protocols available via interfaces providing Application-based protocols of the Network Product for an amount of time sufficient to be effective.
- ii. Execution of available effective robustness test tools against the protocols available via interfaces providing IP-based protocols of the Network Product for an amount of time sufficient to be effective. (Use of TCP/UDP Packets with underlying IP packets also works)
- iii. For both step 1 and 2:
 - a. Using a network traffic analyzer on the network product (e.g. TCPDUMP/Wireshark) or an external traffic analyzer directly connected to the network product, the tester verifies that the packets are correctly processed by the network product.
 - b. The testers verifies that the network product and any running network service does not crash.
 - c. The execution of tests shall run sufficient times.

9. Expected Results for Pass

- i. A list of all of the protocols of the network product reachable externally on an IP-based interface, together with an indication whether effective available robustness and fuzz testing tools have been used against them, shall be part of the testing documentation. If no tool can be acquired for a protocol, a free form statement should explain why not.
- ii. The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output is evidence and shall be part of the testing documentation.
- iii. Any input causing unspecified, undocumented, or unexpected behavior, and a description of this behavior shall be highlighted in the testing documentation.
- iv. COTS fuzzing tools, by their nature, may have an acceptable failure rate (e.g. 0.1%) due to different non-deterministic variables in their implementation. At some point the tool's documentation may even mention that the failing test shall be repeated to check whether it is really a recurring problem or not. The tester shall make best effort to determine if there is an issue with NE or the test tool and if necessary, work with the vendor of the network product to come to a consensus on the test result outcome.

10. Expected Form of Evidence: A testing report provided by the testing agency which will consist of the following information:

- i. The used tool(s) name and version information,
- ii. Settings and configurations used
- iii. The output log file of the chosen tool that displays the results (passed/failed).
- iv. Screenshot
- v. Test result (Passed or not)
- vi. Log/evidence tracing possible crashes
- vii. Any input causing unspecified, undocumented, or unexpected behaviour

11. Test Execution

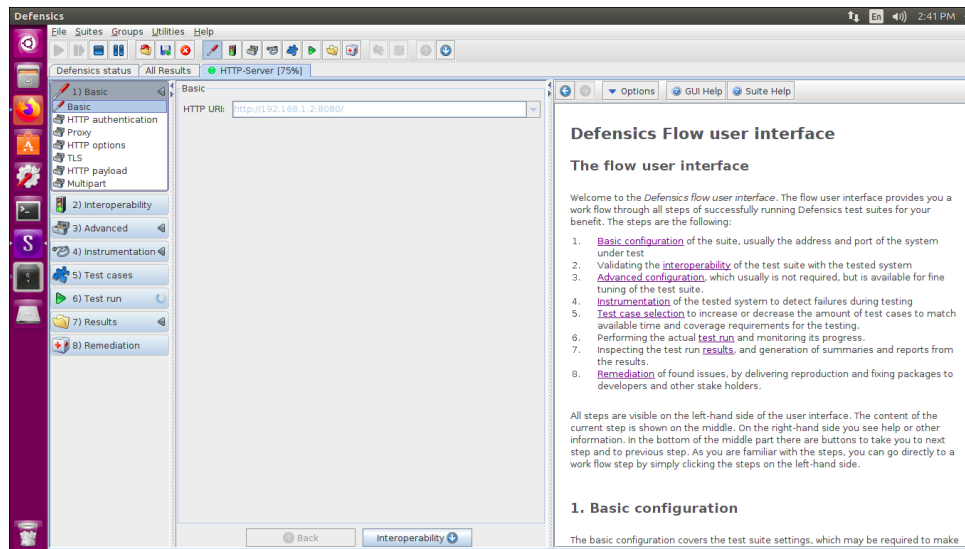
11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_FUZZ_TESTING_APPLICATION

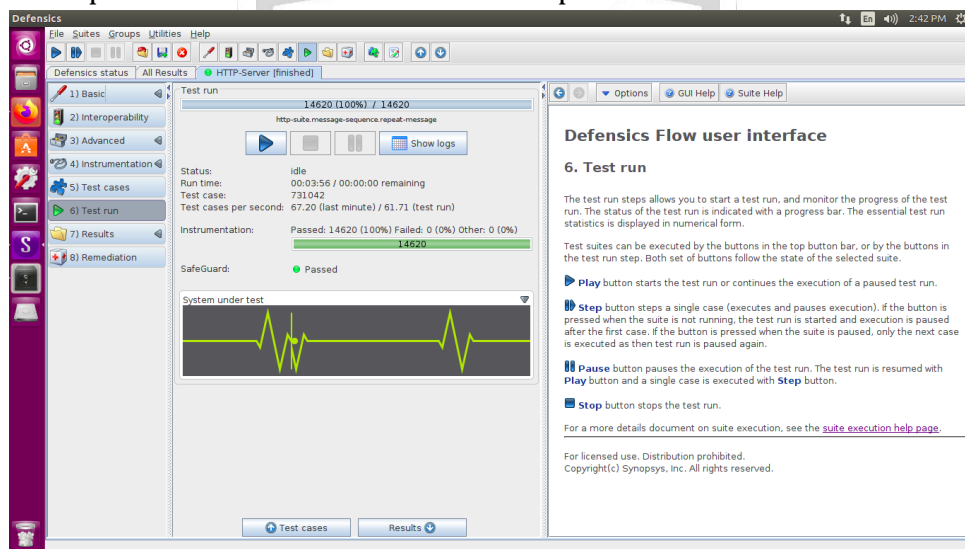
11.1.2. Test Case Description: To verify that the application-level protocols are robust against unexpected input.

11.1.3. Execution Steps:

- i. Tester sets the destination URL in the fuzzing tool including IP and designated incoming open port on DUT.



- ii. Tester turns on Wireshark to capture packets received by the server.
- iii. Tester should be familiar with the workings of designated fuzzing tools the suites used, the protocols to be tested and use maximum amount of test cases possible and repeat test numerous times and compile result.



- 11.1.4. **Test Observations:** Pcap Trace and Report should be available. Sample Report is attached below. Pcap Trace is attached separately due to huge size. (Refer Tar ball attached):

Defensics Fuzz Test Report

Fuzz testing report

Test Setup

System Under Test

Name: Fuzz testing report

Fuzz Test Summary

Overall verdict: **PASS**
Tests executed: 14620
Test duration: 00:03:55
Reported by:

Test Run Summary

Test Run Summary

Suite	Version	Verdict	Number of test cases	Duration	Date	Instrumentation
HTTP Server	4.14.0	PASS	14620	00:03:55	20230816	ENABLED Protocol semantics ENABLED Connection based instrumentation ENABLED SafeGuard
Total		PASS	14620	00:03:56		

11.1.5. Evidence Provided: A testing report provided by the testing agency which will consist of the following information:

- The used tool(s) name and version information,
- Settings and configurations used
- The output log file of the chosen tool that displays the results (passed/failed).
- Screenshot
- Test result (Passed or not)
- Log/evidence tracing possible crashes
- Any input causing unspecified, undocumented, or unexpected behavior

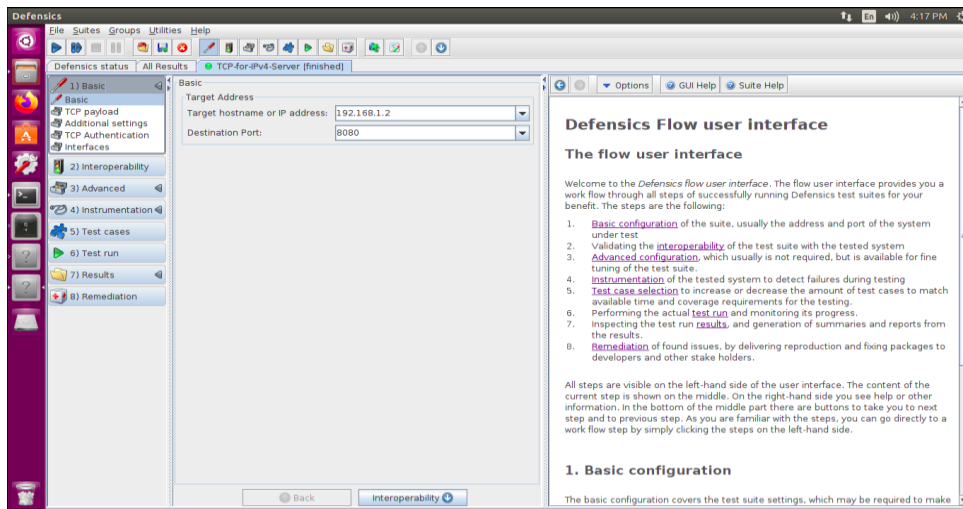
11.2 Test Case Number: 02

11.2.1. Test Case Name: TC_FUZZ_TESTING_NETWORK

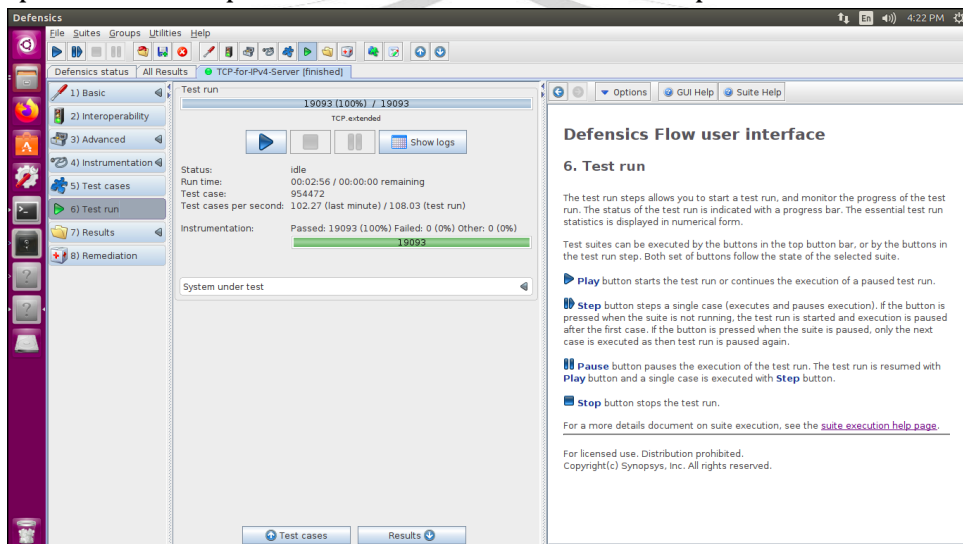
11.2.2. Test Case Description: To verify that the network-level protocols are robust against unexpected input. The following example uses TCP with IPv4. Testing also done with UDP with IPv4. If DUT supports IPv6, testing must also be done with TCP/UDP with IPv6.

11.2.3. Execution Steps:

- Tester sets the destination URL in the fuzzing tool including IP and designated incoming open port on DUT.



- ii. Tester turns on Wireshark to capture packets received by the server.
- iii. Tester should be familiar with the workings of designated fuzzing tools the suites used, the protocols to be tested and use maximum amount of test cases possible and repeat test numerous times and compile result.



11.2.4. Test Observations: Pcap Trace and Report should be available. Sample Report is attached below. Pcap Trace is attached separately due to huge size. (Refer Tar ball attached):

Summary

This is a test report of 20230816-1619-28

Table of contents

[Summary](#)
[Table of contents](#)
[Test runs](#)
[20230816-1619-28 - TCP for IPv4 Server Test Suite](#)
[Analysis](#)
[Detail of service analysis](#)
[Response analysis](#)

Test runs

20230816-1619-28 : TCP for IPv4 Server Test Suite

Diagnoses

Valid case instrumentation	ENABLED
External instrumentation	DISABLED
Protocol semantics	DISABLED
Connection based instrumentation	DISABLED
SafeGuard	DISABLED
SNMP instrumentation	DISABLED
SNMP Trap instrumentation	DISABLED
ISASecure CCM	DISABLED
Syslog instrumentation	DISABLED
Agent instrumentation	DISABLED
Instrumentation fail limit	1
Instrumentation frequency	1

Total of 19093 cases were executed.

Combined overall verdict**PASS**

Verdict from valid case / instrumentation	pass	The test cases passed successfully. No flaws in the system under test were detected by the monitoring facility in context of these test cases.
0 fail	fail	There is a reason to believe that the SUT crashed or malfunctioned in some other detectable way while executing these test cases.
18366 pass	pass	The test cases passed successfully. No flaws in the system under test were detected by the monitoring facility in context of these test cases.
707 not-logged	not-logged	Test cases passed successfully. No flaws in the system under test were detected by the monitoring facility in context of these test cases. In order to save disk space test cases are not logged.

Test run order

11.2.5.Evidence Provided: A testing report provided by the testing agency which will consist of the following information:

- i. The used tool(s) name and version information,
- ii. Settings and configurations used
- iii. The output log file of the chosen tool that displays the results (passed/failed).
- iv. Screenshot
- v. Test result (Passed or not)
- vi. Log/evidence tracing possible crashes
- vii. Any input causing unspecified, undocumented, or unexpected behavior

12. Test Case Results

Sl. No	TEST CASS NAME	PASS/FAIL	Remarks
1	TC_FUZZ_TESTING_APPLICATION		
2	TC_FUZZ_TESTING_NETWORK		

Securing Networks

2.9.2 TSTP for Evaluation of Port Scanning

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.9.2
--	--------------------------	-----------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 9: Vulnerability Testing Requirements

2. <Security Requirement No & Name > 2.9.2 Port Scanning

3. <Requirement Description:> It shall be ensured that on all network interfaces, only vendor documented/identified ports on the transport layer respond to requests from outside the system. List of the identified open ports shall match the list of network services that are necessary for the operation of the ONU/ONT.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.2]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
- ii. Use command to get Application No/Version No & Kernel Info
- iii. Command used: **ifconfig -a** (To find IP information and all interfaces)

```

dot@kali: ~
File Actions Edit View Help
pwd
clear
#ONT/system/shell>ifconfig -a
brf0: Link encap:Ethernet HWaddr 00:1F:E6:2B:83:48
      inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0: Link encap:Ethernet HWaddr 00:1F:E6:2B:83:48
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00
      inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0: Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00
      NOARP MTU:1476 Metric:1

```

The below screenshot shows the firmware version of the DUT

```

#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>

```

The below screenshot shows the information of the DUT

```

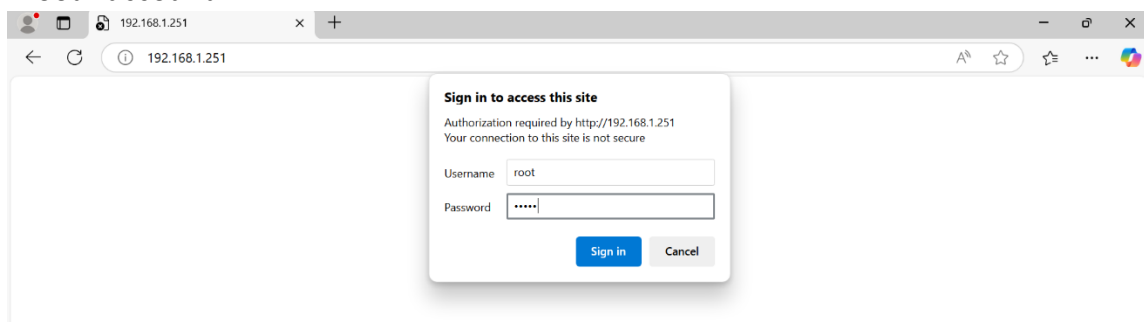
#ONT/system>custom
Customer Information

Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>

```

5. DUT Configuration

- The Tester opens GUI(webpage) of DUT(192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using "root" account.



- Verify the DUT information through device info

← → ↻ ⚠ Not secure 192.168.1.251/html/frame.html

GPON ONT

Status > Device Info

Device Info

Status

Device Info

WAN Status

Network

Advanced

Maintain

Equipment ID:	00142-00029-43
Hardware Version:	02
Software Version:	R2.0.9.6
Build Date:	2017-09-11
MAC Address	00-1F-E6-2B-B3-48
Current Time	2000-01-01 00:29:55

iv. Set the static IP address

Gpon ONT Web Configuration x +

← ↻ ⚠ Not secure | 192.168.1.251/html/frame.html

GPON ONT

Network > WAN

WAN

Status

Network

LAN

WAN

Advanced

Maintain

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Status

Device Info

WAN Status

Network

Advanced

Maintain

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6. Preconditions

- A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:
 - all interfaces providing IP-based protocols;
 - the available transport layer protocols on these interfaces;
 - their open ports and associated services per transport layer protocol;
 - and a free-form description of their purposes.
- The port scanning tool that is used shall be capable to detect open ports on the relevant transport layer protocols.
- NOTE: It might not be possible for certain transport layer protocols (like UDP) to unambiguously detect whether a port is open or not by means of external port scanning. Also, in some circumstances it might not be efficient to do external port scanning, e.g. if there are security measures to limit the rate a system can be probed.

In those cases, the accredited evaluator's test laboratory determines another means suitable to verify which ports are open.

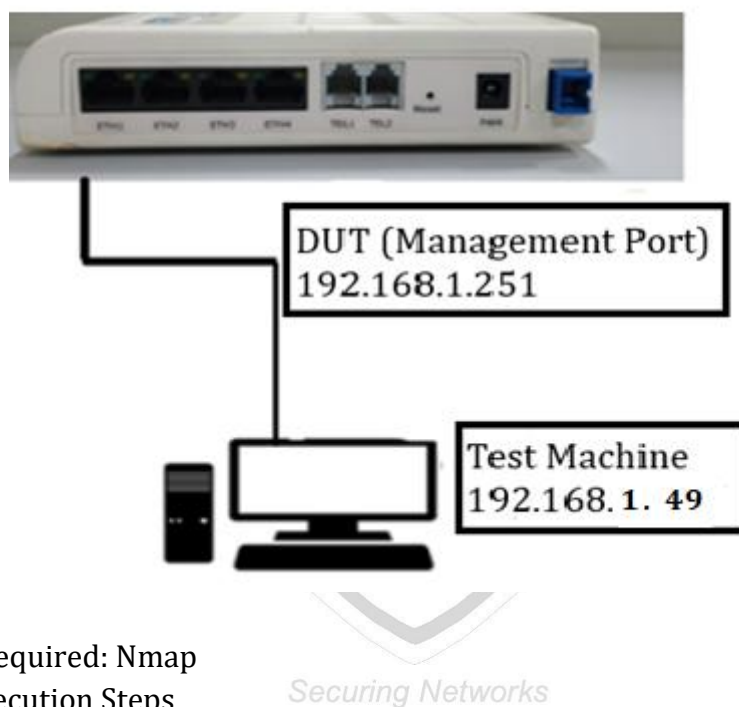
7. Test Objective: To ensure that on all network interfaces, only documented ports on the transport layer respond to requests from outside the system

8. Test Plan

8.1. Number of Test Scenarios

8.1.1. Test Scenario for Port Scanning using Nmap: All the ports on all supported transport layer protocols should be scanned using Nmap. (Additional test scenarios are to be taken into consideration if tools like lsof, netstat are used)

8.2. Test Bed Diagram



8.3. Tools Required: Nmap

8.4. Test Execution Steps

- i. Verification of the compliance to the prerequisites:
 - a. Verification that the list of available network services is available in the documentation of the Network Product.
 - b. Validation that all entries in the list of services are meaningful and reasonably necessary for the operation of the Network Product class
- ii. Identification of the open ports by means of capable port scanning tools or other suitable testing means.
- iii. Verification that the list of identified open ports matches the list of available network services in the documentation of the Network Product

9. Expected Results: The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output containing all the technically relevant information about test results is evidence and shall be part of the testing

documentation. All discrepancies between the list of identified open ports and the list of available network services in the documentation shall be highlighted in the testing documentation.

10. Expected Form of Evidence: Output of port scan and list of identified discrepancies.

11. Test Execution

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_BVT_PORT_SCANNING_NMAP

11.1.2. Test Case Description: On all network interfaces of DUT, only documented ports on the transport layer respond to requests from outside the system

11.1.3. Execution Steps:

- i. Tester shall scan all the available transport layer protocols ports of the DUT using nmap with the following command
 - **For Example,**
- ii. For scanning TCP Ports, use below command.
 - ***sudo nmap -sT -PN -n -sV -T4 -p- -oN <DUT_IP>***
 - ***sudo nmap -p 1-65535 -T4 -A -v <DUT_IP> (Default scan of TCP ports only)***
- iii. For scanning UDP Ports, use below command.
 - ***sudo nmap -sU -PN -n -sV -T4 -p- -oN <DUT_IP>***
- iv. For scanning SCTP Ports, use below command.
 - ***sudo nmap -sY -PN -n -sV -T4 -p- -oN <DUT_IP>***
- v. sT: TCP connect scan.
- vi. sU: UDP scan
- vii. sY: SCTP scan
- viii. PN: Don't ping
- ix. n: Disable reverse DNS
- x. p: Scan all ports
- xi. oN: Output scan is normal. File specification, requests normal output be directed to given filename.
- xii. T4: Faster Execution
- xiii. sV: Service Version
- xiv. **Below screenshots showing port scanning:** The scan report as shown below indicates the open/closed ports and the services running on those ports in the DUT, Amongst the given options, identify all the open ports and services running in transport layer.
- xv. **Command executed: nmap -sV <ip address of DUT>**

xvi. **Command executed:** `nmap -sT -PN -n -sV -p- -oN <filename.txt> <DUT_IP>`

- xvii. Tester then shall verify if the ports mentioned as open by nmap on all the interfaces match the list provided by the vendor and also verify that no extra port is opened. (Note: This step has OEM dependency).

11.1.5. Evidence Provided: Output of port scan.

Sl. No	TEST CASS NAME	PASS/FAIL	Remarks
1	TC_BVT_PORT_SCANNING_N MAP	OEM Dependent	Port scan results to be verified against OEM document for list of open ports.

2.9.3 TSTP for Evaluation of Vulnerability Scanning

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.9.3
---	--------------------------	-----------------

<DUT Details: > Alphion AONT100C

<DUT Software Version:> R2.0.9.6

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **ITSAR Section No & Name:** Section 9: Vulnerability Testing Requirements.
2. **Security Requirement No & Name:** 2.9.3 Vulnerability Scanning.
3. **Requirement Description:** It shall be ensured that no known critical/ high/medium vulnerabilities (as on date of offer of ONU/ONT to designated TSTL for testing) shall exist in the ONU/ONT. For low category vulnerabilities remediation plan is to be provided.

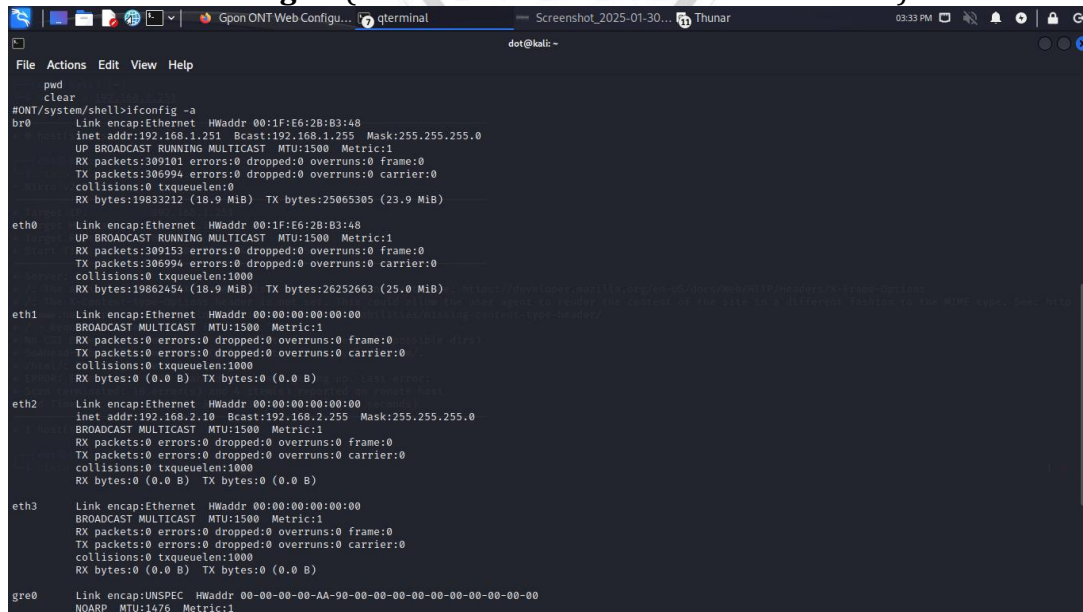
[Reference: TS/DSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3].

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
- ii. Use command to get Application No/Version No & Kernel Info

Command used: **ifconfig -a** (To find IP information and all interfaces)



```
File Actions Edit View Help
pwd
clear
#ONT/system/shell@ifconfig -a
br0    Link encap:Ethernet HWaddr 00:1F:E6:2B:83:48
       inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:309191 errors:0 dropped:0 overruns:0 frame:0
       TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)

eth0    Link encap:Ethernet HWaddr 00:1F:E6:2B:83:48
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
       TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:19862434 (18.9 MiB) TX bytes:26252663 (25.0 MiB)

eth1    Link encap:Ethernet HWaddr 00:00:00:00:00:00
       BROADCAST MULTICAST MTU:1500 Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth2    Link encap:Ethernet HWaddr 00:00:00:00:00:00
       inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0
       BROADCAST MULTICAST MTU:1500 Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth3    Link encap:Ethernet HWaddr 00:00:00:00:00:00
       BROADCAST MULTICAST MTU:1500 Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

gre0    Link encap:UNISPEC HWaddr 00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00-00-00
       NOARP MTU:1476 Metric:1
```

The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>
```

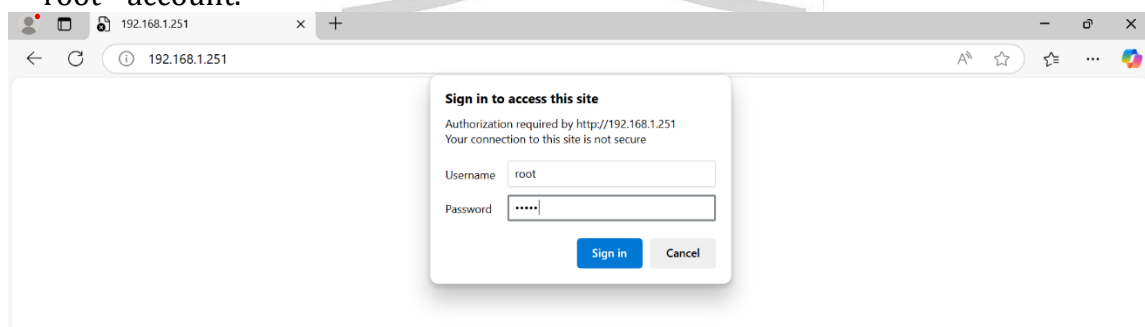
The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

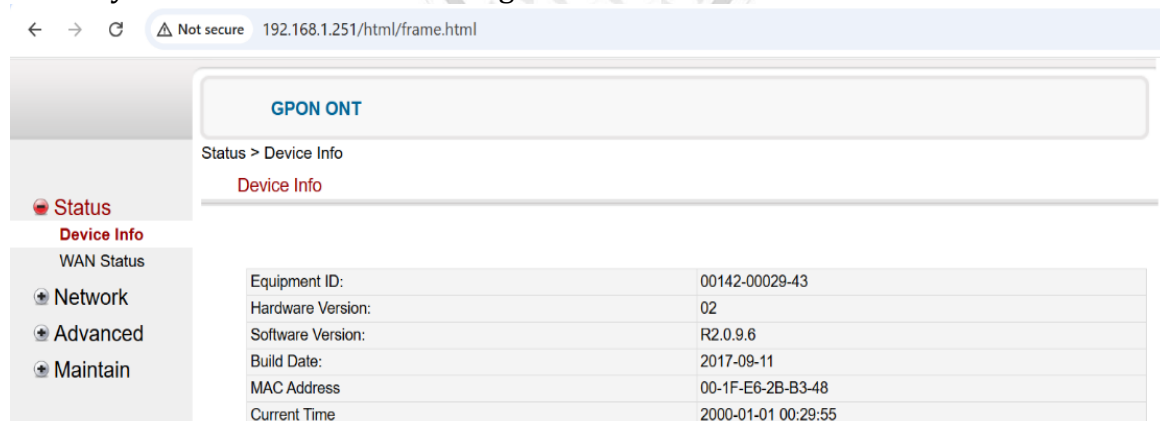
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

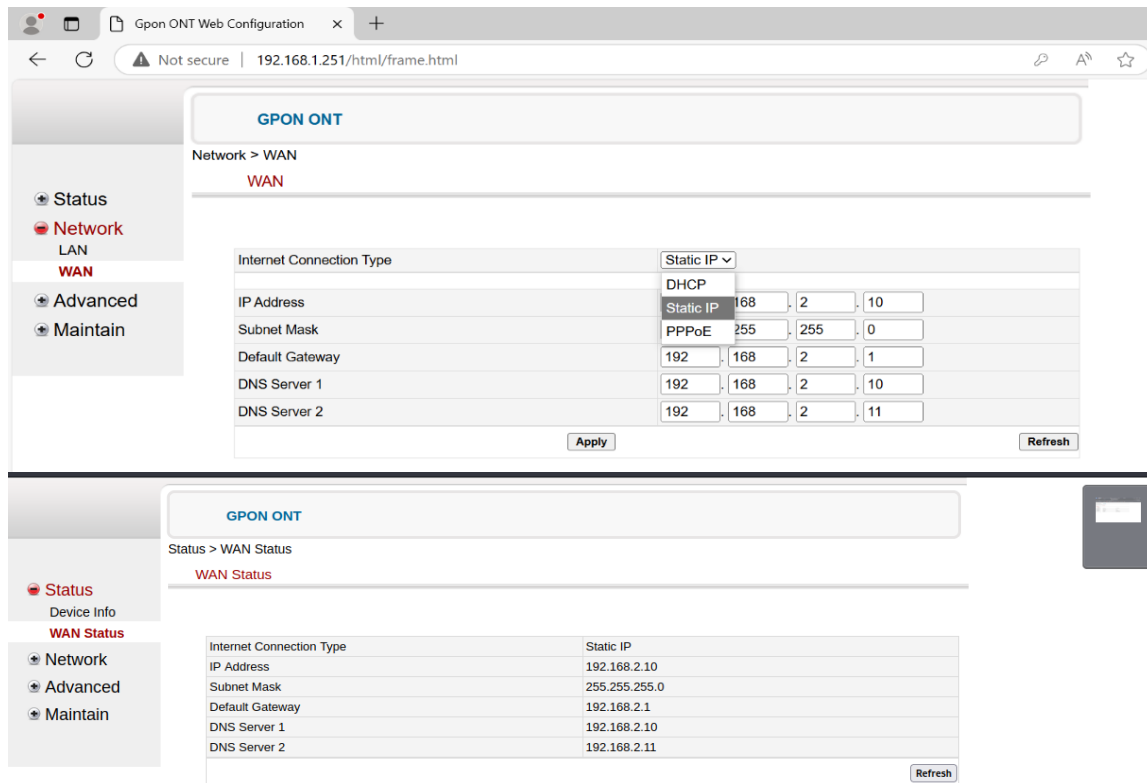
- The Tester opens GUI(webpage) of DUT(192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



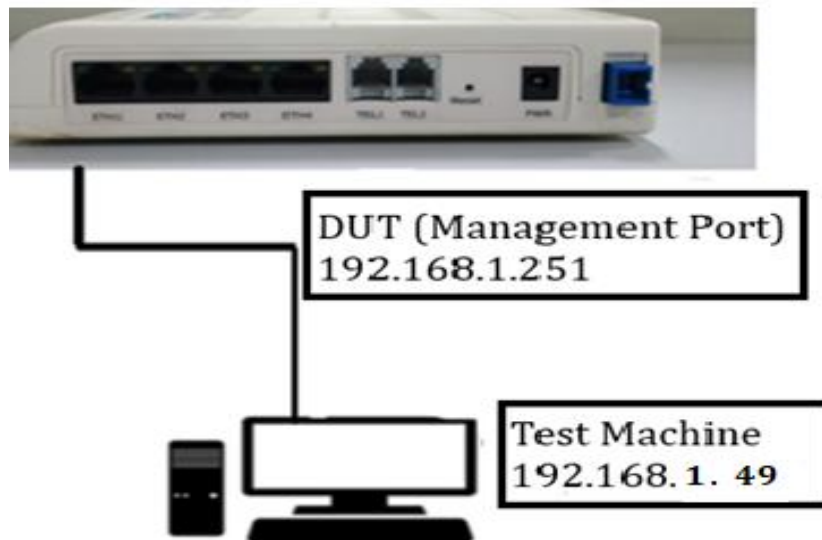
- Verify the DUT information through device info



- Set the static IP address



6. **Preconditions:** A list of all available network services containing at least the following information shall be included in the documentation accompanying the Network Product:
 - i. all interfaces providing IP-based protocols;
 - ii. the available transport layer protocols on these interfaces;
 - iii. their open ports and associated services;
 - iv. and a free-form description of their purposes.
 - v. **NOTE:** A known vulnerability scanning tool that has capabilities to support the given testing should be present. Following TSTP is developed using NESSUS. Any other tool with similar capability can be also used, but documentation should be provided that the tool meets the need of the requirement.
7. **Test Objective:** The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Network Product that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.
8. **Test Plan:**
 - 8.1 Test scenarios: -
 - 8.1.1 The Tester performs an authenticated vulnerability scan of DUT using a suitable vulnerability scanning tool.
 - 8.1.2 Tools Used: Any vulnerability scanner tool (NESSUS)
 - 8.2 Test Bed diagram: -



8.3 Test Execution steps: The accredited evaluator's test lab is required to execute the following steps:

- i. Execution of the suitable vulnerability scanning tool against all interfaces providing IP-based protocols of the Network Product.
- ii. Verify that tool have updated the vulnerability database
- iii. Perform and validate authenticated scan on the Network Product.
- iv. Evaluation of the results based on their severity.

9. **Expected Results for Pass:** Report showing evidences that no known vulnerabilities are present in the network product.

10. Expected Format of Evidence:

- i. The used tool(s) name, their unambiguous version (also for plug-ins if applicable), used settings, and the relevant output is evidence and shall be part of the testing documentation.
- ii. The discovered vulnerabilities (including source, example CVE ID), together with a rating of their severity, shall be highlighted in the testing documentation.

11. Test Execution:

11.1 Test Case Number: 1

11.1.1. **Test Case Name:** TC_BVT_VULNERABILITY_SCANNING

11.1.2. **Test Case Description:** To ensure that DUT is free from any vulnerabilities.

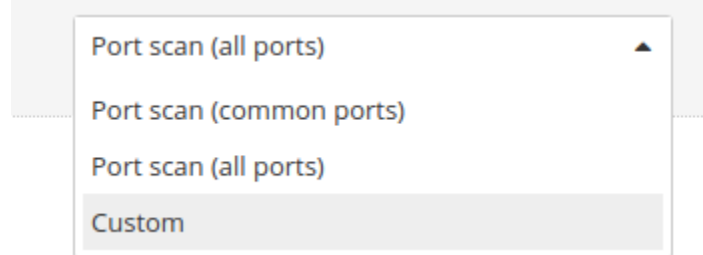
11.1.3. **Execution Steps:** The accredited evaluator's test lab is required to execute the following steps:

- i. Execution of the suitable vulnerability scanning tool against all interfaces providing IP-based protocols of the Network Product.
- ii. Perform and validate authenticated scan on the Network Product.
- iii. Evaluation of the results based on their severity.

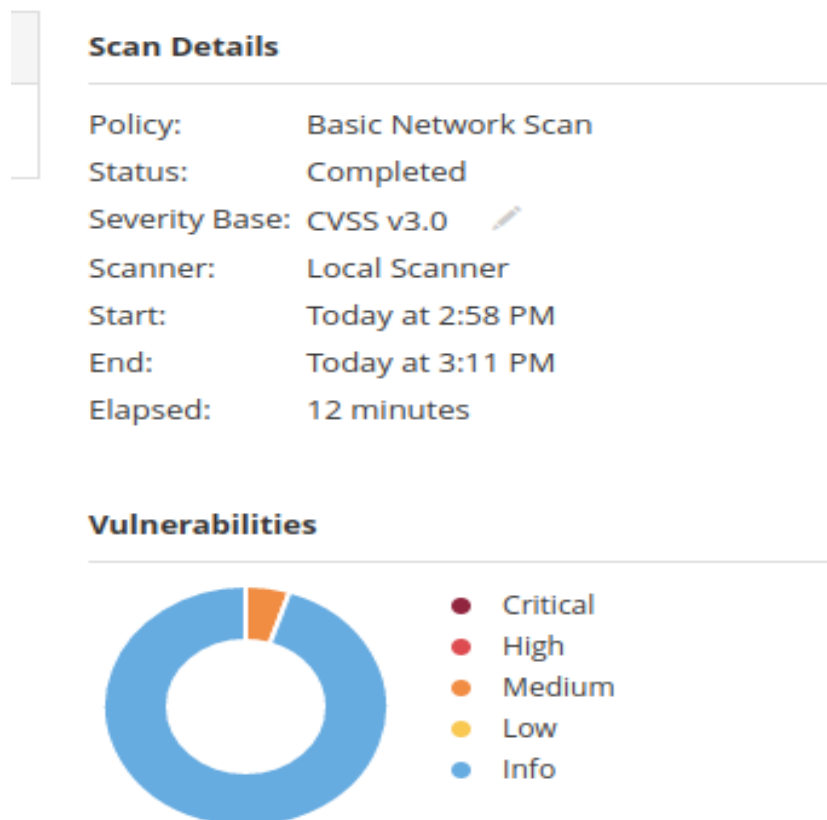
11.1.4. Test Observations:

- i. **Case 1:** Tester scans the required target (IP address) and checks the scan summary. We can see in the screenshot below, the given interface is scanned for vulnerabilities. Various vulnerabilities with their CVE ID's are shown. All the

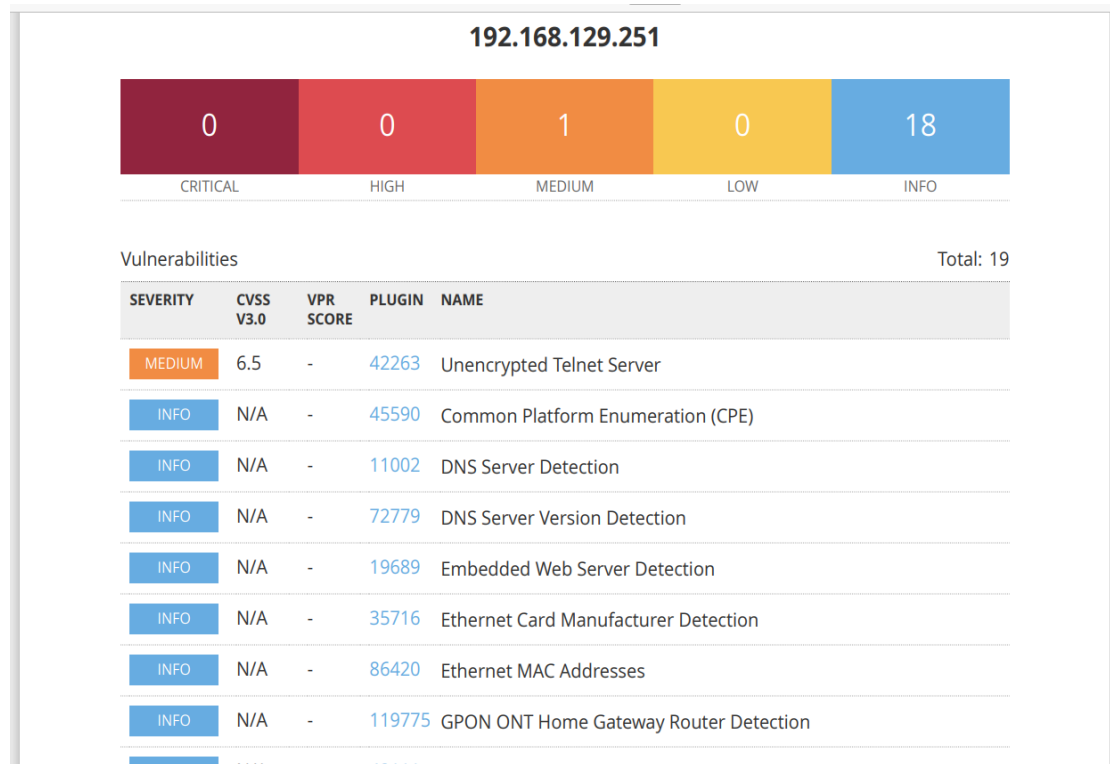
critical/high/medium vulnerabilities should be dealt with seriously. Set the ports for which scan is to be performed by selecting the custom option.



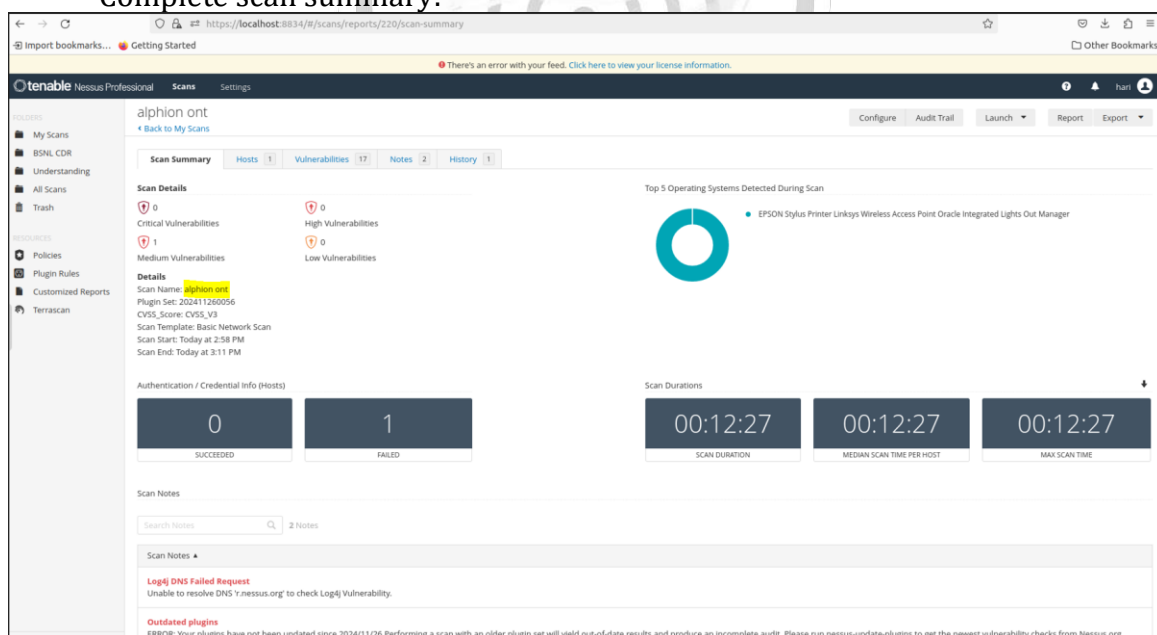
Classification of vulnerability based on the colour: -



Report as shown below is generated. It contains the CVSS score of the vulnerability as well.



Complete scan summary:-



12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_BVT_VULNERABILITY_SCANNING	Fail	DUT is marked as fail as it contains medium vulnerabilities.

Section 10: Operating System

2.10.1 TSTP Report for Evaluation Handling of ICMP

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.10.1
---	--------------------------	------------------

DUT Details: GPON-ONT

DUT Software Version: V 3.2.02-231205

Digest Hash of OS: Hash of DUT OS is required

Digest Hash of Configuration: Hash of DUT configuration is required

Applicable ITSAR: NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

ITSAR Version No: ONT ITSAR403012311 and Version: 1.0.1

OEM Supplied Document list: All the documents provided by OEM to be listed here

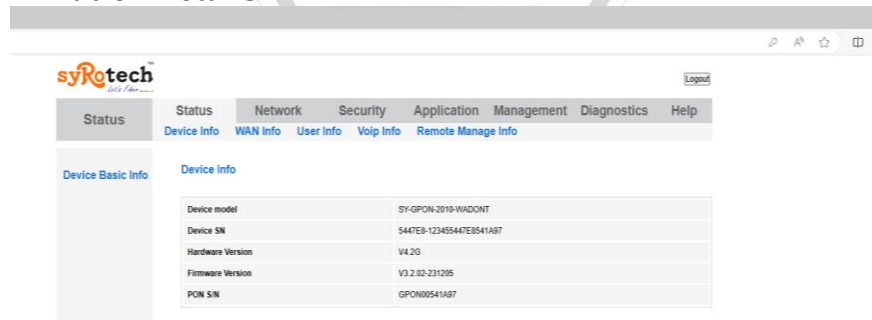
1. Section 1.10: Operating System

2. <Security Requirement No & Name > 1.10.1: Handling of ICMP

3. Requirement Description: Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the ONU/ONT. In particular, there are certain types of ICMPv4 and ICMPv6 that are not used in most networks, but represent a risk. Refer standards such as RFC 6192, RFC 7279, RFC 4890.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. Section 4.2.4.1.1.2.]

4. DUT Confirmation Details:



5. DUT Configuration: DUT is configured to allow/deny ICMP packets in accordance to the requirement

6. Preconditions: OEM shall provide instruction to enable/disable ICMPv4 and ICMPv6 packets which are not required for operation.

7. Test Objective: To verify that DUT has handling mechanism for the required and non-required ICMP packets

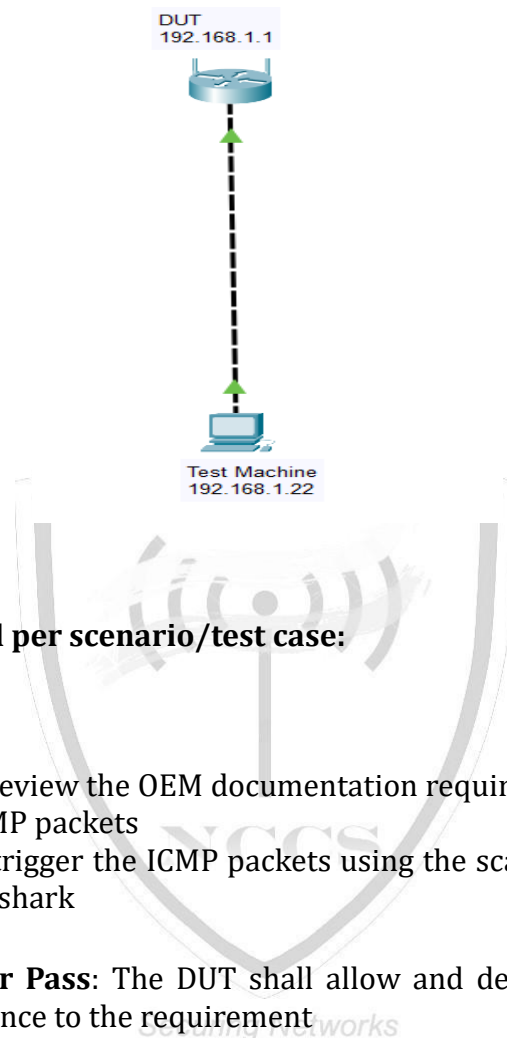
8. Test Plan

8.1 Test Cases:

8.1.1 OEM documentation for ICMP filtering

8.1.2 ICMP testcase

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case:

- i. Scapy,
- ii. Wireshark

8.4 Test Execution

- i. The Tester shall review the OEM documentation required to configure the DUT to allow or deny ICMP packets
- ii. The Tester shall trigger the ICMP packets using the scapy and capture the DUT's response on wireshark

9. **Expected Results for Pass:** The DUT shall allow and deny ICMP packets of types mentioned in accordance to the requirement

10. **Expected Format of Evidence:** screenshots

11. Test Execution:

11.1 Test Case Number:

11.1.1. **Test case Name:** OEM documentation for ICMP filtering

11.1.2. **Test Case Description:** to configure the DUT to filter the wanted and unwanted ICMP packets

11.1.3. Execution Steps

- i. The DUT should support ICMP filtering for the unwanted and the wanted ICMP packets
- ii. The tester can refer the OEM documentation for the same

11.1.4. **Test Observation:**

11.1.5. **Evidence Provided:**

11.2 Test Case Number:

11.2.1. Test case Name: ICMP testcase

11.2.2. Test Case Description: Trigger samples of the certain ICMP types of messages from the tester machine (e.g., Scapy) to the DUT and verifies by appropriate means.

11.2.3. Execution Steps:

- i. The tester creates a script to send icmpv4 packets. This script will send ICMPv4 type 0,3,5,8,11,12 and 13 to the DUT.

```
#!/usr/bin/env python3

from scapy.all import *

# Set target IP address and ICMP message types to test
target_ip = "192.168.1.1"
icmp_types = [0, 3, 8, 11, 12, 5, 13] # Adding ICMPv4 types

# Send ICMP packets of each type and check response
for icmp_type in icmp_types:
    # Create ICMP packet with specified type and target IP address
    icmp_packet = IP(dst=target_ip)/ICMP(type=icmp_type)

    # Send packet and receive response
    response = sr1(icmp_packet, timeout=2, verbose=False)

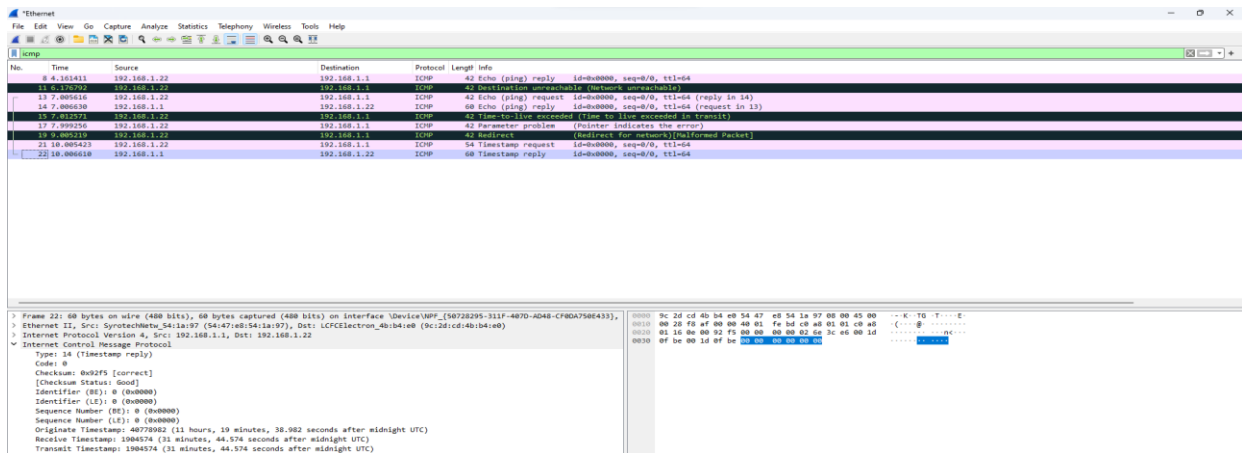
    # Check if response was received
    if response is None:
        print(f"No response received for ICMP type {icmp_type}")
    else:
        # Check if response was dropped or no response sent
        if response.haslayer(ICMP) and response[ICMP].type == icmp_type:
            print(f"ICMP type {icmp_type} was dropped or no response sent")
        else:
            # Check if response caused configuration change
            # (This check may need to be customized for specific network products)
            print(f"ICMP type {icmp_type} did not cause configuration change")
```

- ii. The tester runs the script using cmd.

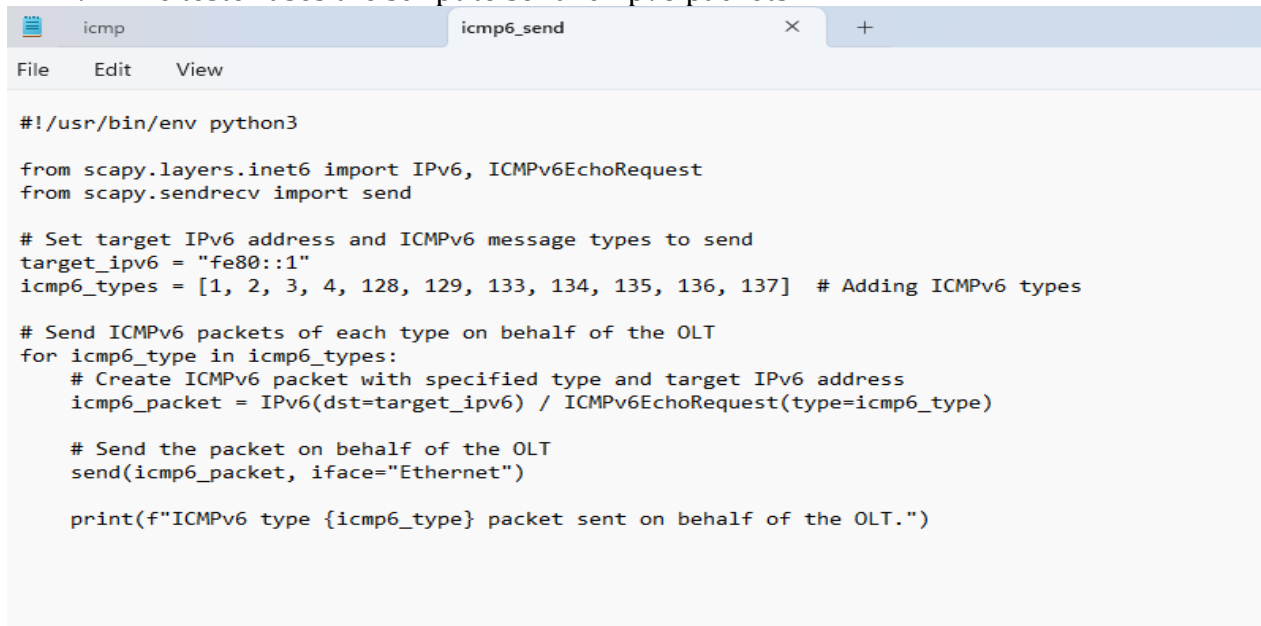
```
C:\Users\GRL\Documents>python3 icmp.py
WARNING: Wireshark is installed, but cannot read manuf !
No response received for ICMP type 0
ICMP type 3 did not cause configuration change
ICMP type 8 did not cause configuration change
ICMP type 11 did not cause configuration change
ICMP type 12 did not cause configuration change
ICMP type 5 did not cause configuration change
ICMP type 13 did not cause configuration change

C:\Users\GRL\Documents>|
```

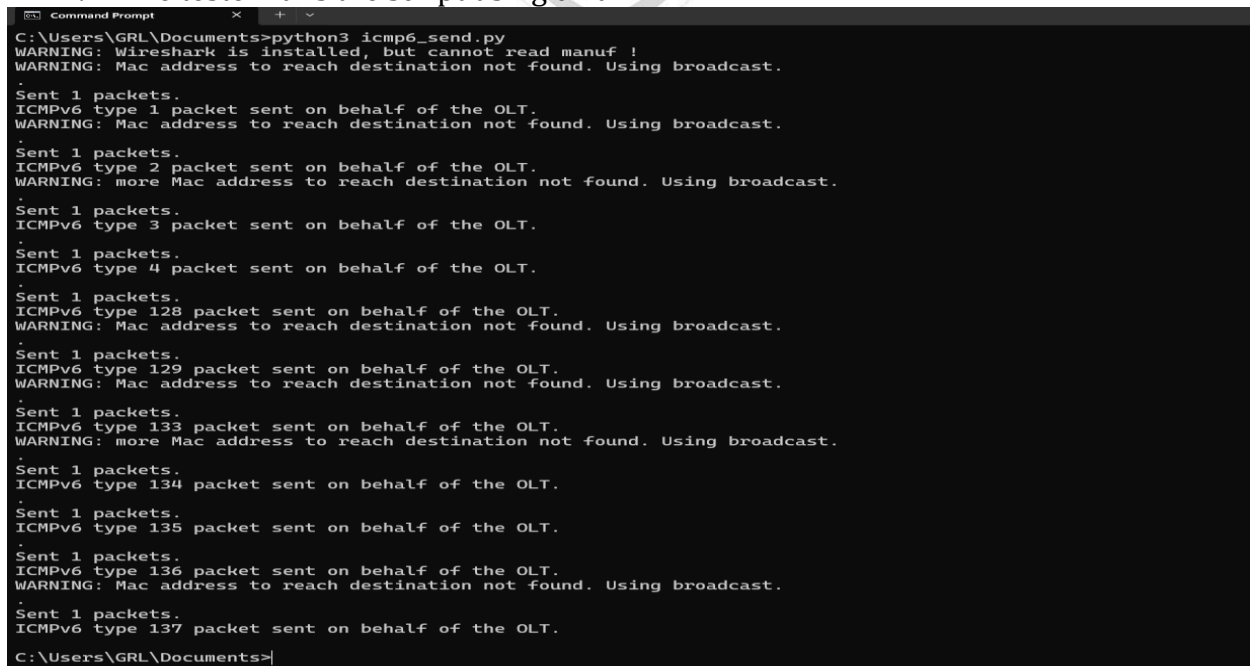
- iii. The tester captures the traffic using Wireshark



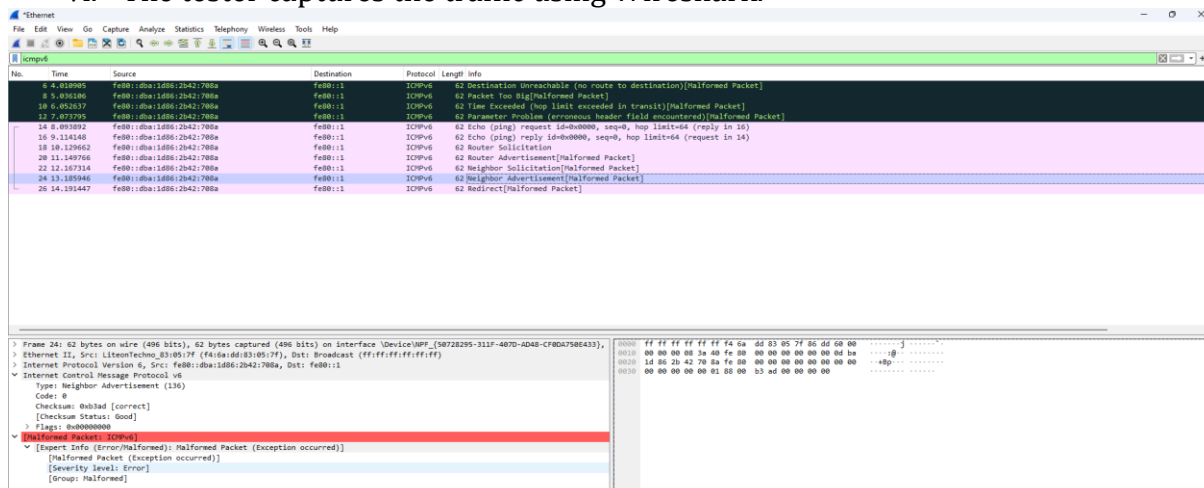
iv. The tester uses the script to send icmpv6 packets



v. The tester runs the script using cmd.



vi. The tester captures the traffic using Wireshark.



11.2.4. Test Observation:

- The tester observed that the DUT is responding to the ICMPv4 type 13 and in response DUT is providing the timestamping which is not permitted.
- DUT is not responding to the ICMPv6 type packets specifically for which responding is not permitted and they are not able to change anything in the configuration.

11.2.5. Evidence Provided: The screenshot of the Wireshark capture is attached.

12. Test Case Results:

SL.NO	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM documentation for ICMP filtering		
2	ICMP testcase		

The clause is marked as fail because the tester observed that the DUT is responding to the ICMPv4 type 13 and in response DUT is providing the timestamping which is not permitted.

Securing Networks

2.10.2 TSTP for Authentic Privilege Escalation Only

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.10.2
---	--------------------------	------------------

DUT Details: GPON-ONT

DUT Software Version: V 3.2.02-231205

Digest Hash of OS: Hash of DUT OS is required

Digest Hash of Configuration: Hash of DUT configuration is required

Applicable ITSAR: NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

ITSAR Version No: ONT ITSAR403012311 and Version: 1.0.1

OEM Supplied Document list: All the documents provided by OEM to be listed here

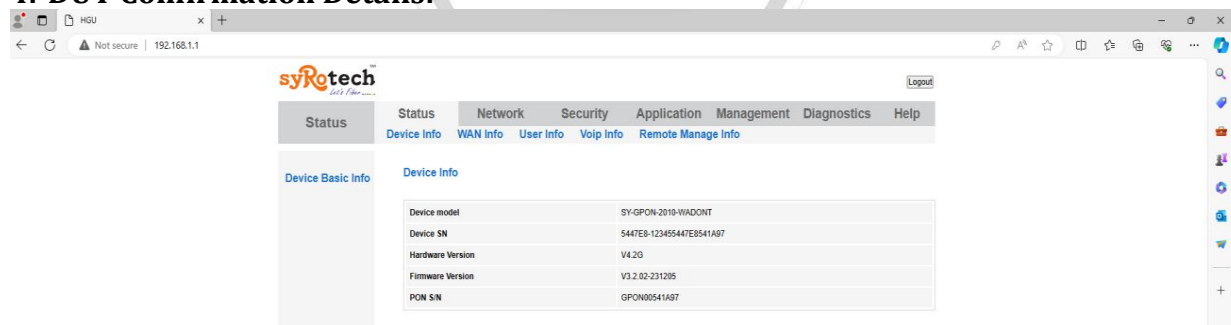
1. <ITSAR Section No & Name> **Section 1.10: Operating System**

2. <Security Requirement No & Name > **1.10.2: Authenticated Privilege Escalation Only**

3. **Requirement Description:** There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allows a lower privileged / guest user to gain administrator/root privileges from another user account without re-authentication or thru exploitation of authentication bypass vulnerabilities.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.1.2.1]

4. **DUT Confirmation Details:**



5. **DUT Configuration:** There is no additional configuration required for this test case.

6. **Pre-Conditions:**

- OEM shall provide documentation of the operating system(s) used in the network product.
- OEM shall supply a list of operating system functions which a system user can use to explicitly gain higher privileges, and how these functions are configured.

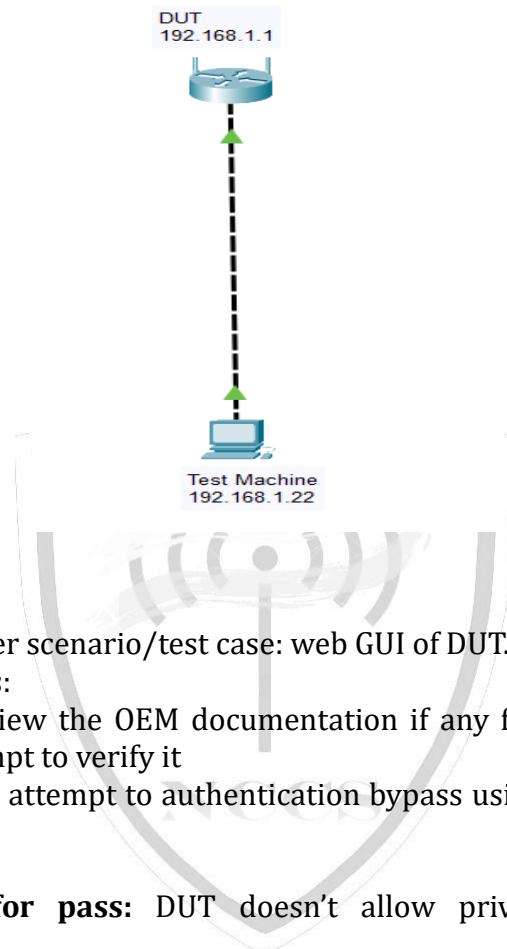
7. **Test Objective:** To verify no privilege is allowed in DUT without authentication

8. Test Plan

8.1 Test Cases:

- 8.1.1 Review OEM documentation
- 8.1.2 Check privilege escalation method in GUI.
- 8.1.3 Attempt authentication bypass to gain privilege access to the DUT

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: web GUI of DUT.

8.4 Test Execution Steps:

- i. The tester shall review the OEM documentation if any feature exists for privilege escalation and attempt to verify it
- ii. The tester shall also attempt to authentication bypass using session id capturing or SQL injection

9. **Expected Results for pass:** DUT doesn't allow privilege escalation without authentication

10. **Expected Format of Evidence:** screenshots

11. Test Execution:

11.1 Test Case Number: 01

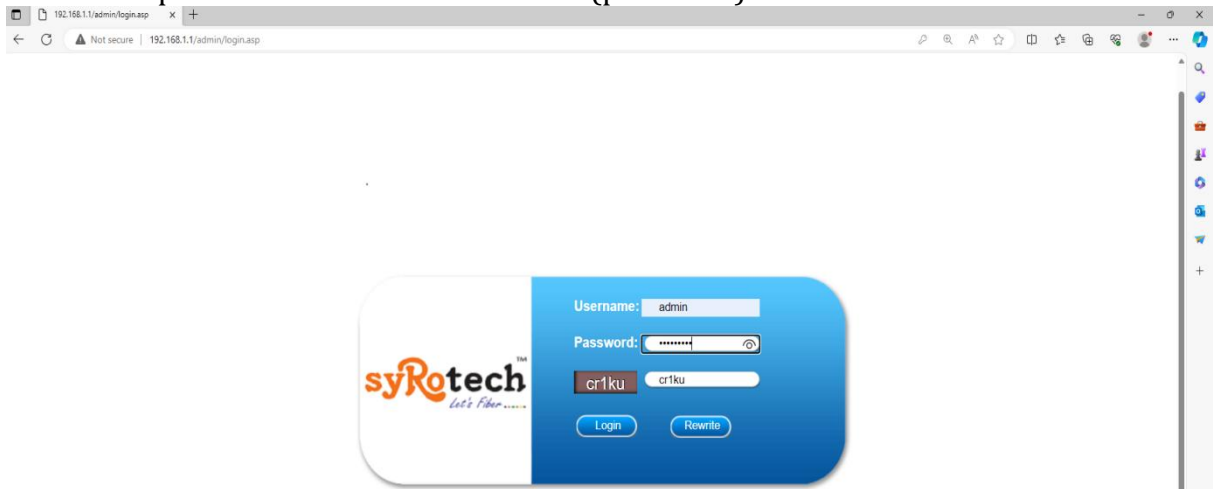
- 11.1.1. Test case Name:** Review OEM documentation
- 11.1.2. Test Case Description:** The Tester shall review a list of operating system functions which a system user can use to explicitly gain higher privileges, and how these functions are configured.
- 11.1.3. Execution Steps:** Review the OEM documentation
- 11.1.4. Test Observation:**
- 11.1.5. Evidence Provided:** -NA-

11.2 Test Case Number: 02

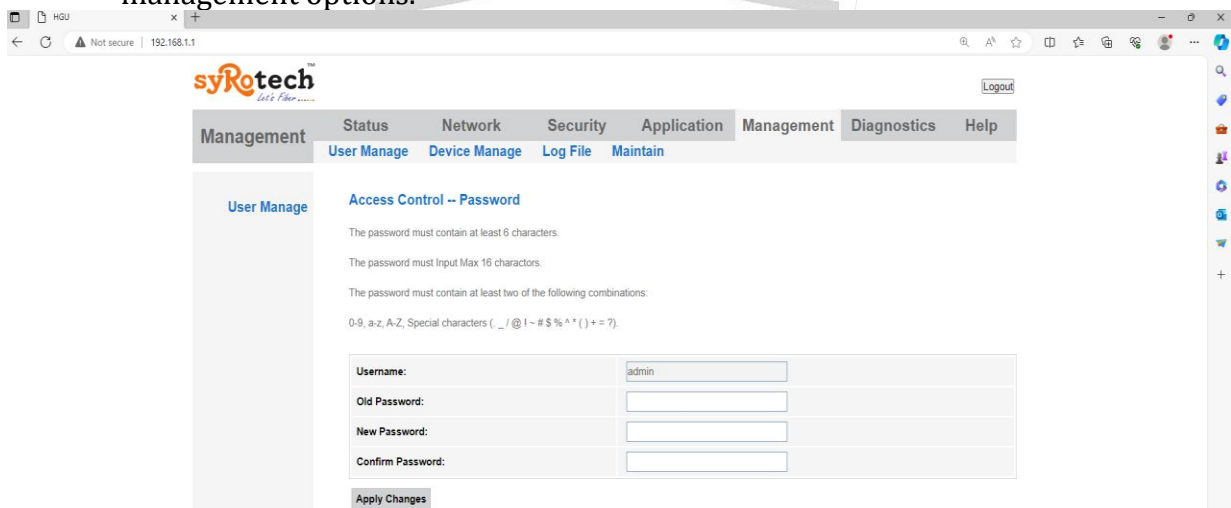
- 11.2.1. Test case Name:** Check privilege escalation method in GUI.
- 11.2.2. Test Case Description:** Check privilege escalation method in GUI.

11.2.3.Execution Steps:

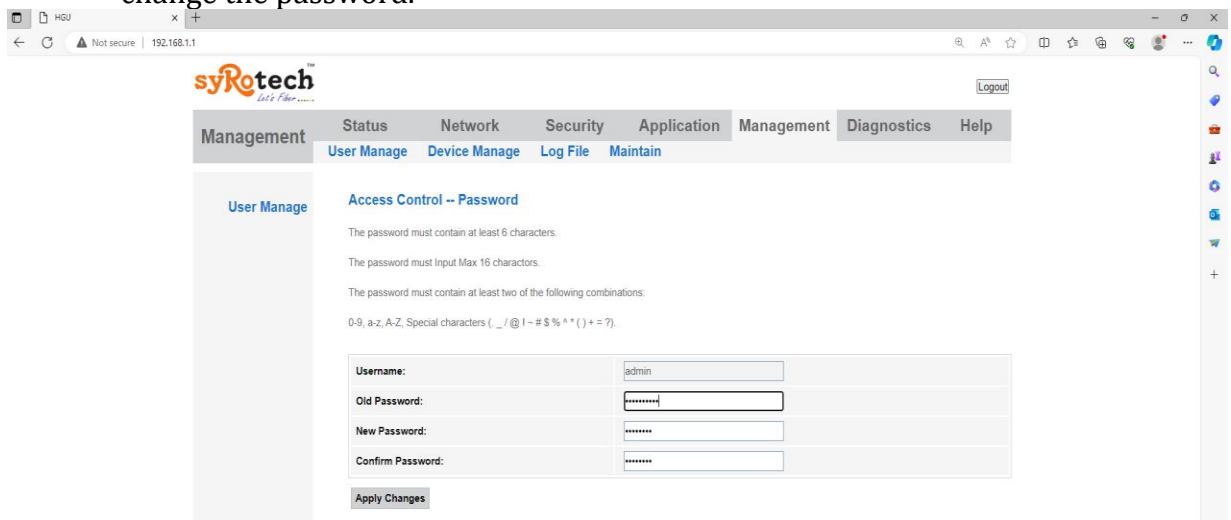
- i. The tester logged into the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) using account "admin" with using the respective authentication attribute(password).



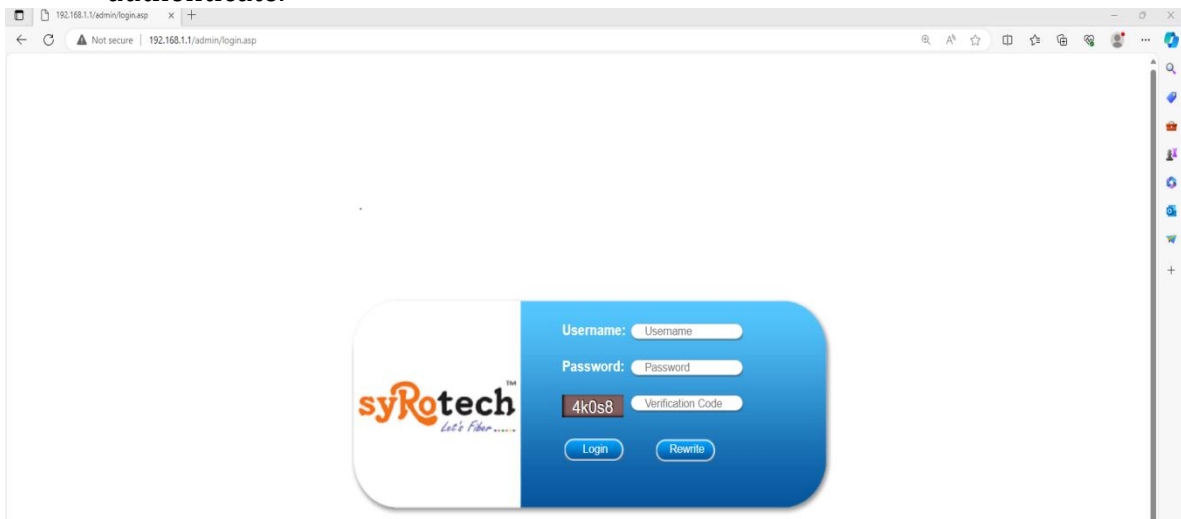
- ii. The Tester clicked on Management > User Manage and check for various user management options.



- iii. The Tester observed that the DUT do not have options of configuring user privileges and other options related to clause requirement. The tester can only change the password.



- iv. The Tester also observed that after every password change user requires to re-authenticate.



11.2.4. Test Observation: The DUT is supplied with a pre-configured single user which acts as an admin user and have all the required privileges to manage the DUT. The tester can only change the password of the DUT and after every password change the user needs to re-authenticate immediately.

11.2.5. Evidence Provided: Screenshots are attached above

11.3 Test Case Number: 03

11.3.1. Test case Name: Authentication bypass

11.3.2. Test Case Description: The tester shall attempt authentication bypass

11.3.3. Execution Steps

- i. The tester shall attempt authentication bypass by using SQL injection
- ii. The Tester may also attempt capturing session cookies/id and use it to bypass authentication

11.3.4. Test Observations: The DUT is supplied with a pre-configured single user which acts as an admin user and have all the required privileges to manage the DUT. The tester can only change the password of the DUT and after every password change the user needs to re-authenticate immediately.

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	REMARKS
1	The Tester shall review a list of operating system functions which a system user can use to explicitly gain higher privileges, and how these functions are configured.		
2	Check privilege escalation method in GUI.		
3	Authentication bypass		

2.10.3 TSTP for System account identification

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.10.3
---	--------------------------	------------------

DUT Details: GPON-ONT

DUT Software Version: V 3.2.02-231205

Digest Hash of OS: Hash of DUT OS is required

Digest Hash of Configuration: Hash of DUT configuration is required

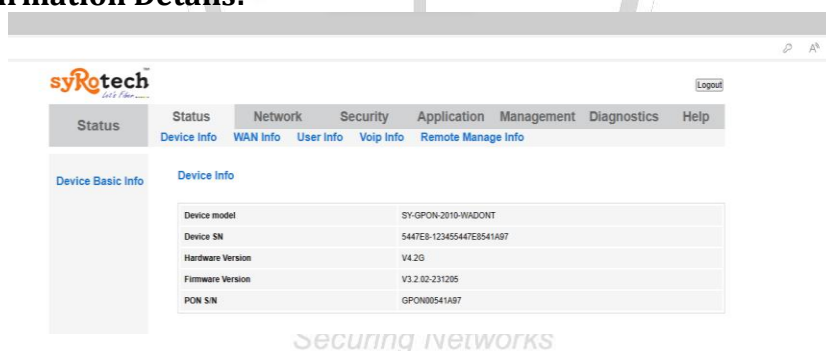
Applicable ITSAR: NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

ITSAR Version No: ONT ITSAR403012311 and Version: 1.0.1

OEM Supplied Document list: All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> **Section 2.10.3: Operating System**
2. <Security Requirement No & Name > 1.10.3: System account identification
3. **Requirement Description:** Each system account in ONU/ONT shall have a unique identification with non-repudiation controls.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. Section 4.2.4.2.2]

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.
6. **Pre-Condition:** OEM shall provide confirmation that each system account in Operating system of the ONT shall have a unique identification. OEM should share the supporting document.
7. **Test Objective/ Purpose:** To verify that each system account in DUT shall have a unique identification with non-repudiation controls
8. **Test Plan**
 - 8.1 **Test Cases:**
 - 8.1.1 Multiple system accounts
 - 8.1.2 Unique Identification (UID)
 - 8.2 **Test-bed setup Diagram:**



8.3 Test tool required per scenario/test case: CLI /GUI Interface

9. Expected Results: DUT each system account in DUT shall have a unique identification with non-repudiation controls

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test case Name: Multiple system accounts

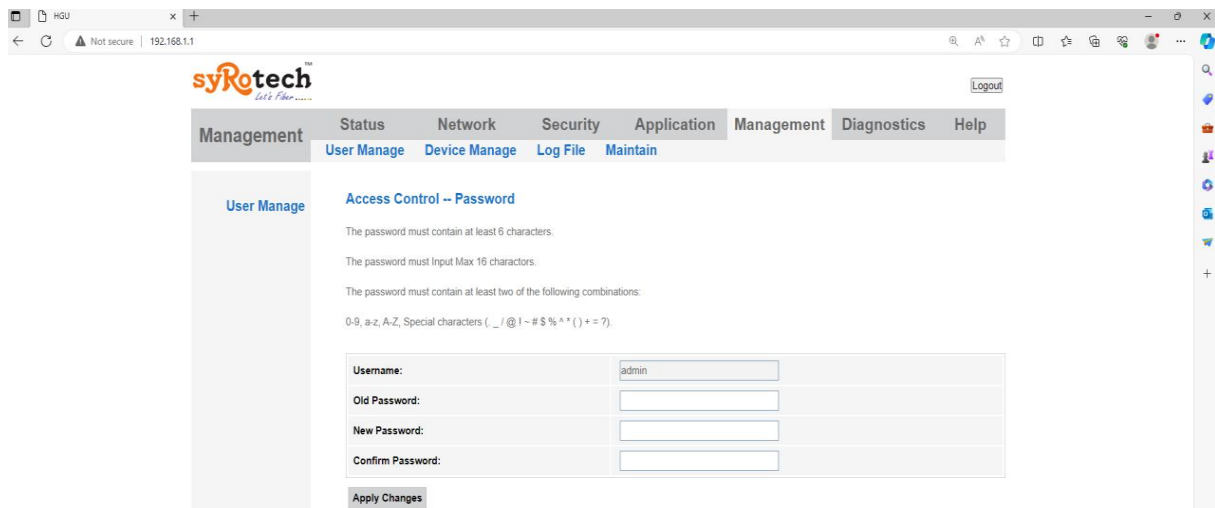
11.1.2. Test Case Description: The Tester shall create multiple system accounts on DUT.

11.1.3. Execution Steps:

- i. In DUT, there is no option to create any system or user account.
- ii. Further to identify system account in Operating system of the DUT, the Tester logged into the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) using account "admin" with using the respective authentication attribute (password).



- iii. The Tester clicked on Management > User Manage and check the various user



iv. The Tester observed that the DUT do not have any option to create the multiple users and check uniqueness of each account. The tester can only change the password.

11.1.4. Test Observation: The Tester observed that the DUT do not have any option to create the multiple users and check uniqueness of each account. The tester can only change the password.

11.1.5. Evidence Provided: Screenshots are attached above

11.2 Test Case Number: 02

11.2.1. Test case Name: The Tester shall check whether all newly created system accounts having a unique identification (UID).

11.2.2. Test Case Description: The Tester shall check whether all newly created system accounts having a unique identification (UID).

11.2.3. Execution Steps: DUT does not have option to create multiple accounts hence unique identification (UID cannot be verified).

11.2.4. Test Observation: DUT does not have option to create multiple accounts hence unique identification (UID cannot be verified).

11.2.5. Evidence Provided: -NA-

i. CASE 1: The Tester observes that the DUT comes with a single user and creation of multiple user accounts is not supported by the DUT.

ii. CASE 2: UIDs cannot be verified at this stage and OEM support is required.

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Multiple system accounts		
2	unique identification (UID)		

2.10.4 TSTP Report for Evaluation OS-Hardening

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.10.4
---	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

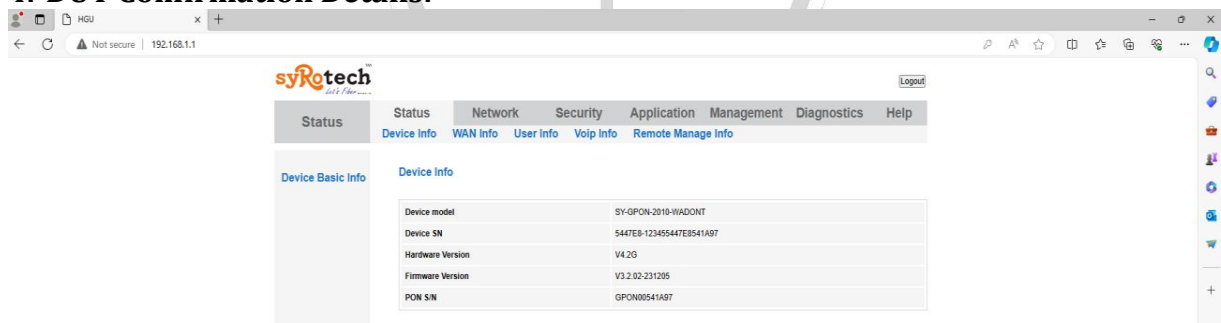
1. <ITSAR Section No & Name> **Section 1.10: Operating System**

2. <Security Requirement No & Name > **1.10.4: OS-Hardening**

3. **Requirement Description:** Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in ONU/ONT Kernel based network functions not needed for the operation of the ONU/ONT shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.2]

4. DUT Confirmation Details:



5. **DUT Configuration:** The DUT is configured to check that the kernel functions are disabled to harden the OS

6. **Precondition:** OEM shall provide OS Hardening undertaken and provide information on steps taken in this regard

7. **Test Objective:** to verify that the Kernel based network functions not needed for the operation of the ONU/ONT are deactivated

8. Test Plan

8.1 Test Cases:

8.1.1 OEM documentation for kernel functions

8.1.2 OS hardening verification

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: CLI/GUI Interface

8.4 Test Execution Steps

- i. The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened
- ii. The Tester shall verify that IP Packet Forwarding / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature are disabled by default on the network product

9. Expected Results for Pass: The Kernel based network functions not needed for the operation of the ONU/ONT are deactivated.

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test case Name: The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened.

11.1.2. Test Case Description: The Tester reviews the process for OS Hardening undertaken from OEM that justify that the OS is sufficiently hardened.

11.1.3. Execution Steps:

- i. Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.4. Test Observation:

- i. Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.5. Evidence Provided: -NA-

11.2 Test Case Number: 02

11.2.1. Test case Name: OS hardening verification

11.2.2. Test Case Description: The Tester shall verify that IP Packet Forwarding / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature are disabled by default on the network product.

11.2.3. Execution Steps:

- i. The Tester checked the DUT and found that there is no IP Packet Forwarding / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature shown in DUT.
- ii. The Tester shall review the OEM document to verify the OS hardening document.

11.2.4. Test Observation:

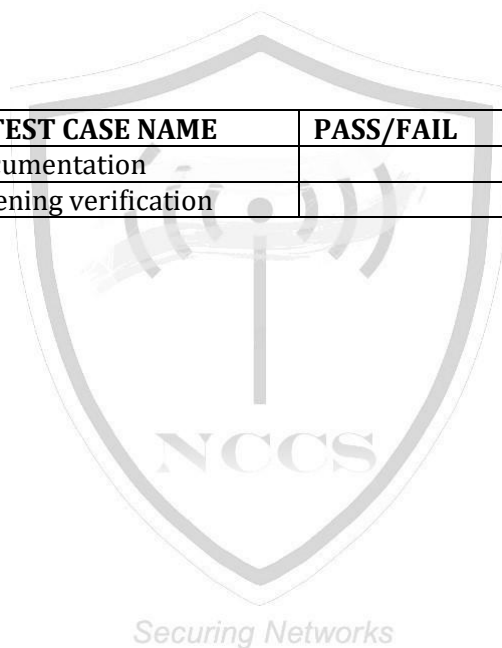
- i. The Tester checked the DUT and found that there is no IP Packet Forwarding / Proxy ARP / Directed broadcast / IP Multicast / Gratuitous ARP feature shown in DUT.
- ii. The Tester shall review the OEM document to verify the OS hardening document.

11.2.5. Evidence Provided: -NA-

- i. CASE 1: Expected observation "DUT is sufficiently hardened and security measures are implemented to ensure the Kernel Security and miniaturization".
- ii. CASE 2: Observation and result will be drawn once the TSTP have OEM support and OEM document.

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM documentation		
2	OS Hardening verification		



2.10.5 TSTP Report for Evaluation No automatic launch of removable media

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.10.5
---	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

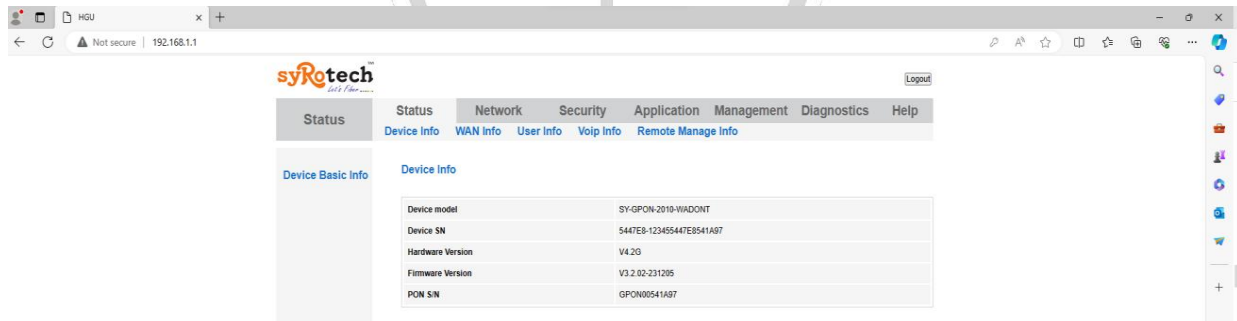
1. <ITSAR Section No & Name> **Section 1.10: Operating System**

2. <Security Requirement No & Name > 2.10.5: No automatic launch of removable media

3. **Requirement Description:** ONU/ONT shall not automatically launch any application when removable media device is connected.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.3.1.3]

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.

6. **Precondition:** OEM shall provide support mechanisms for buffer overflow protection and enabled and/or implemented shall be provided.

7. Test Objective / Purpose:

8. Test Plan

8.1 Test Cases:

8.1.1 The Tester shall review the OEM documentation which supports that the proper restrictions set properly in order to prevent the automatic launch of removable media.

8.1.2 The Tester inserts removable media device (like CD, DVD USB Stick/USB storage device) whichever is supported by the DUT.

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: CLI/GUI Interface

8.4 Test Execution Steps:

- i. The tester log in the network product.
- ii. The tester inserts a removable media device (CD-, DVD-, USB-Sticks and/or USB-Storage drives) in the network product.
- iii. Tester checks if there is launch of any application from the mounted content

9. Expected Results for Pass: The network product does not launch any applications to open the contents in the removable media device. In Linux® machines, the removable media device is not automatically mounted in the filesystem

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test case Name: OEM documentation

11.1.2. Test Case Description: The Tester shall review the OEM documentation which supports that the proper restrictions set properly in order to prevent the automatic launch of removable media.

11.1.3. Execution Steps: -NA-

11.1.4. Test Observation:

- i. Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.5. Evidence Provided: -NA-

11.2 Test Case Number: 02

11.2.1. Test case Name: auto-launch of application.

11.2.2. Test Case Description: The tester checks for the auto-launch of application

11.2.3. Execution Steps:

- i. Load the autorun script onto the external media drive (e.g., USB) that is supported by the DUT.

- ii. Connect the external media drive to the DUT and check if the DUT launches the application or scripts.
- iii. Additionally, reload the DUT and verify if the external media drive is accessible or not.
- iv. The Tester checks if auto-mounting is enabled or not

11.2.4. Test Observation: The tester observes that DUT does not have any option to mount any removable media device like CD/DVD, SD card or USB stick/USB Storage devices. Images of the DUT are attached for reference.

11.2.5. Evidence Provided: -NA-

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	OEM documentation		
2	auto-launch of application.		

Note: This requirement is marked as not applicable as the DUT does not any option to mount any removable media device.



2.10.6 TSTP Report for Evaluation Protection from buffer overflows

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2. 10.6
---	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

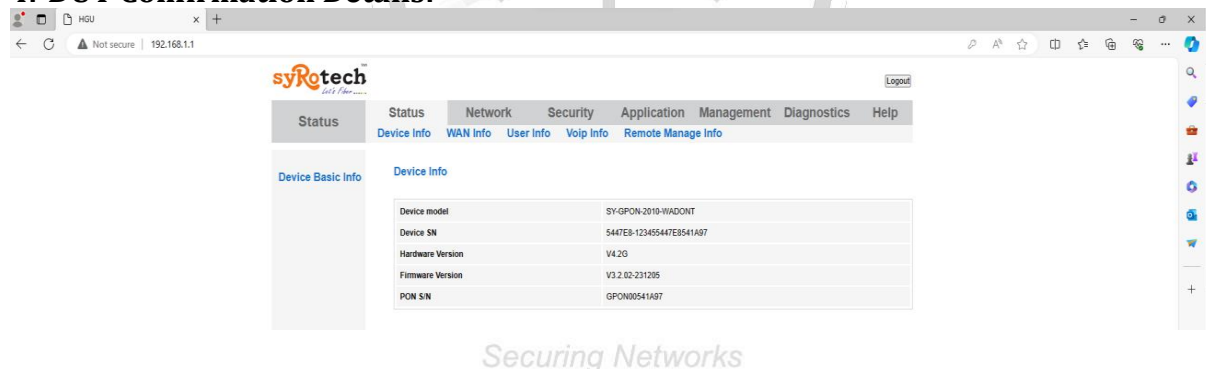
1. <ITSAR Section No & Name> Section 2.10: Operating System

2. <Security Requirement No & Name > 2.10.6: Protection from buffer overflows

3. Requirement Description: ONU/ONT shall support mechanisms for buffer overflow protection.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.5]

4. DUT Confirmation Details:



5. **DUT Configuration:** There is no additional configuration required for this test case.

6. **Precondition:** OEM shall provide support mechanisms for buffer overflow protection and enabled and/or implemented shall be provided.

7. **Test Objective:** To verify that DUT has protection mechanism against buffer overflow

8. Test Plan

8.1 Test Cases:

8.1.1 The Tester shall review the OEM documentation which supports OS-level restrictions set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

8.1.2 The Tester shall review the OEM documentation which supports OS-level restrictions set properly to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems).

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case: CLI/GUI interface

8.4 Test Execution Steps : The accredited evaluator's test lab is required to execute the following steps:

- i. The tester verifies that there is:
 - a. A technical description of the buffer overflow protection mechanisms that have been implemented on the system.
 - b. Details of whether the buffer overflow protection mechanisms are implemented by default or if additional actions (e.g. scripts or commands manually executed) are required.
 - c. If manually executed actions are required then detailed instructions should be included in the technical description.
- ii. The tester verifies that the test results:
 - a) Describe test procedures used to verify the buffer overflow protection mechanisms,
 - b) Contain data which demonstrates/indicates that the buffer overflow protection mechanisms described in the technical description document have been implemented.
 - c) Contains details of the test set-up for the testing of the buffer overflow protection mechanisms. Where simulators and/or scripts are used to artificially create the conditions to trigger the buffer overflow protection mechanism then details of these should also be inc

9. Expected Results for Pass:

- a. A technical description of the buffer overflow protection mechanisms that have been implemented on the system.

- i. Details of whether the buffer overflow protection mechanism are implemented by default or if additional actions (e.g. scripts or commands manually executed) are required.
- ii. If manually executed actions are required then detailed instructions should be included in the technical description.
- b. The test results should:
 - i. Describe test procedures used to verify the buffer overflow protection mechanisms,
 - ii. Contain data which demonstrates/indicates that the buffer overflow protection mechanisms described in the technical description document have been implemented.
 - iii. Contains details of the test set-up for the testing of the buffer overflow protection mechanisms. Where simulators and/or scripts are used to artificially create the conditions to trigger the buffer overflow protection mechanism then details of these should also be inc

10. Expected Format of Evidence: screenshots

11. Test Execution:

11.1 Test Case Number: 01

11.1.1.Test case Name: Buffer overflow protection

11.1.2.Test Case Description: The Tester shall review the OEM documentation which supports OS-level restrictions set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

11.1.3.Execution Steps:

- i. Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.4.Test Observation:

- i. Note: Software test document is not available with lab because this is the market purchased product used for demo testing.

11.1.5.Evidence Provided: -NA-

12. Test Case Results:

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	Buffer Overflow protection		
2			

2.10.7 TSTP Report for External file system mount restrictions

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2. 10.7
---	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1) <ITSAR Section No & Name> **Section 10: Operating System**

2) <Security Requirement No & Name > **10.7: External file system mount restrictions**

3) **Requirement Description:** If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in ONU/ONT in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems. OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g. USB drive, CD ROM etc.) for data transfer.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.6

4) **DUT Confirmation Details:**

The screenshot displays the syrotech web interface. At the top left is the syrotech logo with the tagline 'Let's Fiber...'. The main interface has a 'Status' tab selected, with sub-tabs for Status, Network, Security, Application, Management, Diagnose, and Help. Below these are links for Device Information, WAN Connection Info, User Information, VOIP Information, and Remote Management Status. The 'Device Basic Info' section is expanded, showing a table with the following details:

Device Model	HGU
Device ID	8014A8-F32428014A8000000
Hardware Version	STD-ONU
Software Version	3.1.02-220505
Serial No	RTKG11111111



Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
FXS	1 Port(s)	Physical	FXS
GUI	-	Man-Machine	Syrotech

5) **DUT Configuration:** Configure the DUT to mount external file system

6) Precondition:

- i. OEM to give the details on the list of files, directories and their associated permissions.
- ii. OEM should provide documentation on the list of functions and commands supported by the DUT's OS.
- iii. The OEM should provide documentation specifying whether the DUT supports external media drives, such as USB. If supported, the USB mount path should be included.

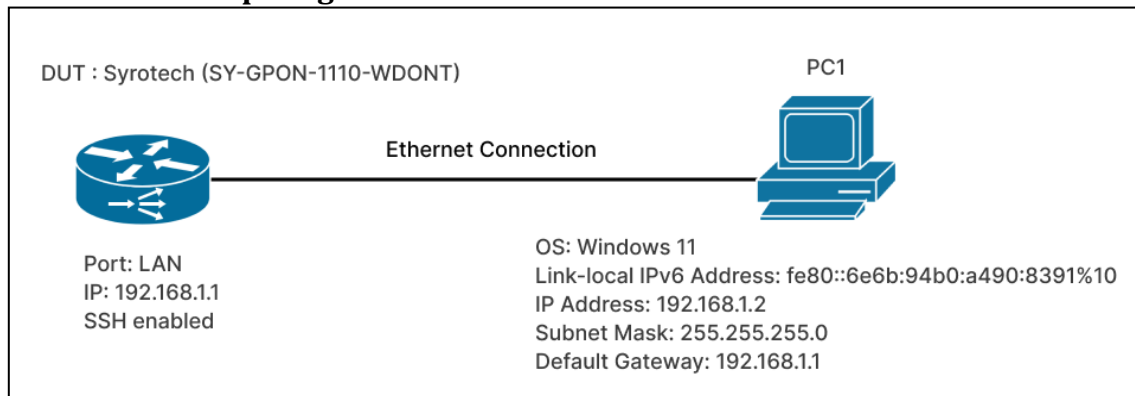
7) Test Objective: - To verify that DUT doesn't allow privilege escalation due to external mounted contents

8) Test Plan

8.1 Test Cases:

8.1.1 Mount external file system

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case:

8.4 Test Execution steps

- i. Create an executable file that requires root privileges using SUID configuration and make the root user the owner of the file.
- ii. Connect the external media drive to the DUT and move/ or copy the file to an external media drive.
- iii. Check and verify the privilege/ or permission of the moved file on the external media drive.
- iv. Ensure that the SUID bit has been disabled or not.

9) Expected Results for Pass: - DUT should not let privilege escalation upon executing the mounted contents in the DUT

10) Expected format of evidence: screenshots

11) Test Execution:

11.1 Test Case Number: 8.1

11.2 Test case Name: Mount external file system

11.3 Test Case Description: Verification of the user account not allowed to mount external file system.

11.4 Execution Steps:

- i. Create an executable file that requires root privileges using SUID configuration and make the root user the owner of the file.
- ii. Connect the external media drive to the DUT and move/ or copy the file to an external media drive.
- iii. Check and verify the privilege/ or permission of the moved file on the external media drive.
- iv. Ensure that the SUID bit has been disabled or not.

11.5 Evidence provided:- DUT lacks USB port hence the test cannot be performed

11.6 Test Observations

- i. **Test Case 8.1:** DUT lacks USB port hence the test cannot be performed

12) Test Result

ITSAR ONU-ONT No.	Test name	Actual Result
1.	Mount external file system	



2.10.8 TSTP Report for File-system Authorization privileges

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2. 10.8
---	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1) **<ITSAR Section No & Name>**: Section 10: Operating System

2) **<Security Requirement No & Name >** 10.8: File-system Authorization privileges

3) **Requirement Description:** ONU/ONT shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.

4) **DUT Confirmation Details:**

The screenshot displays the syrotech web management interface. At the top left is the syrotech logo with the tagline 'Let's Fiber.....'. The main navigation bar includes tabs for Status, Network, Security, Application, Management, Diagnose, and Help. Below this, a secondary bar shows links for Device Information, WAN Connection Info, User Information, VOIP Information, and Remote Management Status. The 'Status' tab is active, showing 'Device Basic Information' on the left and a table of device details on the right. The table lists the following information:

Device Basic Info	
Device Model	HGU
Device ID	8014A8-F32428014A8000000
Hardware Version	STD-ONU
Software Version	3.1.02-220505
Serial No	RTKG11111111

At the top right of the interface, it shows 'Gateway Name: HGU' and a 'Logout' button.



Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
FXS	1 Port(s)	Physical	FXS
GUI	-	Man-Machine	Syrotech

5) DUT Configuration: NA

6) Pre-Condition: - OEM to give the details on authorization policy supported by the DUT.

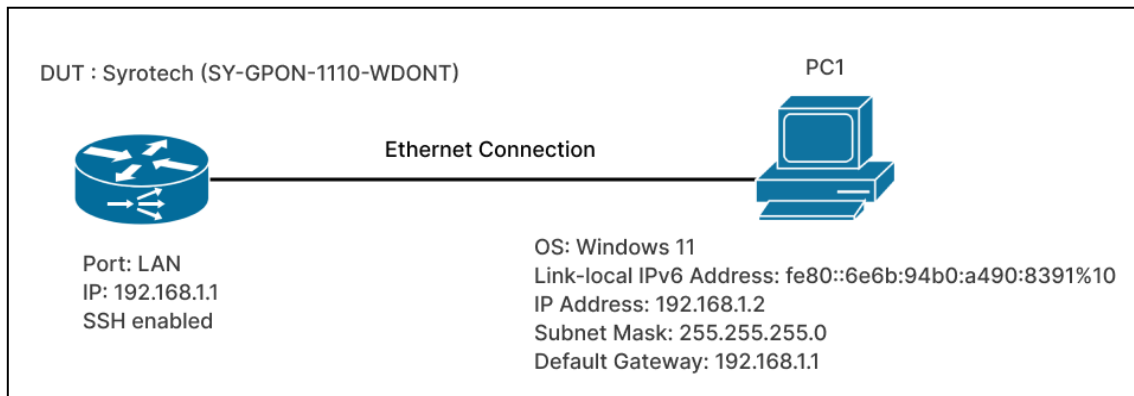
7) Test Objective: - To verify that the DUT allows only privileged users to modify files, data, directories or file systems

8) Test Plan

8.1 Test Cases:

8.1.1 User authorization

8.2 Test-bed setup Diagram:



8.3 Test tool required per scenario/test case:

8.4 Test Execution steps:- Open PuTTY and enter the IP address 192.168.1.1 and verify authorization to modify the file data by running the specified command in the terminal.

admin

admin123

enterlinuxshell

ls

cat chip_type

echo "Deltaphi" > chip_type

cat chip_type

To create a file running the specified command in the terminal.

touch test.txt

ls

rm -rf test.txt

ls

Verify that only the authorized root user can create, edit, delete files and directories, and modify data.

low privilege user: Open PuTTY and enter the IP address 192.168.1.1 and verify user privilege to modify the file data by running the specified command in the terminal

user

user

enterlinuxshell

Verify that only the user privilege cannot create, edit, delete files and directories, and modify data.

9) Expected Results for Pass: - DUT should maintain the authorization policy by letting the authorized users to modify files, data, directories or file systems

10) Expected format of evidence: screenshots

11) Test Execution:

11.1 Test Case Number: 8.1

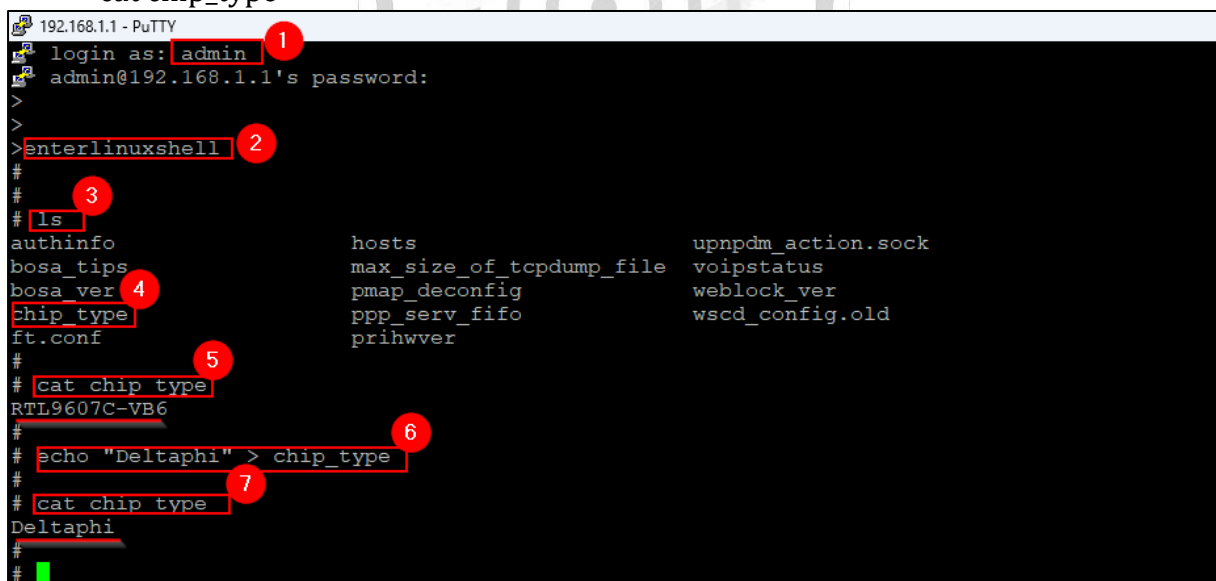
11.2 Test case Name: User authorization

11.3 Test Case Description: The tester verifies that only users that are authorized to modify files, data, directories or file systems have the necessary privileges.

11.4 Execution Steps:

- i. Open PuTTY and enter the IP address 192.168.1.1 and verify authorization to modify the file data by running the specified command in the terminal - as shown in Figure 4.1.6.1.

```
admin
admin123
enterlinuxshell
ls
cat chip_type
echo "Deltaphi" > chip_type
cat chip_type
```



```
192.168.1.1 - PuTTY
login as: admin
admin@192.168.1.1's password:
>
> enterlinuxshell
#
#
# ls
authinfo          hosts             upnpdm_action.sock
bosa_tips         max_size_of_tcpdump_file voipstatus
bosa_ver         pmap_deconfig    webblock_ver
chip_type         ppp_serv_fifo    wscd_config.old
ft.conf          prihwver
#
# cat chip_type
RTL9607C-VB6
#
# echo "Deltaphi" > chip_type
#
# cat chip_type
Deltaphi
#
```

Figure 4.1.6.1- Verify admin privilege edit the modify the data in the file

- ii. To create a file running the specified command in the terminal- as shown in figure 4.1.6.2

```
touch test.txt
ls
rm -rf test.txt
ls
```

```
# touch test.txt 1
# ls
authinfo          hosts             test.txt
bosa_tips         max_size_of_tcpdump_file upnpdm_action.sock
bosa_ver          pmap_deconfig    voipstatus
chip_type         ppp_serv_fifo    webblock_ver
ft.conf           prihwver          wscd_config.old
# rm -rf test.txt 2
# ls
authinfo          hosts             upnpdm_action.sock
bosa_tips         max_size_of_tcpdump_file voipstatus
bosa_ver          pmap_deconfig    webblock_ver
chip_type         ppp_serv_fifo    wscd_config.old
ft.conf           prihwver
#
```

Figure 4.1.6.2 - Verify admin privilege creates and deletes data in the directory.

iii. Verify that only the authorized root user can create, edit, delete files and directories, and modify data.

iv. **low privilege user:**

v. Open PuTTY and enter the IP address 192.168.1.1 and verify user privilege to modify the file data by running the specified command in the terminal - as shown in Figure 4.1.6.3.

user

user

enterlinuxshell

```
192.168.1.1 - PuTTY
login as: user
user@192.168.1.1's password:
>
> enterlinuxshell
command error!

config          Configure system
exit            Exit command line interface
help           Help information
reboot         Reboot system
show           Show system information
>
```

Figure 4.1.6.2 - Verify user privilege cannot enter into linuxshell

vi. Verify that only the user privilege cannot create, edit, delete files and directories, and modify data.

11.5 Evidence Provided:

i. **Admin privilege user (root):**

a. Admin privilege can able to create, edit, and delete files and directories.


```

192.168.1.1 - PuTTY
login as: admin
admin@192.168.1.1's password:
>
> enterlinuxshell
#
#
# ls
authinfo          hosts             upnpdm_action.sock
bosa_tips         max_size_of_tcpdump_file  voipstatus
bosa_ver         pmap_deconfig    weblock_ver
chip_type        ppp_serv_fifo    wscd_config.old
ft.conf          prihwver
#
# cat chip type
RTL9607C-VB6
#
# echo "Deltaphi" > chip_type
#
# cat chip type
Deltaphi
#
#
# touch test.txt
#
# ls
authinfo          hosts             test.txt
bosa_tips         max_size_of_tcpdump_file  upnpdm_action.sock
bosa_ver         pmap_deconfig    voipstatus
chip_type        ppp_serv_fifo    weblock_ver
ft.conf          prihwver         wscd_config.old
#
# rm -rf test.txt
#
# ls
authinfo          hosts             upnpdm_action.sock
bosa_tips         max_size_of_tcpdump_file  voipstatus
bosa_ver         pmap_deconfig    weblock_ver
chip_type        ppp_serv_fifo    wscd_config.old
ft.conf          prihwver
#
#

```

ii. low privilege user:

- a. low privilege user cannot able to create, edit, delete files and directories.

```

192.168.1.1 - PuTTY
login as: user
user@192.168.1.1's password:
>
> enterlinuxshell
command error!
config          Configure system
exit            Exit command line interface
help           Help information
reboot         Reboot system
show           Show system information
>

```

11.6 Test Observations: Test Case 8.1: DUT lacks USB port hence the test cannot be performed

12) Test Result

ITSAR ONU-ONT No.	Test name	Actual Result
1.	Mount external file system	

Section 11: Web Servers

2.11.1 TSTP Evaluation for HTTP

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.1
--	--------------------------	------------------

<DUT Details: > Alphion AONT100C

<DUT Software Version:> R2.0.9.6

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

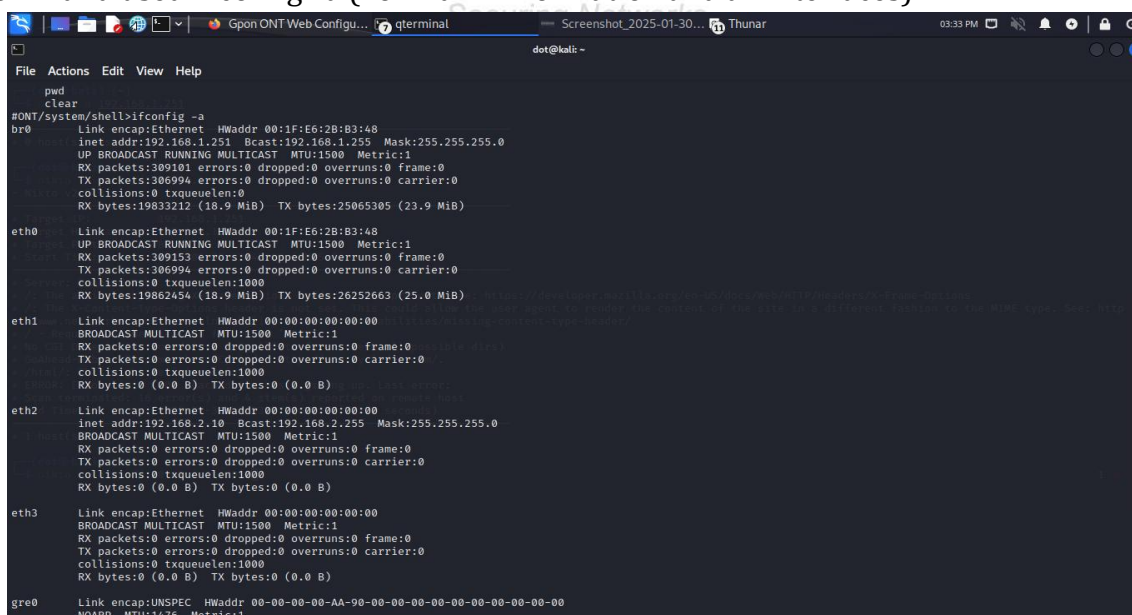
1. <ITSAR Section No & Name> Section 11: Web Server
2. <Security Requirement No & Name > 1.11.1 HTTP
3. <Requirement Description: > The communication between Web client and Web server to be protected using industry standard secured communication protocols TLS/HTTPS. Cipher suites with NULL encryption shall not be supported. ONU/ONT to be protected against sniffing and side jacking attacks.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.1]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
- ii. Use command to get Application No/Version No & Kernel Info

Command used: ifconfig -a (To find IP information and all interfaces)



```
dot@kali: ~
File Actions Edit View Help
pwd
clear
#ONT/system/shell>ifconfig -a
br0:  Link encap:Ethernet  HWaddr 00:1F:E6:2B:B3:48
      inet addr:192.168.1.251  Bcast:192.168.1.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0:  Link encap:Ethernet  HWaddr 00:1F:E6:2B:B3:48
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1:  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2:  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
      inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3:  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0:  Link encap:UNSPEC  HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
      NOARP  MTU:1476  Metric:1
```

The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer N: R2.0.9.6
#ONT/system>
```

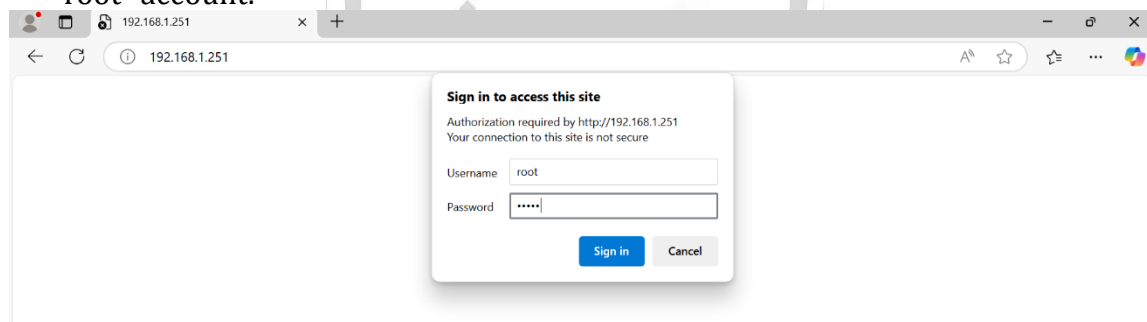
The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

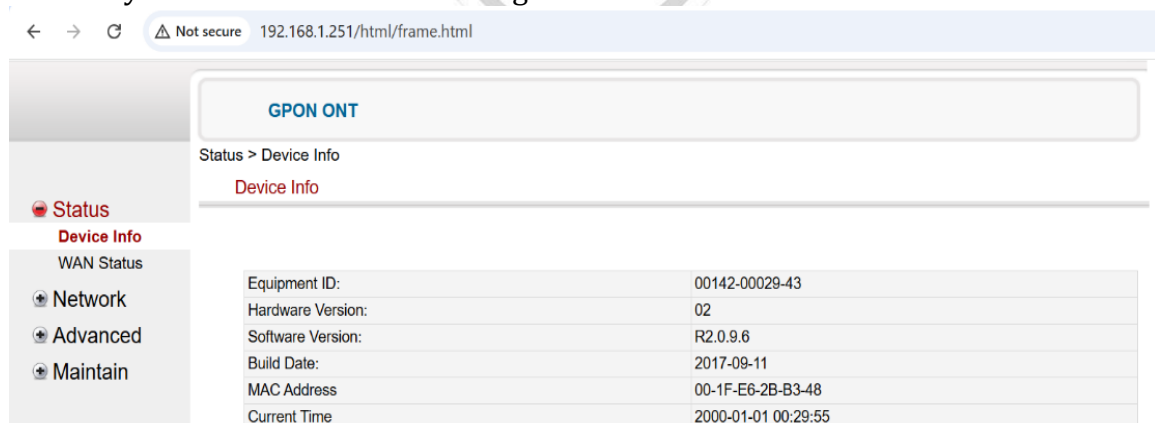
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file  : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address

GPON ONT

Network > WAN

WAN

Internet Connection Type: Static IP

IP Address	192	168	2	10
Subnet Mask	255	255	0	
Default Gateway	192	168	2	1
DNS Server 1	192	168	2	10
DNS Server 2	192	168	2	11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6. Pre-Condition:

- Network product documentation containing information about supported Web Servers and Protocol to communicate with the Web Server in the DUT is provided by the vendor.
- A peer implementing the security protocol same as the one configured by the vendor on DUT for Web Server, (e.g., HTTPS client) shall be available.
- Network product documentation stating which security protocols for protection of data in transit are implemented and which profiles in TS 33.310 [9] and TS 33.210 [X] are applicable is provided by the vendor.
- For TLS, the tester shall base the tests on the profile defined by 3GPP in TS 33.310 [9].
- Test environment with a Web Browser.
- All ciphers supported by the server need to be checked that they are as per Table 1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)"
- For example in apache httpd running on ubuntu 20.04 the command *openssl ciphers -v* is used to check all supported ciphers. The tester must ensure there are no weak ciphers and if so those ciphers must be removed from configuration before conducting the rest of the test. If this fails - **TEST FAILS**

```

naan30@naa30-pc:~$ openssl ciphers -v
TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any Enc=CHACHA20/POLY1305(256) Mac=AEAD
TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=any Au=any Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-ECDSA-AES256-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
ECDHE-RSA-AES256-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
RSA-PSK-AES256-GCM-SHA384 TLSv1.2 Kx=RSAPSK Au=RSA Enc=AESGCM(256) Mac=AEAD
DHE-PSK-AES256-GCM-SHA384 TLSv1.2 Kx=DHEPSK Au=PSK Enc=AESGCM(256) Mac=AEAD
RSA-PSK-CHACHA20-POLY1305 TLSv1.2 Kx=RSAPSK Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
DHE-PSK-CHACHA20-POLY1305 TLSv1.2 Kx=DHEPSK Au=PSK Enc=CHACHA20/POLY1305(256) Mac=AEAD
ECDHE-PSK-CHACHA20-POLY1305 TLSv1.2 Kx=ECOEPSK Au=PSK Enc=CHACHA20/POLY1305(256) Mac=AEAD
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
PSK-AES256-GCM-SHA384 TLSv1.2 Kx=PSK Au=PSK Enc=AESGCM(256) Mac=AEAD
PSK-CHACHA20-POLY1305 TLSv1.2 Kx=PSK Au=PSK Enc=CHACHA20/POLY1305(256) Mac=AEAD
RSA-PSK-AES128-GCM-SHA256 TLSv1.2 Kx=RSAPSK Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-PSK-AES128-GCM-SHA256 TLSv1.2 Kx=DHEPSK Au=PSK Enc=AESGCM(128) Mac=AEAD
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
PSK-AES128-GCM-SHA256 TLSv1.2 Kx=PSK Au=PSK Enc=AESGCM(128) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
ECDHE-PSK-AES256-CBC-SHA384 TLSv1 Kx=ECOEPSK Au=PSK Enc=AES(256) Mac=SHA384
PSK-AES256-CBC-SHA TLSv1 Kx=ECOEPSK Au=PSK Enc=AES(256) Mac=SHA1
SRP-RSA-AES-256-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(256) Mac=SHA1
SRP-AES-256-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(256) Mac=SHA1
RSA-PSK-AES256-CBC-SHA384 TLSv1 Kx=RSAPSK Au=RSA Enc=AES(256) Mac=SHA384
DHE-PSK-AES256-CBC-SHA384 TLSv1 Kx=DHEPSK Au=PSK Enc=AES(256) Mac=SHA384
RSA-PSK-AES256-CBC-SHA SSLv3 Kx=RSAPSK Au=RSA Enc=AES(256) Mac=SHA1
DHE-PSK-AES256-CBC-SHA SSLv3 Kx=DHEPSK Au=PSK Enc=AES(256) Mac=SHA1
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
PSK-AES256-CBC-SHA384 TLSv1 Kx=PSK Au=PSK Enc=AES(256) Mac=SHA384
PSK-AES256-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(256) Mac=SHA1
ECDHE-PSK-AES128-CBC-SHA256 TLSv1 Kx=ECOEPSK Au=PSK Enc=AES(128) Mac=SHA256
ECDHE-PSK-AES128-CBC-SHA TLSv1 Kx=ECOEPSK Au=PSK Enc=AES(128) Mac=SHA1
SRP-RSA-AES-128-CBC-SHA SSLv3 Kx=SRP Au=RSA Enc=AES(128) Mac=SHA1
SRP-AES-128-CBC-SHA SSLv3 Kx=SRP Au=SRP Enc=AES(128) Mac=SHA1
RSA-PSK-AES128-CBC-SHA256 TLSv1 Kx=RSAPSK Au=RSA Enc=AES(128) Mac=SHA256
DHE-PSK-AES128-CBC-SHA256 TLSv1 Kx=DHEPSK Au=PSK Enc=AES(128) Mac=SHA256
RSA-PSK-AES128-CBC-SHA SSLv3 Kx=RSAPSK Au=RSA Enc=AES(128) Mac=SHA1
DHE-PSK-AES128-CBC-SHA SSLv3 Kx=DHEPSK Au=PSK Enc=AES(128) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
PSK-AES128-CBC-SHA256 TLSv1 Kx=PSK Au=PSK Enc=AES(128) Mac=SHA256
PSK-AES128-CBC-SHA SSLv3 Kx=PSK Au=PSK Enc=AES(128) Mac=SHA1

```

7. **Test Objective:** The communication between Web client and Web server shall be protected using TLS.

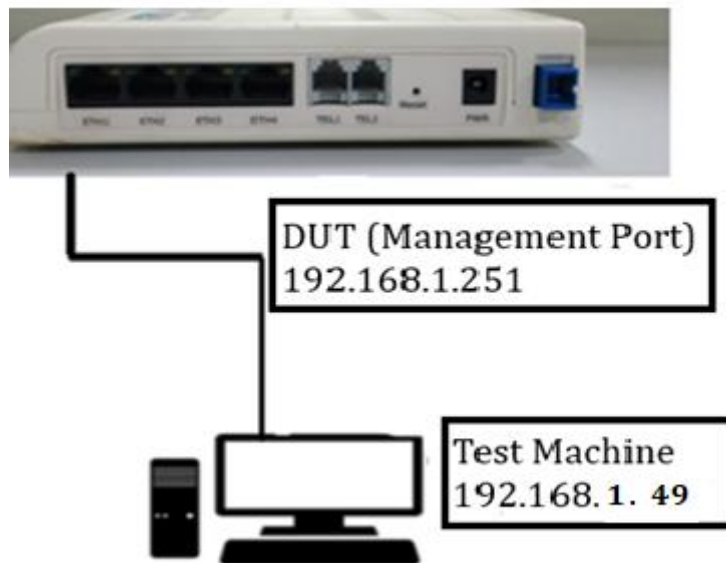
8. Test Plan

8.1. **Test Cases:** Check traffic is properly protected and TLS is being used or not

8.2. Number of Test Scenarios:

8.1.1 **Test Scenario for HTTP:** Check traffic is properly protected and TLS is being used or not

8.3. **Test-bed setup Diagram:**



8.4. Tools Required

- i. Testssl
- ii. Browser

8.5. Test Execution Steps

- i. Open any web browser and initiate a connection to the target server using the HTTP protocol to verify whether the communication between the client and server occurs over HTTP.
- ii. The tester initiates a connection to the target server using the SSL/TLS protocol, specifying a particular version (e.g., TLS 1.0, TLS 1.2).
- iii. Take note of the cipher suites supported by the Device Under Test (DUT) during the SSL/TLS handshake.
- iv. Follow the steps for each supported cipher suite, both secure and weak, to thoroughly test the server's configuration.
- v. Check all supported ciphers and verify that the DUT supports secure ciphers. Ensure that the server does not support null encryption.
Note: Utilize an automated tool such as **Testssl** to streamline and automate the testing process.
- vi. Verify DUT is protected against sniffing and side jacking attacks.

9. Expected Results for Pass:

- i. **Case 1:** The ciphers supported by the Device Under Test (DUT) should align with the recommendations outlined in the Cryptography ITSAR.

10. Expected Format of Evidence: Screenshots of Testing

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC1_SUPPORT_CIPHERS

11.1.2. **Test Case Description:** The communication between Web client and Web server shall be protected using TLS.

11.1.3. **Execution Steps:**

- i. Step 1: Open kali Linux and type the command “testssl https://172.16.1.50” and observe the response

```
(kali@kali)-[~]
$ testssl https://172.16.1.50

#####
testssl      3.2rc3 from https://testssl.sh/dev/

This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

Please file bugs @ https://testssl.sh/bugs/

#####

Using "OpenSSL 3.1.4 24 Oct 2023 (Library: OpenSSL 3.1.4 24 Oct 2023)" [~94 ciphers]
on kali:/usr/bin/openssl
(built: "Nov 25 20:35:59 2023", platform: "debian-amd64")

Start 2024-02-22 01:35:07      —> 172.16.1.50:443 (172.16.1.50) <—

rDNS (172.16.1.50):      --
Service detected:      HTTP

Testing protocols via sockets except NPN+ALPN

SSLv2      not offered (OK)
SSLv3      not offered (OK)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
NPN/SPDY   not offered
ALPN/HTTP2 not offered

Testing cipher categories

NULL ciphers (no encryption)      not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL)      not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export) not offered (OK)
Triple DES Ciphers / IDEA          not offered
Obsoleted CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) with no FS offered (OK)
Forward Secrecy strong encryption (AEAD ciphers) not offered
```

```

Testing server's cipher preferences.
Hexcode Cipher Suite Name (OpenSSL) KeyExch. Encryption Bits Cipher Suite Name (IANA/RFC)
SSLv2
-
SSLv3
-
TLSv1
-
TLSv1.1
-
TLSv1.2 (server order)
x9d AES256-GCM-SHA384 RSA AESGCM 256 TLS_RSA_WITH_AES_256_GCM_SHA384
x9c AES128-GCM-SHA256 RSA AESGCM 128 TLS_RSA_WITH_AES_128_GCM_SHA256
x3c AES128-SHA256 RSA AES 128 TLS_RSA_WITH_AES_128_CBC_SHA256
x3d AES256-SHA256 RSA AES 256 TLS_RSA_WITH_AES_256_CBC_SHA256
x35 AES256-SHA RSA AES 256 TLS_RSA_WITH_AES_256_CBC_SHA
x84 CAMELLIA256-SHA RSA Camellia 256 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
x2f AES128-SHA RSA AES 128 TLS_RSA_WITH_AES_128_CBC_SHA
x41 CAMELLIA128-SHA RSA Camellia 128 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLSv1.3
-
Has server cipher order? yes (OK)

Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES, RC4
No ciphers supporting Forward Secrecy (FS) offered

Testing server defaults (Server Hello)
TLS extensions (standard) "renegotiation info/#65281" "session ticket/#35" "heartbeat/#15"
Session Ticket RFC 5077 hint 7200 seconds, session tickets keys seems to be rotated < daily
SSL Session ID support yes
Session Resumption Tickets: yes, ID: yes
TLS clock skew Random values, no fingerprinting possible
Client Authentication none
Signature Algorithm SHA256 with RSA
Server key size RSA 2048 bits (exponent is 65537)
Server key usage
Server extended key usage TLS Web Server Authentication
Serial 73640A80 NOT ok: length should be ≥ 64 bits entropy (is: 4 bytes)
Fingerprints
SHA1 E9DA90E81AE84653F9438F310843EFA154904D33
SHA256 02129264D298591045C8D1A524B99362EA27931CB8D9709C006E52744E6FB512
Common Name (CN) ciscobusiness.cisco
subjectAltName (SAN) 172.16.1.50 ciscobusiness.cisco https://ciscobusiness.cisco

OpenSSL 1.1.0l (Debian) TLSv1.2 AES256-GCM-SHA384 No FS
OpenSSL 1.1.1d (Debian) TLSv1.2 AES256-GCM-SHA384 No FS
OpenSSL 3.0.3 (git) TLSv1.2 AES256-GCM-SHA384 No FS
Apple Mail (16.0) TLSv1.2 AES256-GCM-SHA384 No FS
Thunderbird (91.9) TLSv1.2 AES256-GCM-SHA384 No FS

Rating (experimental)
Rating specs (not complete) SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
Specification documentation https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
Protocol Support (weighted) 0 (0)
Key Exchange (weighted) 0 (0)
Cipher Strength (weighted) 0 (0)
Final Score 0
Overall Grade F
Grade cap reasons
Grade capped to T. Issues with the chain of trust (self signed)
Grade capped to B. Forward Secrecy (FS) is not supported
Grade capped to A. HSTS is not offered

Done 2024-02-22 01:36:22 [ 695s ] —> 172.16.1.50:443 (172.16.1.50) <—

```

ii. From the above image, we verified the fingerprints, signature, TLS version, supported cipher and null encryption by the server.

11.1.4. Test Observations:

- i. The communication channel between the Network product and its client is encrypted using TLSv1.2,
- ii. The DUT supported the weak cipher, Fingerprint and signature algorithm

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC1_SUPPORT_CIPHERS		

211.2 TSTP for Evaluation of Web Server Logging

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.2
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed her

1. <ITSAR Section No & Name> Section 11: Webserver

2. <Security Requirement No & Name > 1.11.2 Webserver logging

3. <Requirement Description:> Access to the ONU/ONT webserver (for both successful as well as failed attempts) shall be logged by ONU/ONT.

The web server log shall contain the following information:

- i. Access timestamp
- ii. Source (IP address)
- iii. Account (if known)
- iv. Attempted login name (if the associated account does not exist)
- v. Relevant fields in http request. The URL should be included whenever possible.
- vi. Status code of web server response

These logs should be exportable to external syslog server using secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)".

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.2.1]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
- ii. Use command to get Application No/Version No & Kernel Info
 - Command used: **ifconfig -a** (To find IP information and all interfaces)

```

dot@kali: ~
File Actions Edit View Help
pwd
clear
#ONT/system>shell>ifconfig -a
br0
Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48
inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)

eth0
Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)

eth1
Link encap:Ethernet HWaddr 00:00:00:00:00:00
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth2
Link encap:Ethernet HWaddr 00:00:00:00:00:00
inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth3
Link encap:Ethernet HWaddr 00:00:00:00:00:00
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

gre0
Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00
NOARP MTU:1476 Metric:1

```

- The below screenshot shows the firmware version of the DUT

```

#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>

```

- The below screenshot shows the information of the DUT

```

#ONT/system>custom
Customer Information

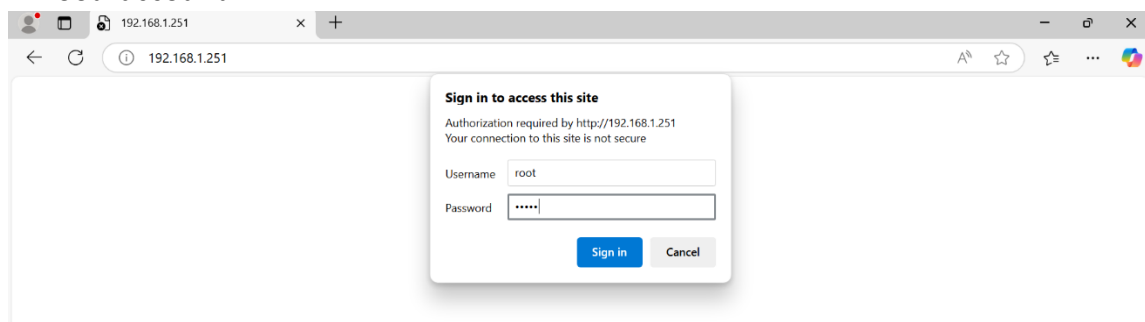
Customer Name       : UUAP
Customer Full Name  : Alphion
System Config file  : /etc/sys.cfg.alp
#ONT/system>

```

Securing Networks

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using "root" account.



- Verify the DUT information through device info

← → ↻ ⚠ Not secure 192.168.1.251/html/frame.html

GPON ONT

Status > Device Info

Device Info

Status
 Device Info
 WAN Status
 Network
 Advanced
 Maintain

Equipment ID:	00142-00029-43
Hardware Version:	02
Software Version:	R2.0.9.6
Build Date:	2017-09-11
MAC Address	00-1F-E6-2B-B3-48
Current Time	2000-01-01 00:29:55

iv. Set the static IP address

Gpon ONT Web Configuration × +

← ↻ ⚠ Not secure | 192.168.1.251/html/frame.html

GPON ONT

Network > WAN

WAN

Status
 Network
 LAN
 WAN
 Advanced
 Maintain

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Status
 Device Info
 WAN Status
 Network
 Advanced
 Maintain

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6. Preconditions

- Network Product documentation which contains information on log file location and procedure to access it.
- Tester has the necessary privileges to access the log files.
- Test environment with a Web Browser.

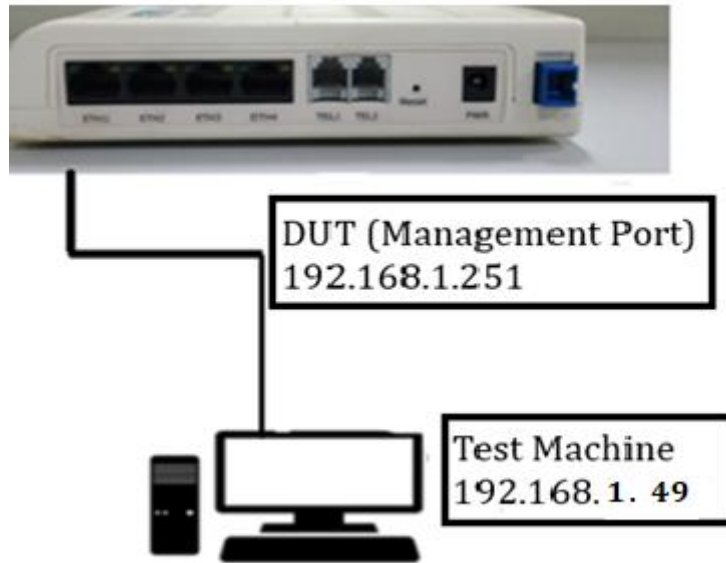
7. Test Objective: Verify that all accesses to the webserver are logged with the required information.

8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Check whether the web server is logging the user login

8.2 Test Setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to login to the webserver using the correct and incorrect login credentials.
- iii. The tester verifies whether the login attempts were logged correctly with all the required information.

9. Expected Results for Pass: All webserver events are logged with all of the required information.

10. Expected Format of Evidence: Testing report contains copies of the log file showing the captured information.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_WEBSERVER_LOGGING

11.1.2. Test Case Description: Verify that all accesses to the webserver are logged with the required information

The web server log shall contain the following information:

- i. Access timestamp - Source (IP address)
- ii. Account (if known)
- iii. Attempted login name (if the associated account does not exist)
- iv. Relevant fields in http request. The URL should be included whenever possible.
- v. Status code of web server response

11.1.3. Execution Steps: The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT

- i. URL: <http://<IP address of DUT>> And enter the right credentials.

2.11.3 TSTP Report for Evaluation

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.3
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

24. <ITSAR Section No & Name> Section 11: Web Server

1. <Security Requirement No & Name > 1.11.3 HTTPS input validation

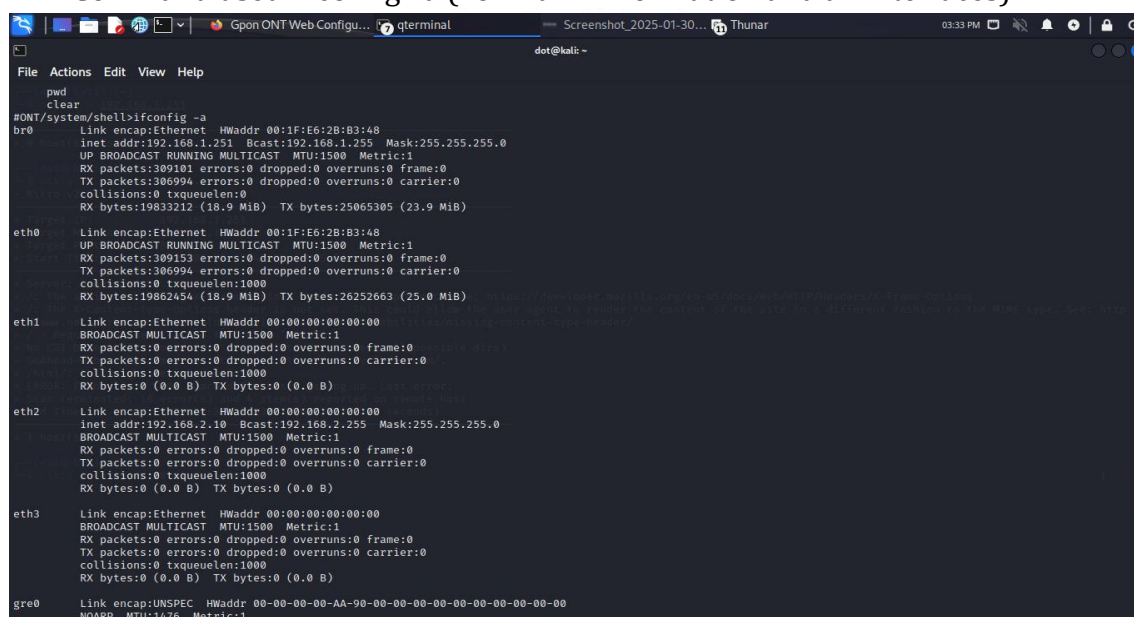
25.<Requirement Description: > The ONU/ONT shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The ONU/ONT shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

26.[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]

27. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info
 - Command used: `ifconfig -a` (To find IP information and all interfaces)



```
File Actions Edit View Help
pwd
clear
#ONT/system/shell>ifconfig -a
br0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48
     inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     RX packets:389101 errors:0 dropped:0 overruns:0 frame:0
     TX packets:386994 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)

eth0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     RX packets:389153 errors:0 dropped:0 overruns:0 frame:0
     TX packets:386994 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)

eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00
     BROADCAST MULTICAST MTU:1500 Metric:1
     RX packets:0 errors:0 dropped:0 overruns:0 frame:0
     TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00
     inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0
     BROADCAST MULTICAST MTU:1500 Metric:1
     RX packets:0 errors:0 dropped:0 overruns:0 frame:0
     TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00
     BROADCAST MULTICAST MTU:1500 Metric:1
     RX packets:0 errors:0 dropped:0 overruns:0 frame:0
     TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:1000
     RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

gre0: Link encap:UNSPEC HWaddr 00-00-00-AA-90-00-00-00-00-00-00-00-00
     NOARP MTU:1476 Metric:1
```


- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer N: R2.0.9.6
#ONT/system>
```

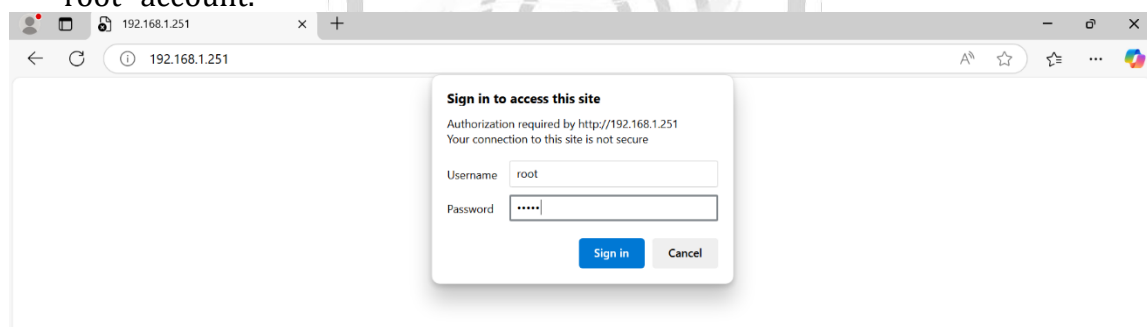
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

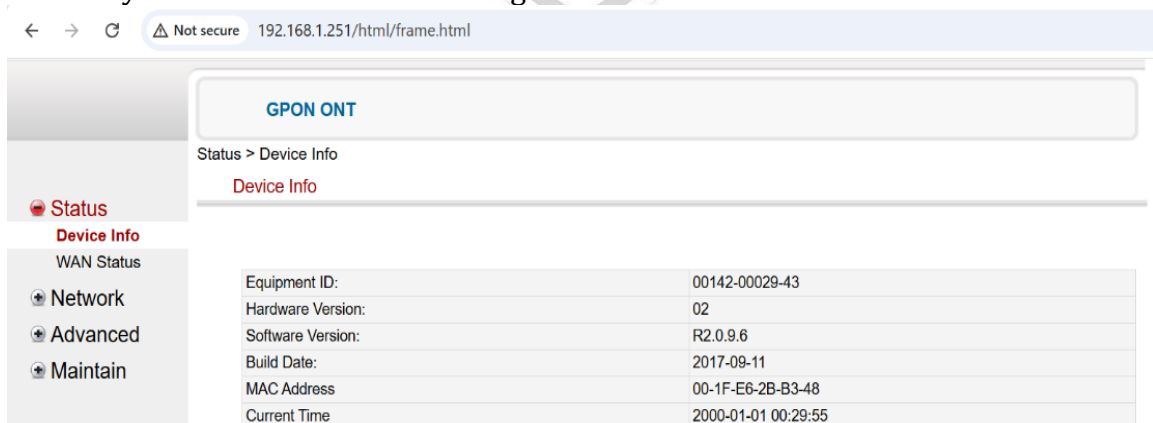
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

28. DUT Configuration

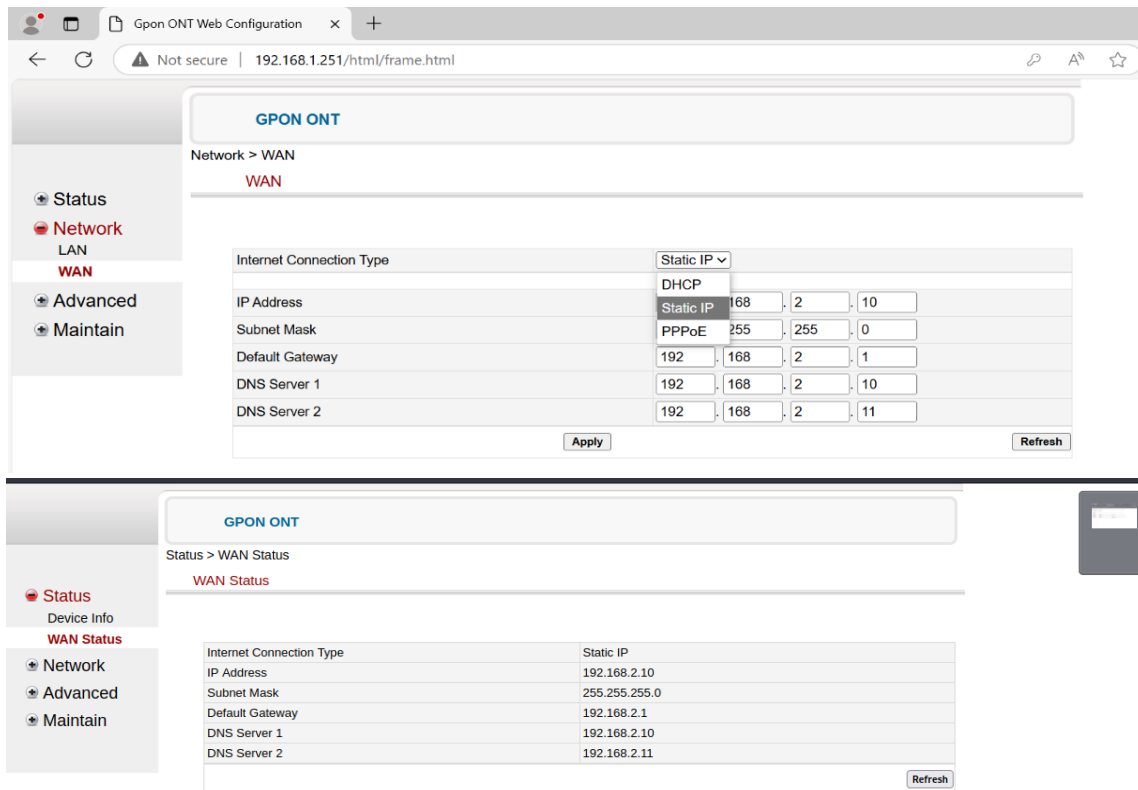
- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address



29. Preconditions

- The Vendor must provide a Certificate stating that the Web Application is tested and free from command injection or cross-site scripting attacks.
- Network Product documentation which contains information on log file location and procedure to access it.
- Tester has the necessary privileges to access the log files.
- Test environment with a Web Browser.
- Knowledge about XSS and Command Injection attacks.

30. Test Objective: The DUT shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks

31.

32. Test Plan

8.1 Number of Test Scenarios:

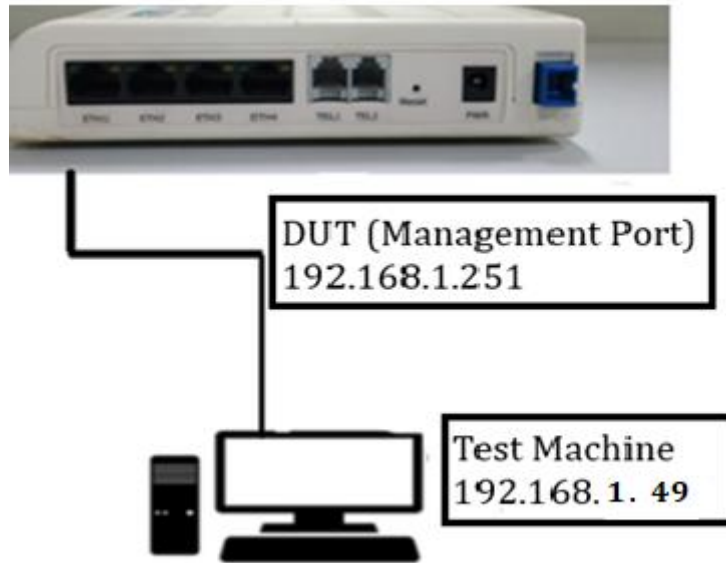
8.1.1 Test Scenarios for XSS attack

- Manual check via Cheat Sheet
- Automated check via tool

8.1.2 Test Scenarios for Command Injection attack

- Manual check via Cheat Sheet
- Automated check via tool

8.2 Test-bed setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

- i. XSSStrike (<https://github.com/s0md3v/XSSStrike>)
- ii. Commix (<https://github.com/commixproject/commix>)

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester manually tries to find the inputs in the Web Application.
- iii. Perform manual test on inputs for XSS and Command Injection vulnerability based on cheat sheets.
- iv. The tester using automated tools like XSSStrike and Commix to find Command Injection vulnerability.

33. Expected Results for Pass: The Web Application must be free from XSS and Command Injection vulnerability.

34. Expected Format of Evidence: Testing report contains copies of the log file showing the captured information.

35. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_XSS_TESTING

11.1.2. Test Case Description: Verify that all the input in the WEB Application is free from XSS attack.

- i. Manual approach
- ii. Automated approach

11.1.3. Execution Steps: The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.

- i. URL: `http://<IP address of DUT>`

DUT - WEB SERVER

- ii. Find all the input in the WEB Application/Page
 - a. Manual Approach
 - i. Use the below cheat sheet for XSS and try it in the input and observe the behaviour.
 - (https://gist.github.com/kurobeats/9a613c9ab68914312cbb415134795b45/raw/c24dd91dd91c324ae5c28b124aa4d379dbcb8e59/xss_vectors.txt)

```
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
<IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onafterprint="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onbeforeprint="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onbeforeunload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onerror="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onhashchange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmessage="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ononline="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onoffline="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpagehide="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpageshow="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onpopstate="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onresize="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onstorage="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onunload="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onblur="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onchange="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oncontextmenu="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oninput="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x oninvalid="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onreset="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onsearch="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onselect="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onsubmit="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeydown="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeypress="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onkeyup="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onclick="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondblclick="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousedown="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousemove="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseout="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseover="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmouseup="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onmousewheel="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onwheel="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondrag="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragend="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragenter="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragleave="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragover="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondragstart="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x ondrop="alert(String.fromCharCode(88,83,83))">
<IMG SRC=x onscroll="alert(String.fromCharCode(88,83,83))">
```

- (A snapshot of few XSS payloads)
- ii. Automated Approach.
 - Command used: **xsstrike -crawl -u <URL of WEB Application>**

```

[ashwini@ashwini-news-lab]~/XSStrike
$ python3 xsstrike.py --crawl -u http://172.18.0.8/

XSStrike v3.1.5

[~] Crawling the target
[!] Progress: 1/1

[ashwini@ashwini-news-lab]~/XSStrike
$ 

```

- (Here we can see the tool has not detected any vulnerable object)

```

[ashwini@ashwini-news-lab]~/XSStrike
$ python3 xsstrike.py --crawl -u http://172.18.0.8/

XSStrike v3.1.5

[~] Crawling the target
[+] Potentially vulnerable objects found at http://172.18.0.8/
-----
6  output.innerHTML = input.value;
-----
[!] Progress: 1/1

```

- (Here we can see the tool has detected a vulnerable object this must be manually checked and if found vulnerable the test case will fail)

11.1.4. **Test Observations:** It should be ensured that any input on the WEB Application should not be vulnerable to XSS attacks.

11.2 Test Case Number: 02

11.2.1. **Test Case Name:** TC_CI_TESTING

11.2.2. **Test Case Description:** Verify that all the input in the WEB Application is free from Command Injection attack.

- i. Manual approach
- ii. Automated approach

11.2.3. **Execution Steps:** The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT. URL: <http://<IP address of DUT>>



DUT - WEB SERVER

- i. Find all the input in the WEB Application/Page
 - a. Manual Approach
 - i. Use the below cheat sheet for Command Injection and try it in the input and observe the behaviour.
 - ii. (<https://hackersonlineclub.com/command-injection-cheatsheet/>)

```

&lt;!--#exec%20cmd=&quot;/bin/cat%20/etc/passwd&quot;--&gt;
&lt;!--#exec%20cmd=&quot;/bin/cat%20/etc/shadow&quot;--&gt;
&lt;!--#exec%20cmd=&quot;/usr/bin/id;--&gt;
&lt;!--#exec%20cmd=&quot;/usr/bin/id;--&gt;
/index.html|id|
;id;
;id
;netstat -a;
;id;
|id
|/usr/bin/id
|id|
|/usr/bin/id|
|/usr/bin/id|
|id;
|/usr/bin/id;
;id|
;|/usr/bin/id|
\n/bin/ls -al\n
\n/usr/bin/id\n
\nid\n
\n/usr/bin/id;
\nid;
\n/usr/bin/id|
\nid|
;usr/bin/id\n
;id\n
|usr/bin/id\n
\nid\n

```

iii. (A snapshot of few Command Injection payloads)

b. Automated Approach.

i. Command used: *<Read the utility documentation to get information about the usage>*

```

[ashwint@ashwint-news-lab]~$ python3 commix.py -u http://localhost:8888/ci.php
v3.8-dev#42
https://commixproject.com
@commixproject

***
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2023 Anastasios Stasinopoulos (@ancst)
***

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage cau
sed by this program.

[16:40:23] [info] Testing connection to the target URL.
[16:40:23] [info] Performing identification checks to the target URL.
[16:40:23] [critical] No parameter(s) found for testing on the provided target URL. You are advised to rerun with '--crawl=2'.

```

ii. (Here we can see the tool has not detected any vulnerable object)

```

[ashwini@ashwini-newsLab]~[-/commix]
$ python3 commix.py --url="http://192.168.17.2/vulnerabilities/exec/#" --data="ip=127.0.0.1&Submit=submit" --cookie="security=low; PHPSESSID=3pnaechpnhqjjb56qgf4udc62"

v3.8-dev#42
https://commixproject.com
(@commixproject)

---
Automated All-in-One OS Command Injection Exploitation Tool
Copyright © 2014-2023 Anastasios Stasinopoulos (@ancst)
---

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage cau
sed by this program.

[16:36:57] [info] Testing connection to the target URL.
Got a redirect to 'http://192.168.17.2/vulnerabilities/exec/'. Do you want to follow? [Y/n] >
[16:37:15] [info] Following redirection to 'http://192.168.17.2/vulnerabilities/exec/'.
[16:37:15] [info] Performing identification checks to the target URL.
[16:37:18] [warning] Target's estimated response time is 3 seconds. That may cause serious delays during the data extraction procedure an
d/or possible corruptions over the extracted data.
[16:37:18] [info] Setting POST parameter 'ip' for tests.
[16:37:27] [info] Heuristic (basic) tests shows that POST parameter 'ip' might be injectable (possible OS: 'Unix-like').
[16:37:38] [info] Testing the (results-based) classic command injection technique.
[16:37:38] [info] POST parameter 'ip' appears to be injectable via (results-based) classic command injection technique.
127.0.0.1;echo CJZATJS((56+49))$(echo CJZATJ)CJZATJ
POST parameter 'ip' is vulnerable. Do you want to prompt for a pseudo-terminal shell? [Y/n] > Y
Pseudo-Terminal Shell (type '?' for available options)
commix(os_shell) > ls
help index.php source

```

iii. (Here we can see the tool has detected a vulnerable object this must be manually checked and if found vulnerable the test case will fail)

11.2.4. **Test Observations:** It should be ensured that any input on the WEB Application should not be vulnerable to Command Injection attacks.

36. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_XSS_TESTING		
2	TC_CI_TESTING		

2.11.4 TSTP for Evaluation No unused HTTPS methods

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.4
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed her

1. **<ITSAR Section No & Name>** Section 11: Web Servers
2. **<Security Requirement No & Name >** 1.11.4 No unused HTTPS methods
3. **<Requirement Description:>** HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3].

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info
 - a. Command used: **ifconfig -a** (To find IP information and all interfaces)


```
dot@kali: ~  
File Actions Edit View Help  
pwd  
clear  
#ONT/system>shell>ifconfig -a  
br0  
Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:309101 errors:0 dropped:0 overruns:0 frame:0  
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)  
  
eth0  
Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:309153 errors:0 dropped:0 overruns:0 frame:0  
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)  
  
eth1  
Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth2  
Link encap:Ethernet HWaddr 00:00:00:00:00:00  
inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth3  
Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
gre0  
Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00  
NOARP MTU:1476 Metric:1
```

b. The below screenshot shows the firmware version of the DUT

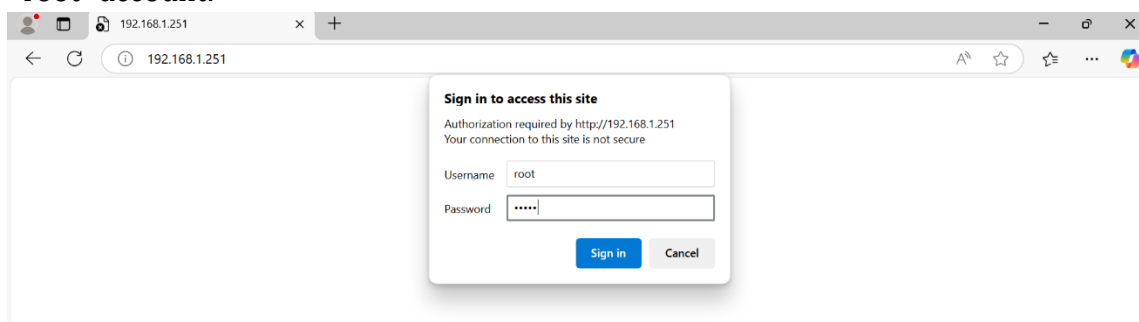
```
#ONT/system>ontver  
OntSwVer N:R2.0.9.6  
#ONT/system>
```

c. The below screenshot shows the information of the DUT

```
#ONT/system>custom  
Customer Information  
  
Customer Name : UUAP  
Customer Full Name : Alphion  
System Config file : /etc/sys.cfg.alp  
#ONT/system>
```

5. DUT Configuration

- iv. The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- v. The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- vi. Verify the DUT information through device info

← → ↻ ⚠ Not secure 192.168.1.251/html/frame.html

GPON ONT

Status > Device Info

Device Info

Equipment ID:	00142-00029-43
Hardware Version:	02
Software Version:	R2.0.9.6
Build Date:	2017-09-11
MAC Address	00-1F-E6-2B-B3-48
Current Time	2000-01-01 00:29:55

Status

Device Info

WAN Status

Network

Advanced

Maintain

vii. Set the static IP address

Gpon ONT Web Configuration × +

← ↻ ⚠ Not secure | 192.168.1.251/html/frame.html

GPON ONT

Network > WAN

WAN

Internet Connection Type: Static IP

IP Address: 192.168.2.10

Subnet Mask: 255.255.0.0

Default Gateway: 192.168.2.1

DNS Server 1: 192.168.2.10

DNS Server 2: 192.168.2.11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6. Preconditions

- The tester must have administrative privilege
- A tester machine is available.
- Test environment with a provision to access the DUT.
- Vendor list of Enabled and necessary methods in the DUT Web-Server.

7. Test Objective: Verify if the DUT supports any HTTP methods other than GET, HEAD, POST as mentioned in the requirement.

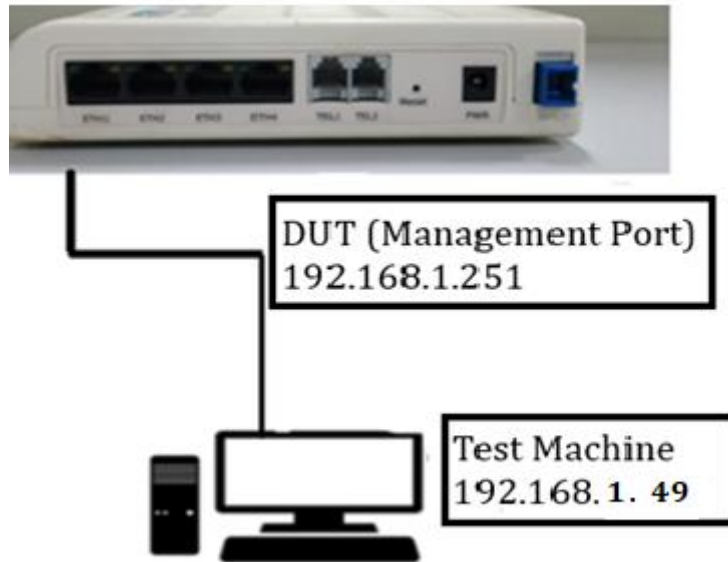
8. Test Plan:

8.1. Number of Test Scenarios:

8.1.1. Test Scenario if OPTIONS is enabled

8.1.2. Test Scenario if OPTIONS is disabled: Custom Script to be used to check for enabled Methods

8.2. Test Bed Diagram



8.3. **Tools Required:** Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4. Test Execution Steps

- Power up the testbed
- The tester tries to check the available HTTP Methods in webserver.
- The tester verifies whether the only required HTTP Methods are enabled or not.
- If the OPTIONS method is not enabled in WEB-SERVER, the manual checking via script is to be used.

9. **Expected Results for Pass:** System settings and configurations have been found adequately set, in all Web components of the system, to ensure that unneeded HTTP methods are deactivated.

10. **Expected Format of Evidence:** Testing report contains screenshots showing the captured information.

11. Test Execution:

11.1. Test Case Number: 01

11.1.1. **Test Case Name:** TC_NO_UNUSED_HTTP_METHODS_OPTIONS_DISABLED

11.1.2. **Test Case Description:** Verify that the Web server has deactivated all HTTP methods that are not required if OPTIONS method is not enabled.

11.1.3. Execution Steps:

1. The tester shall open any terminal or any tool to access DUT shell

- Command used: ***python3 WebServer-Methods.py <IP address of DUT>***

```
(dot@kali)-[~]
$ cd Documents

(dot@kali)-[~/Documents]
$ python3 pythonscript.py http://192.168.129.251
http://192.168.129.251
[GET]: Enabled (401)
[POST]: Error
[PUT]: Enabled (400)
[DELETE]: Enabled (400)
[PATCH]: Enabled (400)
[HEAD]: Enabled (401)
[OPTIONS]: Enabled (400)
[TRACK]: Enabled (400)
[TRACE]: Enabled (400)
[CONNECT]: Enabled (400)

(dot@kali)-[~/Documents]
$
```

- The tester will compare the vendor list of enabled and necessary methods.
- If any method other than the vendor list is present the test case will fail.

(This should not be present

Pythonscript.py script (Script used for testing)

#!/usr/bin/env python3

import requests

import urllib

import validators

*methods = ["GET", "POST", "PUT", "DELETE",
"PATCH", "HEAD", "OPTIONS", "TRACK", "TRACE", "CONNECT"]*

def main(URL):

for method in methods:

try:

res = requests.request(method, URL, verify=False)

if (res.status_code == 405):

*print(f"\033[1;94m[{method}]\033[00m:\033[1;91mDisabled
\033[00m(\033[1;93m{res.status_code}\033[00m)\033[00m")*

else:

*print(f"\033[1;94m[{method}]\033[00m:\033[1;92mEnabled
\033[00m(\033[1;93m{res.status_code}\033[00m)\033[00m")*

except:

print(f"\033[1;94m[{method}]\033[00m: \033[1;91mError\033[00m")

pass

if __name__ == '__main__':

if len(sys.argv) < 2:

exit(f"Usage: {sys.argv[0]} <URL>")

```
URL = sys.argv[1]
```

```
if not validators.url(URL):  
    exit(f"Error: Invalid URL")  
print(URL)  
main(URL)
```

11.1.4. **Test Observations:** It should be ensured that HTTP methods that are not required for DUT operation shall be deactivated.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_UNUSED_HTTP_METHODS_OPTIONS_DISABLED		



2.11.5 TSTP Report for Evaluation No unused add-ons

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no2.11.5
--	--------------------------	-----------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 11: Web Server

2. <Security Requirement No & Name > 1.11.5 No unused add-ons

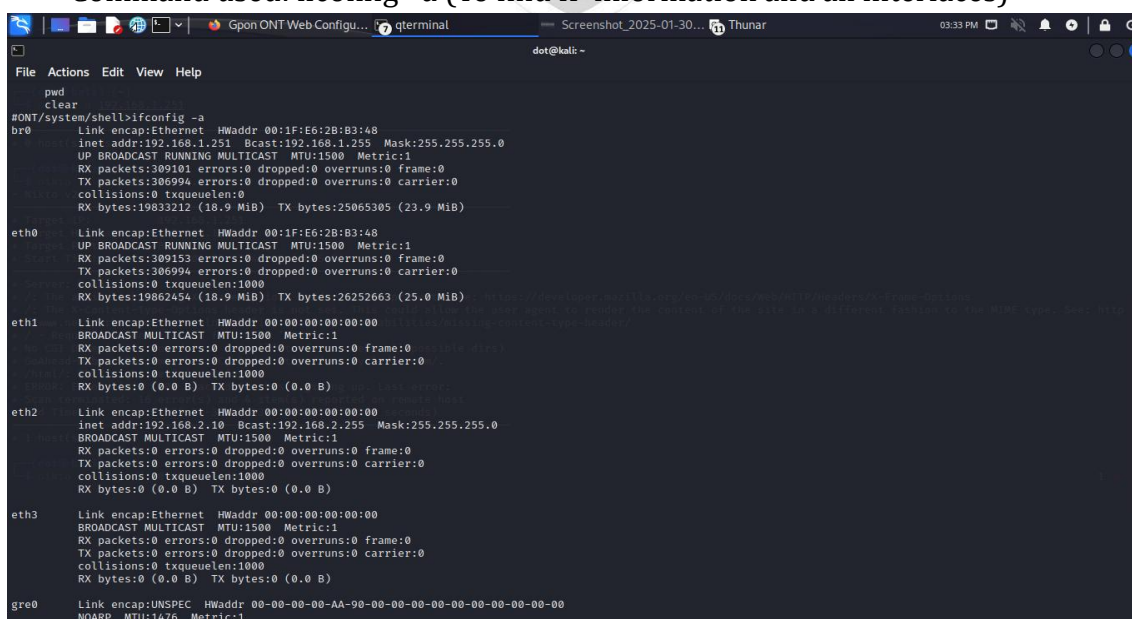
3. <Requirement Description: > All optional add-ons and components of the web server shall be deactivated if they are not required. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.3.4.4]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info
 - Command used: `ifconfig -a` (To find IP information and all interfaces)



```
dot@kali: ~  
File Actions Edit View Help  
pwd  
clear  
#ONT/system/shell>ifconfig -a  
br0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:309101 errors:0 dropped:0 overruns:0 frame:0  
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)  
  
eth0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:309153 errors:0 dropped:0 overruns:0 frame:0  
TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)  
  
eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
gre0: Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00  
NOARP MTU:1476 Metric:1
```

- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer N: R2.0.9.6
#ONT/system>
```

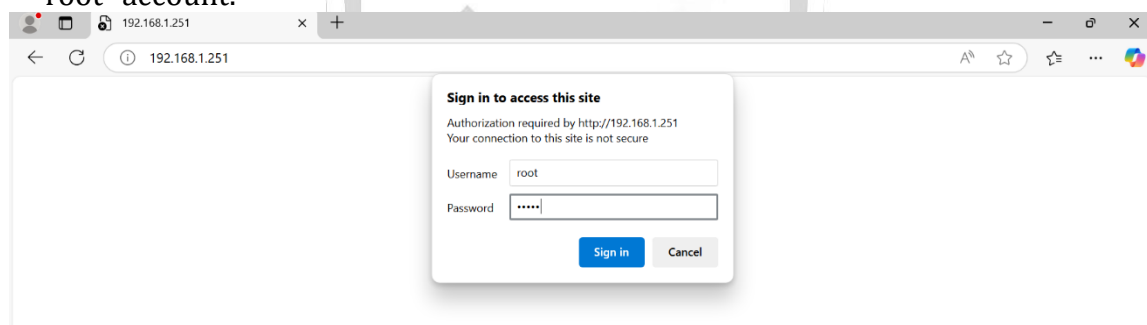
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

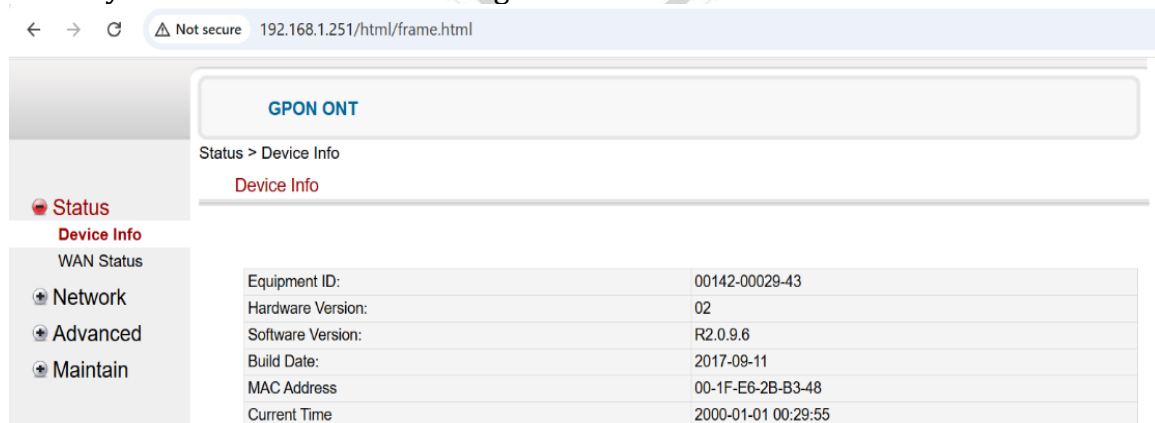
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

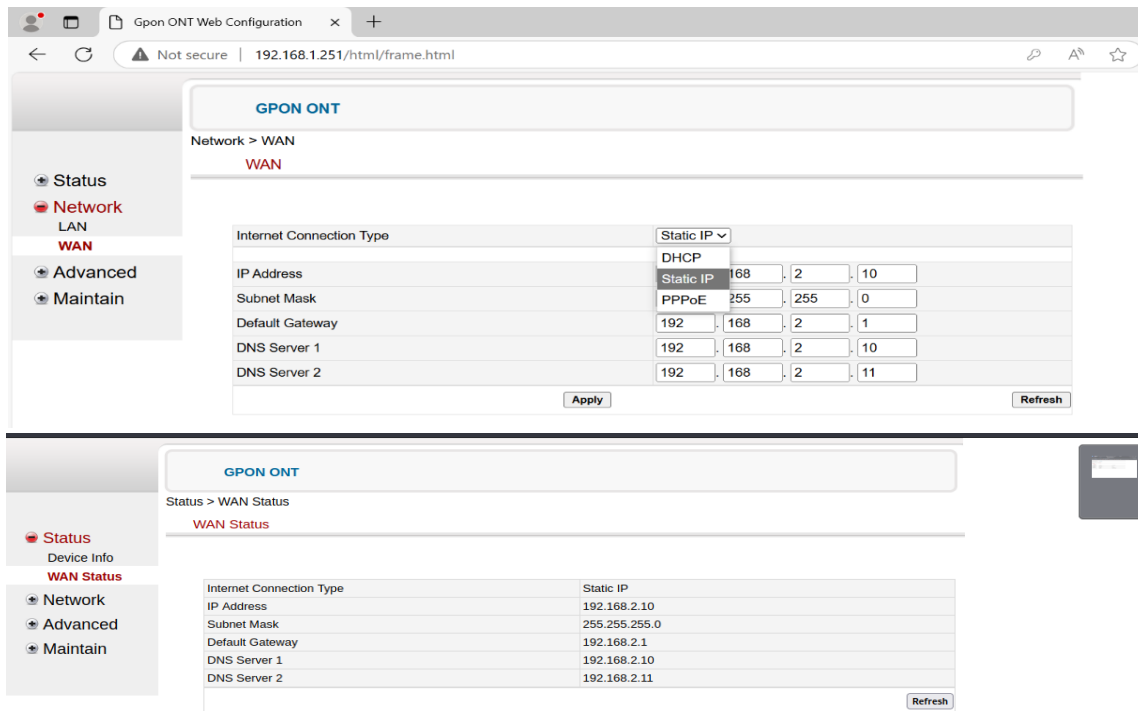
- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address



6. Preconditions

- The OEM has supplied a list of add-ons or scripting tools for Web server components needed for system operation, and that therefore need to be exempted from the test investigation.
- The tester has administrative privileges.
- A tester machine is available.
- Path of the configuration file of the web server.

7. **Test Objective:** To verify that the Web server has deactivated unneeded add-ons and unneeded scripting components.

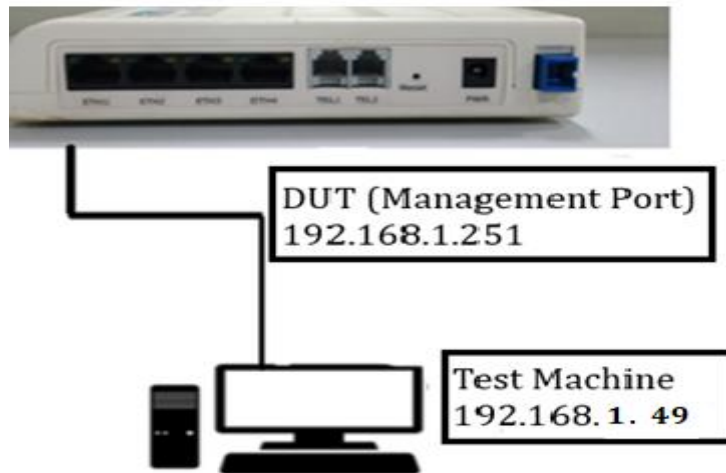
8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for Unused Add-ons: This test scenario will check for the add-ons using DUT command.

8.2 Test Setup Diagram:

8.3 Test-bed setup Diagram:



8.4 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.5 Test Execution Steps

- i. Power up the testbed
- ii. Check that the web server is only running and listening on known ports (e.g., tcp port 80 and/or 443). Check that
- iii. CGI or other scripting components, Server Side Includes (SSI), and WebDAV are deactivated if they are not required.
- iv. The tester verifies that nothing else has been installed than the web server.
- v. The tester verifies that relevant system settings and configurations are correct to ensure fulfilment of the requirement.
- vi. The tester scans the Webserver using a suitable tool (e.g., Nikto) and verifies the tool report for availability of any default content.

9. **Expected Results for Pass:** System settings and configurations have been found adequately set, in all Web components of the system, to ensure that all unneeded add-ons or script components are deactivated.

10. **Expected Format of Evidence:** Testing report contains copies of the log file showing the captured information.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. **Test Case Name:** TC_NO_UNUSED_ADD-ONS

11.1.2. **Test Case Description:** To verify that the Web server has deactivated unneeded add-ons and unneeded scripting components.

11.1.3. Execution Steps:

- i. The tester shall open any terminal or any tool to access DUT shell. Command used: `apache2ctl -M`

```
amf@localhost $ apache2ctl -M
Loaded Modules:
core_module (static)
so_module (static)
watchdog_module (static)
http_module (static)
log_config_module (static)
logio_module (static)
version_module (static)
unixd_module (static)
access_compat_module (shared)
alias_module (shared)
auth_basic_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_host_module (shared)
authz_user_module (shared)
autoindex_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
filter_module (shared)
mime_module (shared)
mpm_event_module (shared)
negotiation_module (shared)
reqtimeout_module (shared)
setenvif_module (shared)
status_module (shared)
allowmethods module (shared)
```

- ii. The tester manually checks for the vendor-supplied list of add-ons or scripting tools for Web server components needed for system operation other than those that must not be present.
- iii. The tester opens any terminal or any tool to access DUT shell
 - Command used: ***apache2ctl -M***

```
amf@localhost $ apache2ctl -M
Loaded Modules:
core_module (static)
so_module (static)
watchdog_module (static)
http_module (static)
log_config_module (static)
logio_module (static)
version_module (static)
unixd_module (static)
access_compat_module (shared)
alias_module (shared)
auth_basic_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_host_module (shared)
authz_user_module (shared)
autoindex_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
filter_module (shared)
mime_module (shared)
mpm_event_module (shared)
negotiation_module (shared)
reqtimeout_module (shared)
setenvif_module (shared)
status_module (shared)
allowmethods module (shared)
mod_actions (shared)
mod_authnz_fcgi (shared)
mod_cgi (shared)
mod_cgid (shared)
mod_suexec (shared)
mod_dav (shared)
mod_dav_fs (shared)
mod_dav_lock (shared)
mod_include (shared)
```

- iv. Here we can see allowed enabled modules that should not be there because they are WEBDAV, CGI, SSI (mod_actions, mod_authnz_fcgi, mod_cgi, mod_cgid, mod_suexec, mod_dav, mod_dav_fs, mod_dav_lock, mod_include)
 - v. (Clickable link so for more info)
 - vi. All this must not be present here only allowed and necessary add-ons must be allowed.
- 11.1.4. **Test Observations:** System settings and configurations have been found adequately set, in all Web components of the system, to ensure that all unneeded add-ons or script components are deactivated.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_UNUSED_ADD-ONS		



2.11.6 TSTP for Evaluation of No compiler, interpreter, or shell via CGI or other server-side scripting

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.6
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

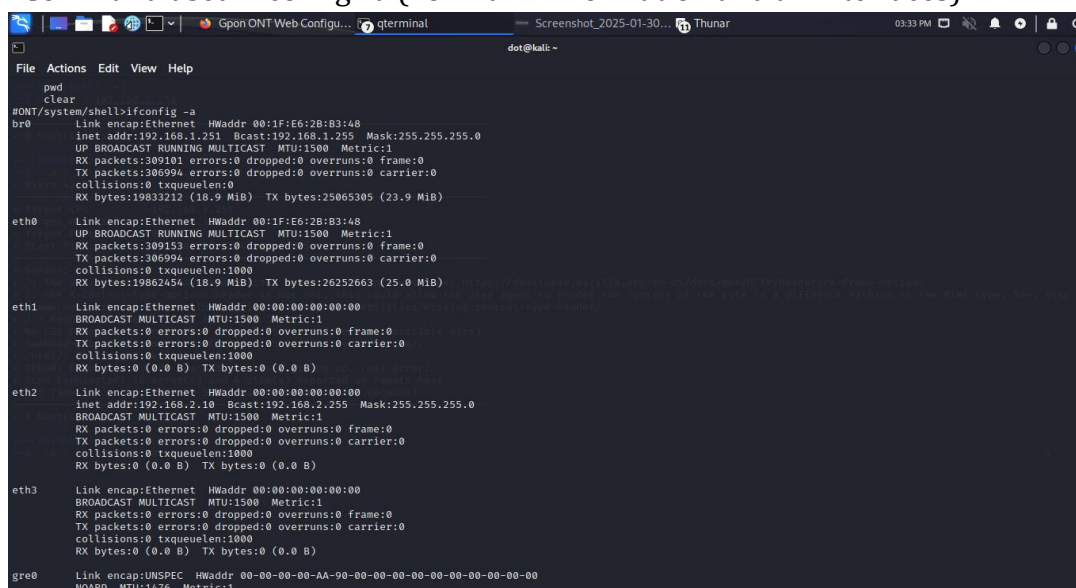
1. <ITSAR Section No & Name> Section 11: Web Server
2. <Security Requirement No & Name > 1.11.6 No compiler, interpreter, or shell via CGI or other server-side scripting
3. <Requirement Description: > If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory -or other corresponding scripting directory - shall not include compilers or interpreters (e.g. PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.5]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
 - ii. Use command to get Application No/Version No & Kernel Info
- Command used: ifconfig -a (To find IP information and all interfaces)



```
File Actions Edit View Help
pwd
clear
#ONT/system/shell>ifconfig -a
br0: Link encap:Ethernet HWaddr 00:1F:E6:28:B3:48
      inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)

eth0: Link encap:Ethernet HWaddr 00:1F:E6:28:B3:48
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)

eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00
      inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

gre0: Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00
      NOARP MTU:1476 Metric:1
```

- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer   : R2.0.9.6
#ONT/system>
```

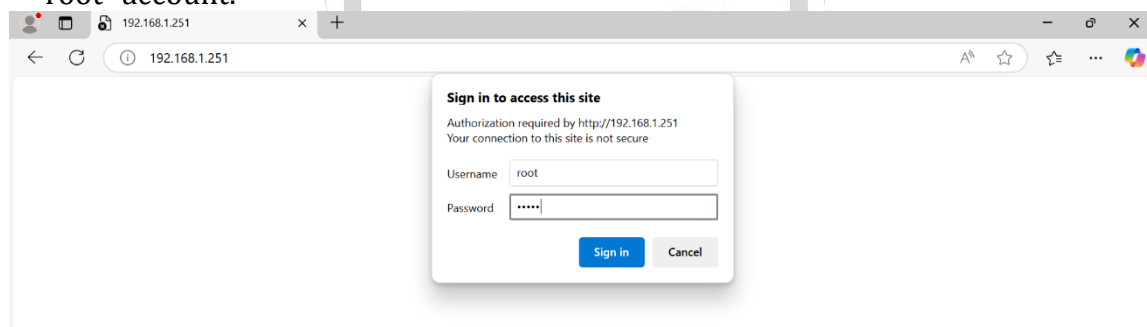
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

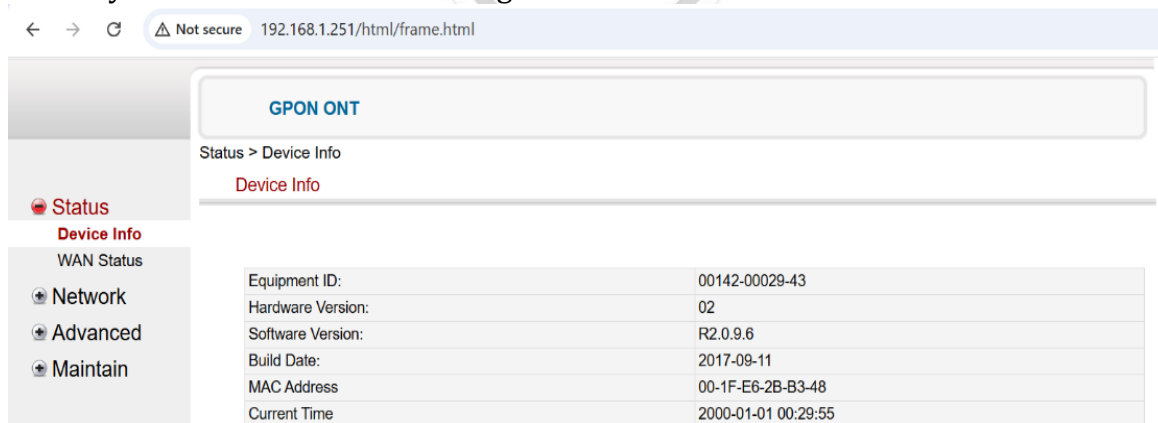
Customer Name       : UUAP
Customer Full Name  : Alphion
System Config file  : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address

GPON ONT Web Configuration - Network > WAN

Internet Connection Type: **Static IP**

IP Address	192	168	2	10
Subnet Mask	255	255	0	
Default Gateway	192	168	2	1
DNS Server 1	192	168	2	10
DNS Server 2	192	168	2	11

GPON ONT Web Configuration - Status > WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

6. Preconditions

- The tester has administrative privileges
- A tester machine is available.
- Test environment with a Terminal.
- OEM should provide path of scripting directories.

7. Test Objective: To verify that there are no compilers, interpreters, or shell accessible via CGI or other scripting components.

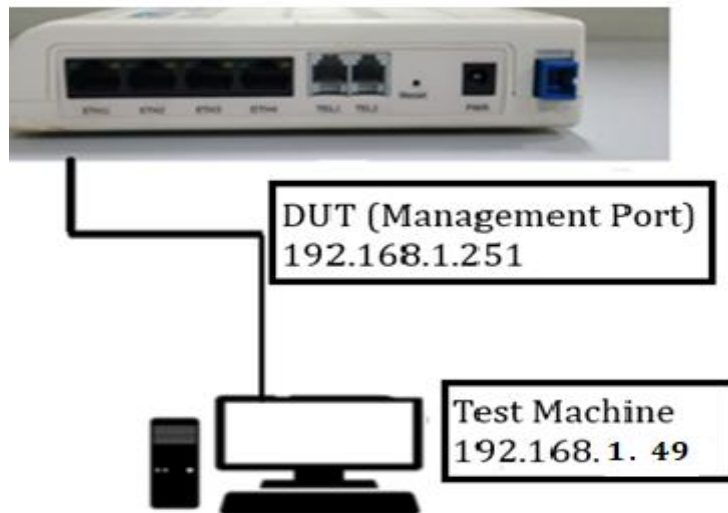
8. Test Plan:

8.1 Test Scenario for CGI

8.1.1 This test scenario is regarding CGI and check for compiler/interpreter or shell in CGI

8.1.2 Manual

8.2 Test bed Diagram



8.3 Test tool required per scenario/test case: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Shell of Web Server.
- iii. Consult the web server configuration to identify all directories used for CGI or other scripting components.
- iv. In case the DUT is using other than CGI they must give the information about different technology used and further tests should be performed on that technology. (This document only deals with CGI Scripts)
- v. The tester manually checks that there are no compilers or interpreters (e.g., PERL® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells) in the directory/directories used for CGI or for other scripting tools (including PERL®, PHP, and others).
- vi. The tester will run some web scanning tools like Nikto, to get the detailed information and verify that there are no compilers or interpreters (e.g., PERL® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells) in the directory/directories used for CGI or for other scripting tools (including PERL®, PHP, and others).

9. Expected Results for Pass: There are no compilers, interpreters or shells in directories accessible via CGI or other scripting components.

10. Expected Format of Evidence: Log files and screen shots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_NO_COMPILER_FOR_CGI

11.1.2. Test Case Description: There are no compilers, interpreters, or shells in directories accessible via CGI or other scripting components.

11.1.3. Execution Steps:

- i. The tester shall open any terminal emulator to access the DUT shell and use the following command.
 - Command used: ***ls <path of the CGI-BIN directory>***

```
amf@localhost $ ls /var/www/html/cgi-enabled/  
test.cgi test.py
```

- We can see that the directory does not contain any compiler/interpreter, shell.
NOTE: OEM should provide path of scripting directories.

- ii. The tester shall open any terminal emulator and use the following command.
 - Command used: ***ls <path of the CGI-BIN directory>***

```
amf@localhost $ ls  
bash python3 test.cgi test.py
```

- We can see that the directory does contain bash shell, python3 interpreter.
 - (This should not be present)

11.1.4. **Test Observations:** There are no compilers, interpreters or shells in directories accessible via CGI or other scripting components.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_COMPILER_FOR_CGI		

Securing Networks

2.11.7 TSTP for Evaluation of No CGI or other scripting for uploads

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.7
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 11: Web Server

2. <Security Requirement No & Name > 1.11.7 No CGI or other scripting for uploads

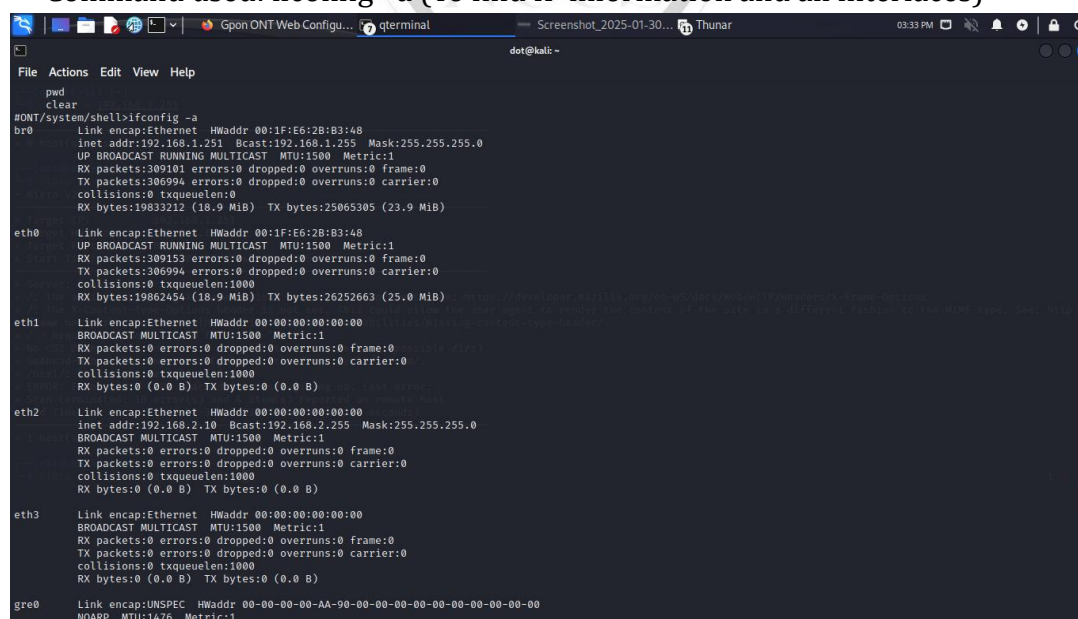
3. <Requirement Description: > If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.6]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- Use command to get Interfaces details
 - Use command to get Application No/Version No & Kernel Info
- Command used: ifconfig -a (To find IP information and all interfaces)



```
File Actions Edit View Help
pwd
clear
#ONT/system/shell>ifconfig -a
br0:    Link encap:Ethernet  HWaddr 00:1F:E6:2B:83:48
        inet addr:192.168.1.251  Bcast:192.168.1.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
        TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0:    Link encap:Ethernet  HWaddr 00:1F:E6:2B:83:48
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
        TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1:    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2:    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
        inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3:    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0:    Link encap:UNSPEC  HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
        NOARP  MTU:1476  Metric:1
```

- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>
```

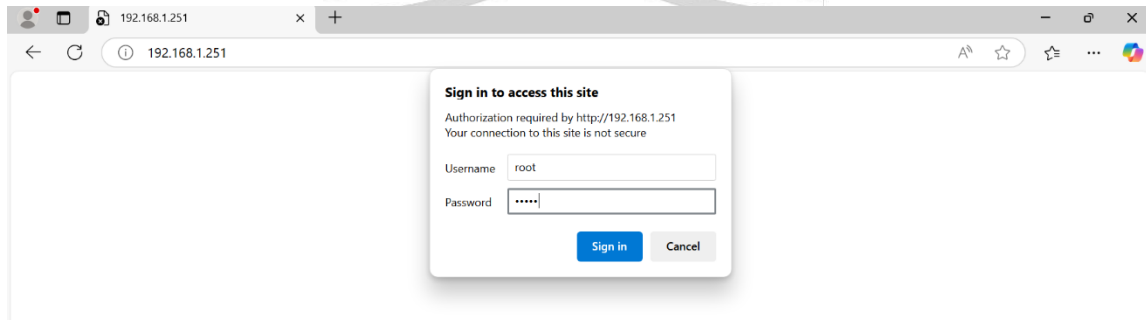
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

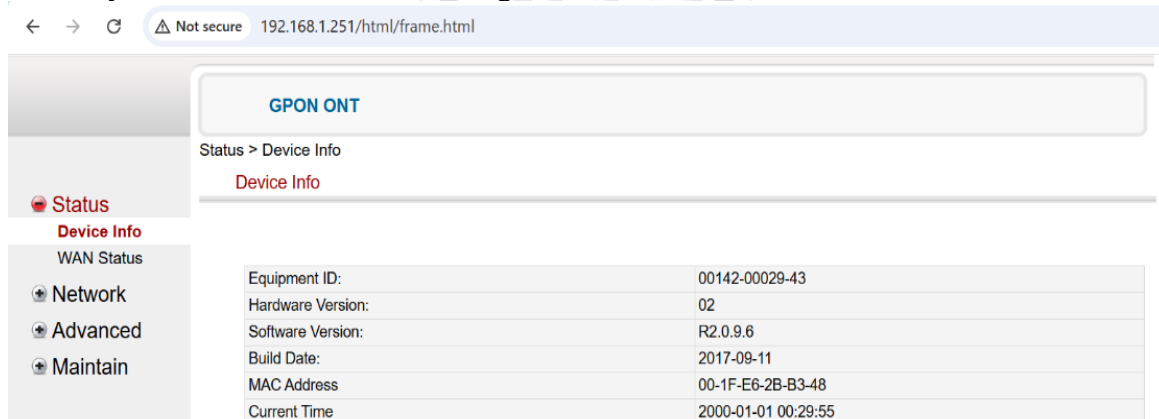
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using "root" account.



- Verify the DUT information through device info



- Set the static IP address

GPON ONT

Network > WAN

WAN

Internet Connection Type	Static IP			
DHCP				
Static IP	192	168	2	10
PPPoE	255	255	0	
Default Gateway	192	168	2	1
DNS Server 1	192	168	2	10
DNS Server 2	192	168	2	11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6. Preconditions

- The tester has administrative privileges
- A tester machine is available.
- Test environment with a Terminal.
- Test Environment with a Browser
- If the web server is configured with CGI/Scripting on, this test applies.
- The tester checks the vendor documentation for the “upload and CGI/scripting directory”.

7. Test Objective: To test whether the upload directory is equal to the CGI/Scripting directory.

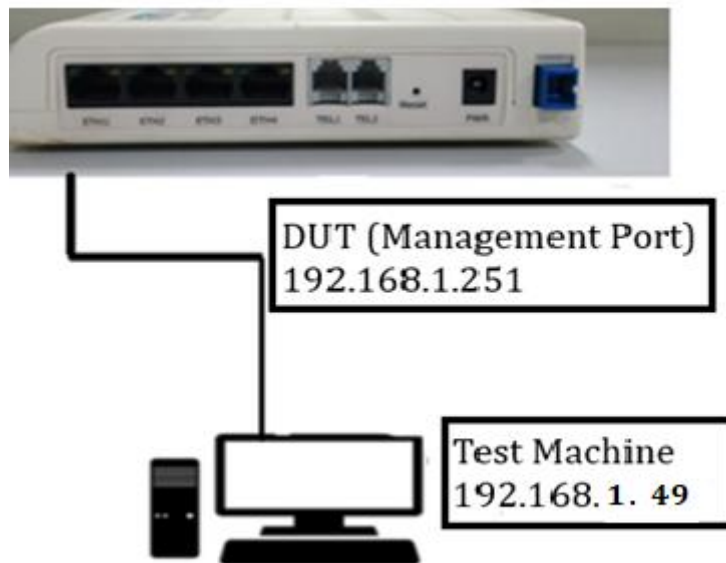
8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for CGI

8.1.2 This test scenario is regarding CGI

8.2 Test-bed setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

Burp suite professional

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Shell of Web Server.
- iii. Consult the web server configuration to identify all directories used for CGI or other scripting components.
- iv. In case the DUT is using other than CGI they must give the information about different technology used and further tests should be performed on that technology. (This document only deals with CGI Scripts)
- v. Consult the vendor documentation to identify all directories used for upload.
- vi. The tester manually checks that the CGI and upload directory are not different and verify it in the DUT.
- vii. The tester will run some web scanning tools like Nikto, to get the detailed information and verify that the CGI and upload directory are different.

9. Expected Results for Pass:

- i. The configured upload directory is different from the CGI/Scripting directory.
- ii. Additional evidence might be provided that shows that the web server has no write rights for the CGI/Scripting directory.

10. Expected Format of Evidence: A part of the configuration file / screenshot of the configuration showing that the web server is properly configured.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_NO_CGI_OR_SCRIPTING_FOR_UPLOADS

11.1.2. Test Case Description: To test whether the upload directory is equal to the CGI/Scripting directory.

11.1.3. Execution Steps:

- i. The tester compares the <path of the CGI-BIN directory> and <path of the upload directory> and confirms that they are not same, if same the test case will fail.
- ii. The tester shall open any terminal emulator to access the DUT shell and use the following command.

- Command used: `ls -la <path of the CGI-BIN directory>`

```
amf@localhost $ ls -la
total 20
drwxr-xr-x 1 www-data www-data 4096 Jun 19 12:07 .
drwxr-xr-x 1 www-data www-data 4096 Apr 26 21:58 ..
dr--r--r-- 2 www-data www-data 4096 Jun 26 10:15 cgi-enabled
-rw-rw-r-- 1 www-data www-data  51 May 26 11:37 index.html
```

- (Here we can see that the <path of the CGI-BIN directory> does not have write access)

- iii. The tester shall open any terminal emulator and use the following command.

- Command used: `ls -la <path of the CGI-BIN directory>`

```
amf@localhost $ ls -la
total 20
drwxr-xr-x 1 www-data www-data 4096 Jun 19 12:07 .
drwxr-xr-x 1 www-data www-data 4096 Apr 26 21:58 ..
drw-r--r-- 2 www-data www-data 4096 Jun 26 10:15 cgi-enabled
-rw-rw-r-- 1 www-data www-data  51 May 26 11:37 index.html
```

- (Here we can see that the <path of the CGI-BIN directory> have write access)

- (This must be not done)

11.1.4. **Test Observations:** The CGI and upload directory are different.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_CGI_OR_SCRIPTING_FOR_UPLOADS		

Securing Networks

2.11.8 TSTP for Evaluation of No execution of system commands with SSI

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.8
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1) <ITSAR Section No & Name> Section 11: Web Server

2) <Security Requirement No & Name > 1.11.8 No execution of system commands with SSI

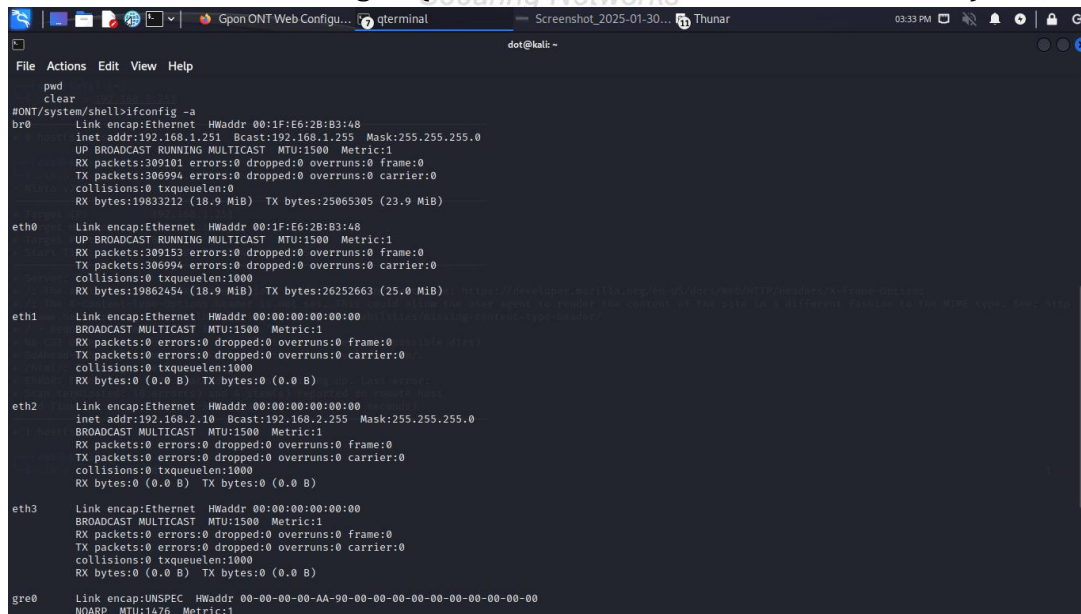
3) <Requirement Description: > If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.7]

4) DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info
 - Command used: ifconfig -a (To find IP information and all interfaces)



```
dot@kali: ~  
File Actions Edit View Help  
pwd  
clear  
#ONT/system/shell>ifconfig -a  
br0: Link encap:Ethernet HWaddr 00:1F:E6:2B:83:48  
      inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0  
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
      RX packets:309101 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:0  
      RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)  
  
eth0: Link encap:Ethernet HWaddr 00:1F:E6:2B:83:48  
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
      RX packets:309153 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)  
  
eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
      BROADCAST MULTICAST MTU:1500 Metric:1  
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
      inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0  
      BROADCAST MULTICAST MTU:1500 Metric:1  
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
      BROADCAST MULTICAST MTU:1500 Metric:1  
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
gre0: Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00  
      NOARP MTU:1476 Metric:1
```


- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer   : R2.0.9.6
#ONT/system>
```

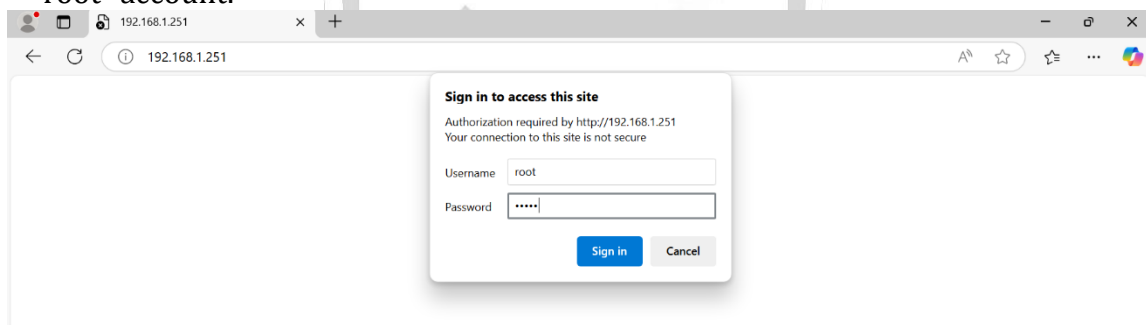
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

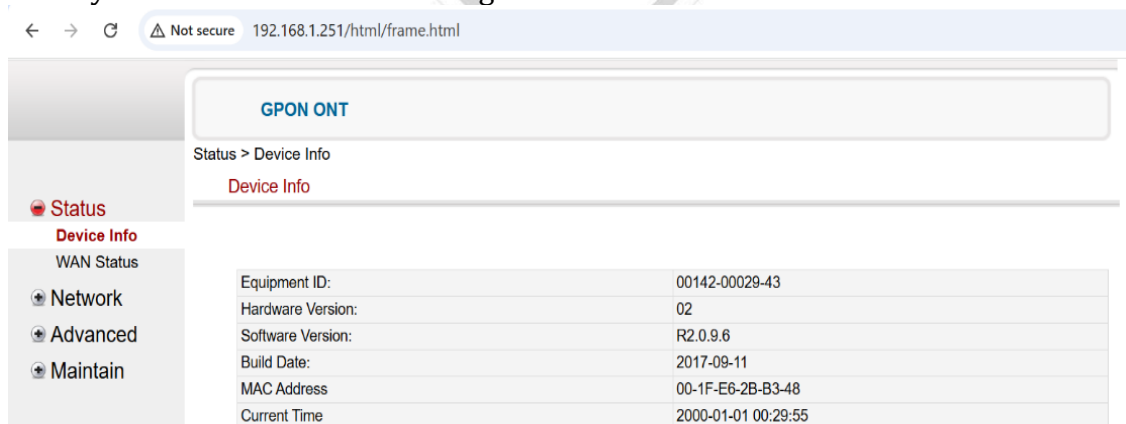
Customer Name       : UUAP
Customer Full Name  : Alphion
System Config file  : /etc/sys.cfg.alp
#ONT/system>
```

5) Dut Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address

GPON ONT Web Configuration

Network > WAN

WAN

Internet Connection Type	Static IP			
DHCP				
Static IP	192	168	2	10
PPPoE	255	255	0	
Default Gateway	192	168	2	1
DNS Server 1	192	168	2	10
DNS Server 2	192	168	2	11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6) Preconditions

- The tester has administrative privileges.
- If the web server is configured with SSL active, this test applies.
- A tester machine is available.
- Test environment with a Terminal.

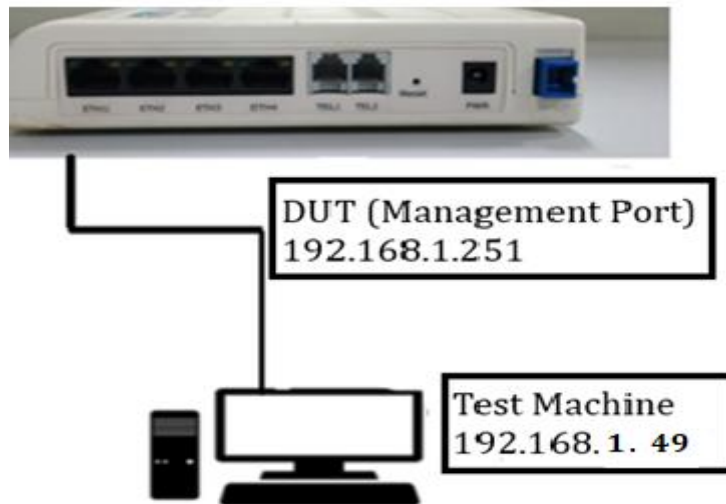
7) **Test Objective:** To test whether it is possible to use the exec directive and if so, whether it can be used for system commands

8) Test Plan:

8.1 Number of Test Scenarios *Securing Networks*

8.1.1 **Test Scenario for SSI:** This test scenario is regarding SSI.

8.2 Test bed setup Diagram



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Shell of Web Server.
- iii. The tester checks whether execution of system commands is disabled in the web server configuration.
- iv. The tester actually attempts to use the exec directive in an SSI file with and without system commands.
- v. Some web scanning tools like Nikto should be used to scan the webserver for the SSI exec.

9) Expected Results for Pass:

- i. The execution of system commands via SSIs exec directive is disabled in the web server configuration.
- ii. It is impossible to execute system commands via SSIs exec directives.

10) Expected Format of Evidence: A part of the configuration file / screenshot of the configuration showing that the web server is properly configured

11) Test Execution:

11.1 Test Case No: 1

11.1.1. Test Case Name: TC_NO_EXECUTION_OF_SYSTEM_COMMANDS

11.1.2. Test Case Description: If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

11.1.3. Execution steps:

- i. The tester shall open any browser to access the DUT webserver using the following URL.
 - a. URL: *http://<ip/hostname of DUT>/<path of the SSI directory>*



[an error occurred while processing this directive]

b. (Here we can see that we got the error when using the exec directive)

c. We can see that the output is an error while using EXEC directive because we have used *Options IncludeNOEXEC*.

d. With proper authentication the tester shall open any terminal emulator and use the following command to see the error log in the DUT.

e. **Command used:** *cat <path to the apache error log file> (cat error.log)*

```
[Fri Jun 30 08:43:25.214042 2023] [cgid:error] [pid 387:tid 140349780350656] [client 172.18.0.1:36286] AH01271: exec used but not allowed in /var/www/html/ssi-enabled/index.html
```

f. We can see that the error stating *exec used but not allowed in <path of the file>*

ii. The tester shall open any browser to access the DUT webserver using the following URL.

a. **URL:** *http://<ip/hostname of DUT>/<path of the SSI directory>*



This executed using is a shell command

b. We can see that a shell command is being run using EXEC directive and it run successfully.

c. (This should not be executed)

11.1.4. d. Test Observations: When Server Side Includes (SSI) is active, the execution of system commands is deactivated using IncludesNOEXEC Options.

12) Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_EXECUTION_OF_SYSTEM_COMMANDS		

2.11.9 TSTP for Evaluation of Access rights for web server configuration

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.9
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 11: Web Server

2. <Security Requirement No & Name > 1.11.9 Access rights for web server configuration

3. <Requirement Description: > Access rights for ONU/ONT webserver configuration files shall only be granted to the owner of the webserver processor to a user with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
- ii. Use command to get Application No/Version No & Kernel Info
 - Command used: ifconfig -a (To find IP information and all interfaces)

```

File Actions Edit View Help
dot@kali: ~
pwd
clear
#ONT/system/shell>ifconfig -a
br0
  Link encap:Ethernet  HWaddr 00:1F:E6:2B:83:48
  inet addr:192.168.1.251  Bcast:192.168.1.255  Mask:255.255.255.0
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
  TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0
  Link encap:Ethernet  HWaddr 00:1F:E6:2B:83:48
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
  TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1
  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
  BROADCAST MULTICAST  MTU:1500  Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2
  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
  BROADCAST MULTICAST  MTU:1500  Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3
  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
  BROADCAST MULTICAST  MTU:1500  Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0
  Link encap:UNSPEC  HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
  NOARP  MTU:1476  Metric:1

```

- The below screenshot shows the firmware version of the DUT

```

#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>

```

- The below screenshot shows the information of the DUT

```

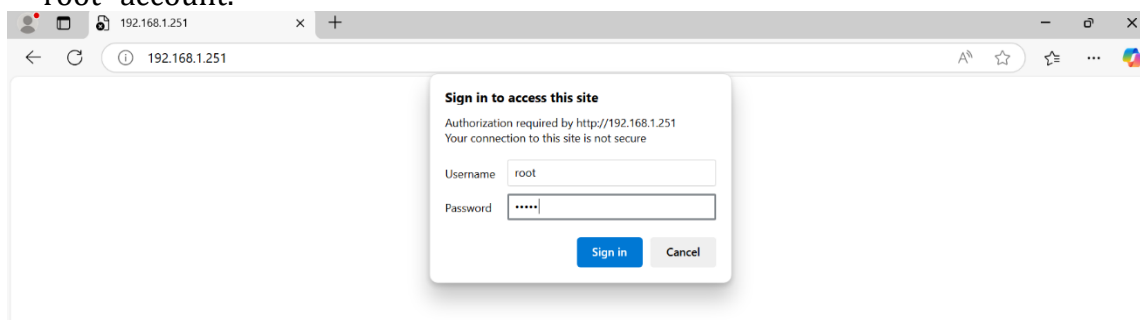
#ONT/system>custom
Customer Information

Customer Name      : UUAP
Customer Full Name : Alphion
System Config file  : /etc/sys.cfg.alp
#ONT/system>

```

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info

← → ↻ ⚠ Not secure 192.168.1.251/html/frame.html

GPON ONT

Status > Device Info

Device Info

Status

Device Info

WAN Status

Network

Advanced

Maintain

Equipment ID:	00142-00029-43
Hardware Version:	02
Software Version:	R2.0.9.6
Build Date:	2017-09-11
MAC Address	00-1F-E6-2B-B3-48
Current Time	2000-01-01 00:29:55

iv. Set the static IP address

Gpon ONT Web Configuration x +

← ↻ ⚠ Not secure | 192.168.1.251/html/frame.html

GPON ONT

Network > WAN

WAN

Status

Network

LAN

WAN

Advanced

Maintain

Internet Connection Type	Static IP ▾			
	DHCP			
IP Address	Static IP	168	2	10
Subnet Mask	PPPoE	255	255	0
Default Gateway	192	168	2	1
DNS Server 1	192	168	2	10
DNS Server 2	192	168	2	11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Status

Device Info

WAN Status

Network

Advanced

Maintain

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6. Pre-Condition: -

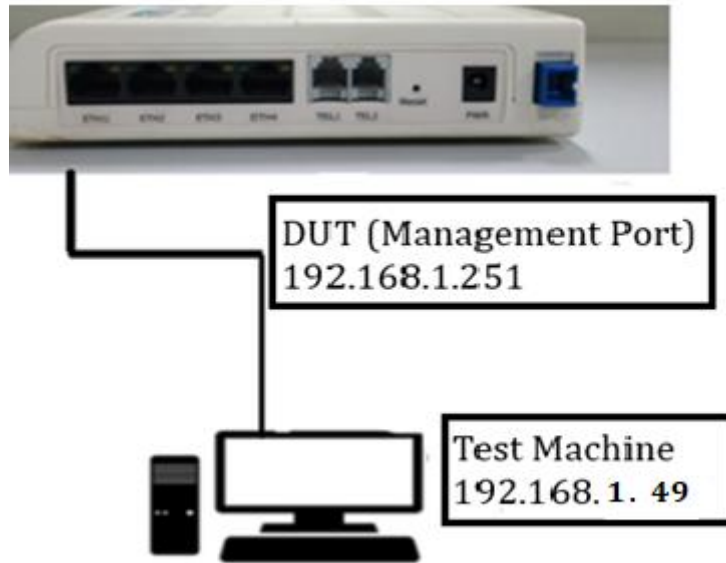
- The tester has administrative privileges
- A tester machine is available.
- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.
- OEM should provide path of the configuration file and access parameter.

7. Test Objective

8. Test Plan

8.1 Test Cases: The Tester shall determine the location of the configuration files used by the web server on DUT as mentioned in OEM documentation.

8.2 Test-bed setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Web Server in the browser.
- iii. Check the access rights settings for Web server system configuration files.
- iv. Check that relevant system settings and configurations are correct to ensure fulfilment of the requirement.
- v. The tester also scans the Web Server using a suitable tool (e.g., Nikto) to verify that the relevant system settings and configurations are correct to ensure fulfilment of the requirement.

9. Expected Results for Pass: Access rights for system configuration files are adequately set.

Securing Networks

10. Expected Format of Evidence: Log files and screen shots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_ACCESS_RIGHTS_WEB_SERVER_FILES

11.1.2. Test Case Description: To verify that the access rights for Web server configuration files are correctly set.

11.1.3. Execution Steps:

NOTE: This test is performed on AMF but testing steps are same or OEM dependent for path of

- i. With the proper privilege in the DUT, we can see the permission on the configuration file.
 - a. Command used: *ls -la <path to the configuration file>*

```
amf@localhost $ ls -la apache2.conf
-rw-r----- 1 www-data www-data 7567 Jun 28 05:03 apache2.conf
```

- b. Here we can see that
 - Owner - RW
 - Group - R
 - Other - <None>
- c. Only granted to the owner of the web server process or to a user with system privileges.
- ii. With the proper privilege in the DUT, we can see the permission on the configuration file.
 - a. Command used: *ls -la <path to the configuration file>*

```
amf@localhost $ ls -la apache2.conf
-rw-rw-r-- 1 www-data www-data 7567 Jun 28 05:03 apache2.conf
```

- b. Here we can see that
 - Owner - RW
 - Group - RW
 - Other - R
- c. Read and Write permission should not be given to the Other and to the Group no write permission.
- iii. With the proper privilege in the DUT, we can see the permission on the configuration file.
 - a. Command used: *ls -la <path to the VHOST configuration file>*

```
amf@localhost $ ls -la 000-default.conf
-rw-r----- 1 ubuntu ubuntu 1402 Jun 26 11:10 000-default.conf
```

- b. Here we can see that
 - Owner - RW
 - Group - R
 - Other - <None>
- c. Only granted to the owner of the web server process or to a user with system privileges.
- iv. With the proper privilege in the DUT, we can see the permission on the configuration file.
 - a. Command used: *ls -la <path to the VHOST configuration file>*

```
amf@localhost $ ls -la 000-default.conf
-rw-rw-r-- 1 ubuntu ubuntu 1402 Jun 26 11:10 000-default.conf
```

- b. Here we can see that
 - Owner - RW
 - Group - RW

- Other - R
- c. Read and Write permission should not be given to the Other and to the Group no write permission.
- v. The Above step for Virtual Host should be done for every Vhosts file.

11.1.4. **Test Observations:** It should be ensured and verify that the relevant system settings and configurations are correct to ensure fulfilment of the requirement.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_ACCESS_RIGHTS_WEB_SERVER_FILES		



2.11.10 TSTP for Evaluation of No Default Content

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.10
--	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

37. <ITSAR Section No & Name> Section 11: Web Server

38. <Security Requirement No & Name > 1.11.10: No Default Content

39.<Requirement Description: > Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed

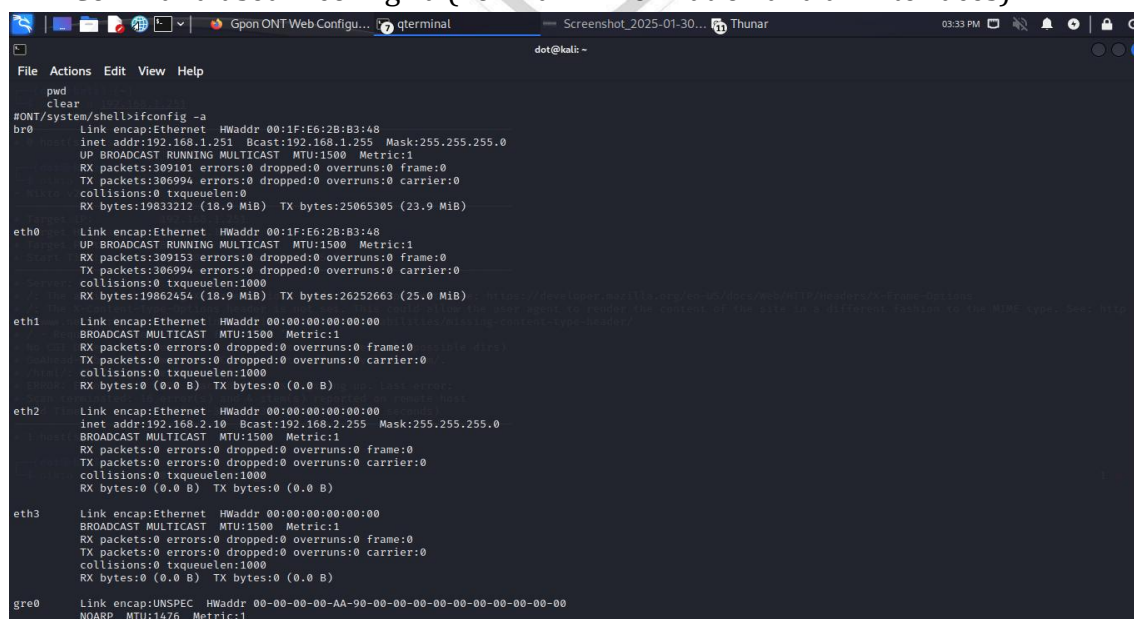
40.Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9

41.

42. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info
 - Command used: ifconfig -a (To find IP information and all interfaces)



```
dot@kali: ~  
File Actions Edit View Help  
pwd  
clear  
#ONT/system/shell>ifconfig -a  
br0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
      inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0  
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
      RX packets:309101 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:0  
      RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)  
  
eth0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
      RX packets:309153 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)  
  
eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
      BROADCAST MULTICAST MTU:1500 Metric:1  
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
      inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0  
      BROADCAST MULTICAST MTU:1500 Metric:1  
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
      BROADCAST MULTICAST MTU:1500 Metric:1  
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
gre0: Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00  
      NOARP MTU:1476 Metric:1
```

- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer N:R2.0.9.6
#ONT/system>
```

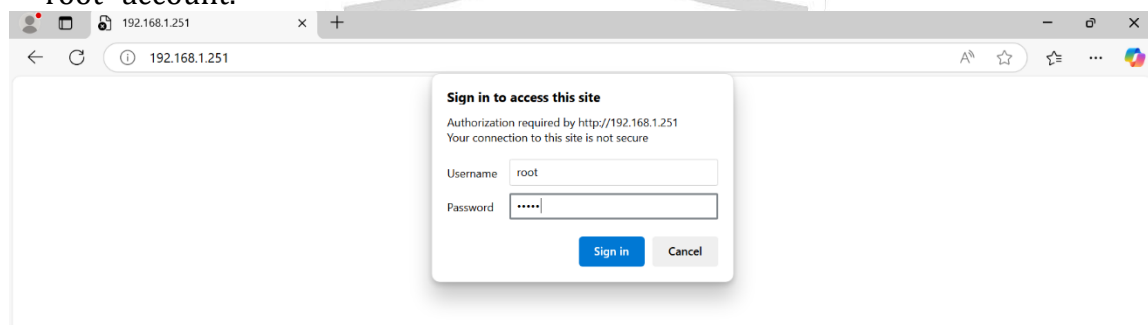
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

43. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info

192.168.1.251/html/frame.html

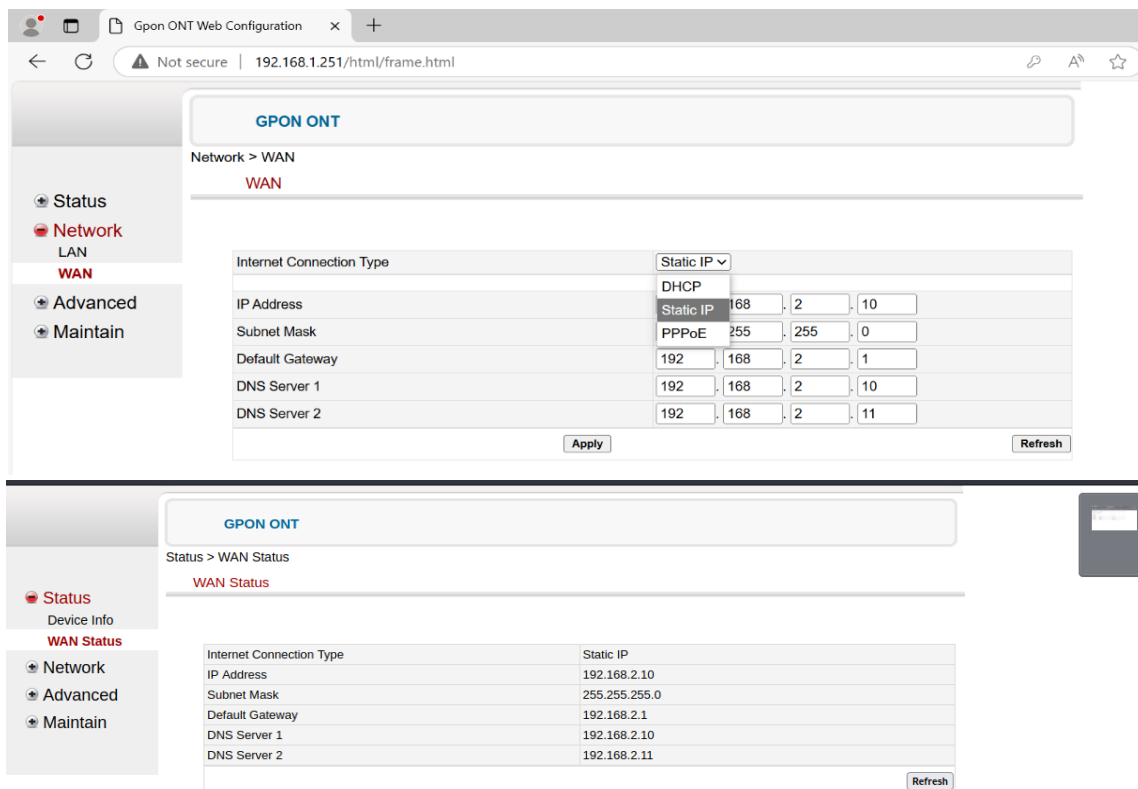
GPON ONT

Status > Device Info

Device Info

Equipment ID:	00142-00029-43
Hardware Version:	02
Software Version:	R2.0.9.6
Build Date:	2017-09-11
MAC Address	00-1F-E6-2B-B3-48
Current Time	2000-01-01 00:29:55

- Set the static IP address



44. Preconditions

- The tester has administrative privileges
- A tester machine is available.
- Test environment with a Web Browser.

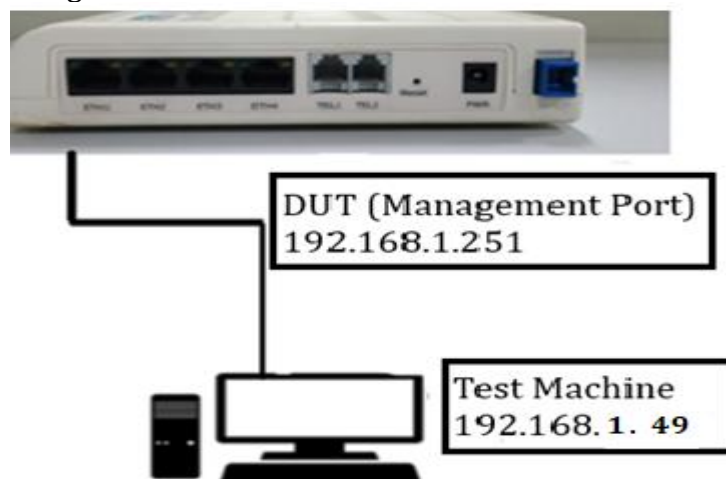
45. Test Objective: To verify that there is no default content on the web server, that is not needed for web server operation, since such default content can be useful for an attacker.

46. Test Plan:

8.5 Number of Test Scenarios: *Securing Networks*

8.1.1 Check whether the webserver has any default content

8.1.2 Test Bed Diagram



8.6 Tools Required: Browser

8.7 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Web Server in the browser.
- iii. The tester should verify the Web-Server documentation to know the default contents which gets installed along with the Web-Server installation.
- iv. The tester manually verifies that the no default content is available.

47. Expected Results for Pass: No default content (examples, help files, documentation, aliases, un-needed directories or manuals) has been found to remain on any Web server component.

48. Expected Format of Evidence: Log files and screen shots of test executions.

49. Test Execution:

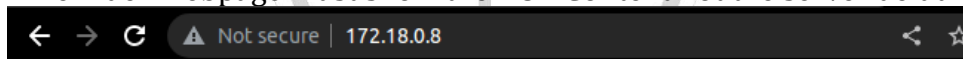
11.1 Test Case Number: 01

11.1.1. **Test Case Name:** TC_NO_DEFAULT_CONTENT

11.1.2. **Test Case Description:** To verify that there is no default content on the web server, that is not needed for web server operation, since such default content can be useful for an attacker.

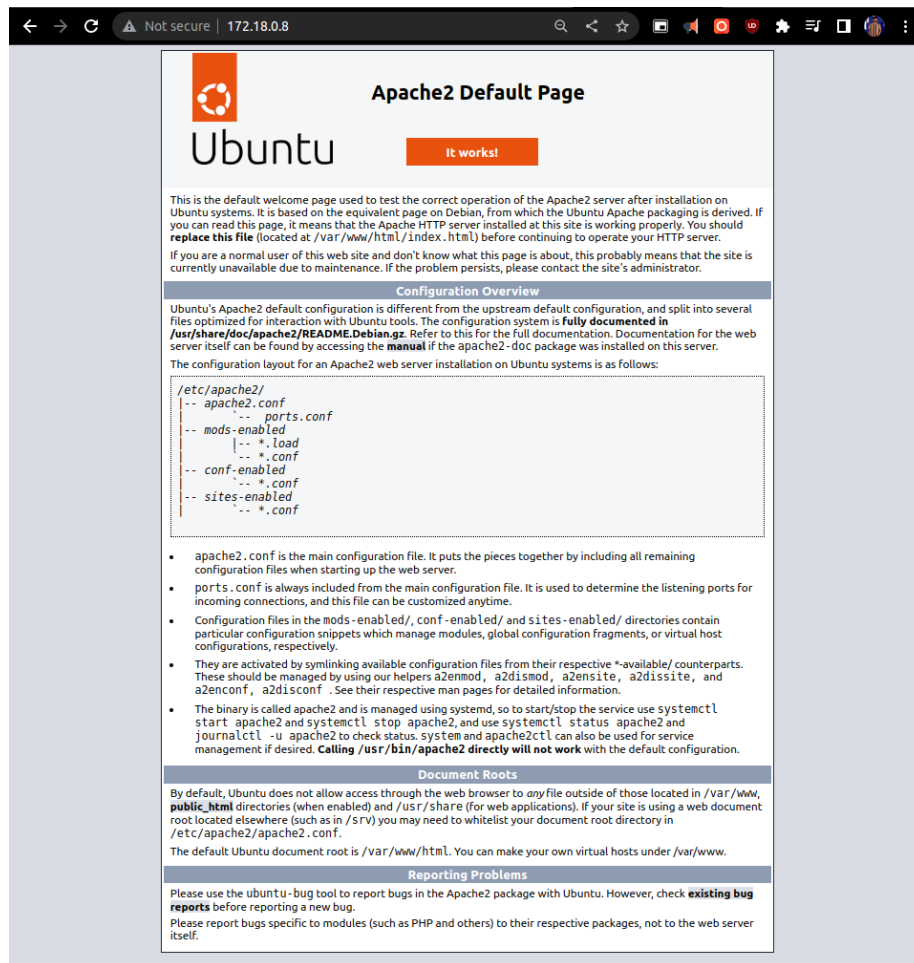
11.1.3. **Execution Steps:**

- i. The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.
- ii. URL: `http://<IP address of DUT>`
- iii. The index webpage must show the DUT Content not the server default content.



DUT - WEB SERVER

- iv. The tester opens any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.
- v. URL: **`http://<IP address of DUT>`**
- vi. (NO Default content should be visible as shown below)



- vii. NOTE: Tester should check the root directory and all accessible directories by the web server and ensure there are no examples, help files, documentation, or aliases. Here there only the root directory is present, so we are only checking that. Test is not complete without a thorough check of all directories present by default.
- viii. For example, the default director is /var/www/html in httpd. As we can see only index.html is present here

```
naan30@naa30-pc: /var/www/html$ ls
index.html
naan30@naa30-pc: /var/www/html$
```

11.1.4. **Test Observations:** It should be ensured that Web Server Component should not serve default content.

50. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_DEFAULT_CONTENT		

2.11.11 TSTP for Evaluation of No directory listings

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no2.11.11
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

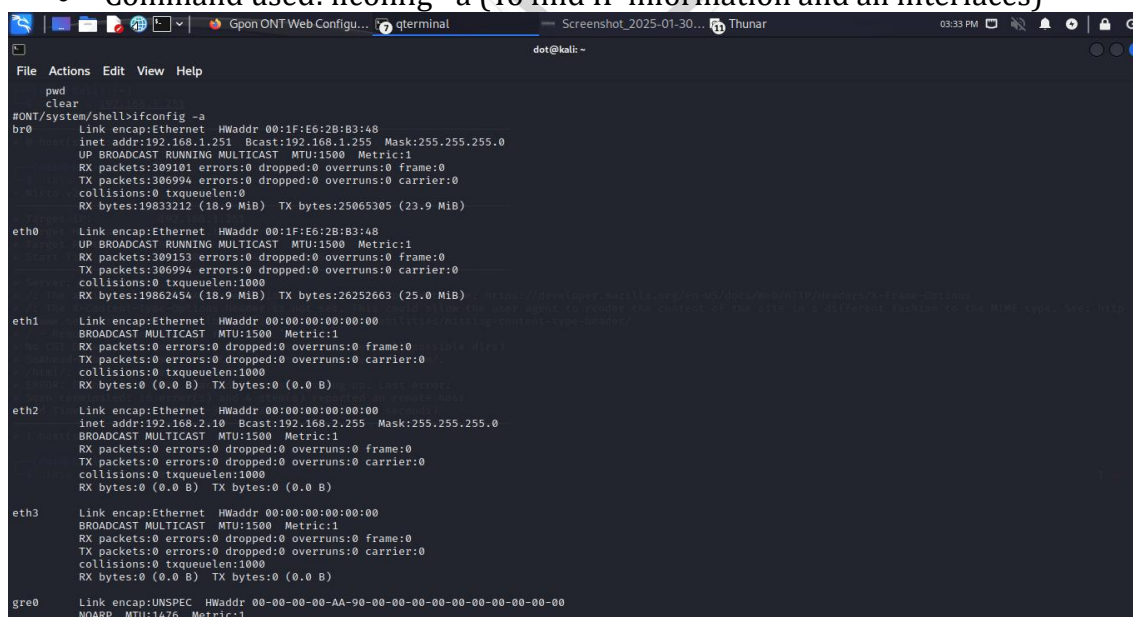
1. <ITSAR Section No & Name> Section 1.11: No directory listings
2. <Security Requirement No & Name > 2.11.11: No Directory Listing
3. **Requirement Description:** Directory listings(indexing) / "Directory browsing" shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. section 4.3.4.10]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
 - ii. Use command to get Application No/Version No & Kernel Info
- Command used: ifconfig -a (To find IP information and all interfaces)



- The below screenshot shows the firmware version of the DUT


```
#ONT/system>ontver
OntSwVer N:R2.0.9.6
#ONT/system>
```

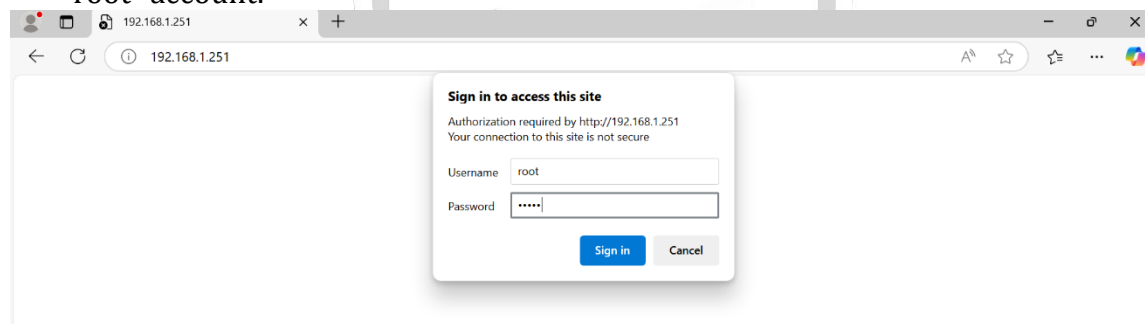
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

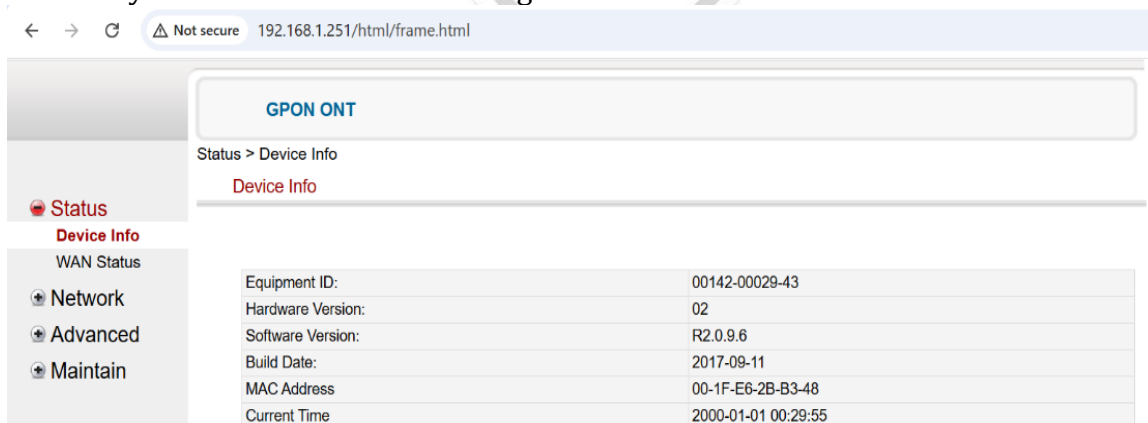
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

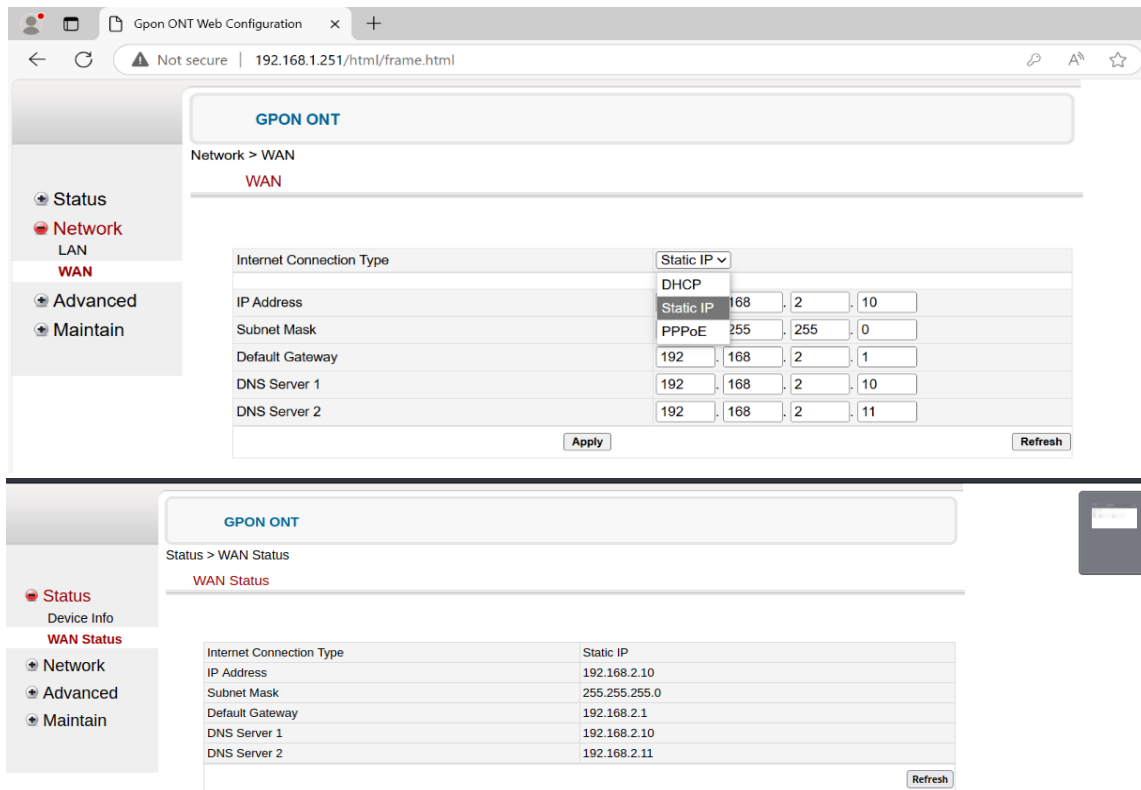
- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address



6. Preconditions

- The tester has administrative privileges
- A tester machine is available.
- Test environment with a Web Browser.

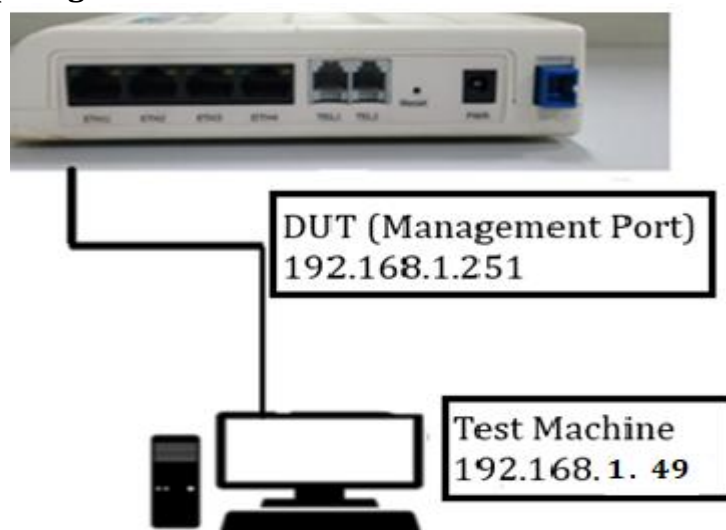
7. **Test Objective:** To verify that Directory listings / Directory browsing has been deactivated in all Web server components.

8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for Apache: This test scenario is regarding Apache Web Serve

8.2 Test Setup Diagram:



8.3 **Tools Used:** Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Web Server in the browser.
- iii. The tester verifies that the Directory Listing/Indexing is disabled.
- iv. The tester also scans the Web Server using a suitable tool (e.g. Nikto) to verify that the Directory listing is not present.

9. **Expected Results for Pass:** Evidence that Directory listing / Directory browsing has been deactivated in all Web server components.

10. **Expected Format of Evidence:** Log files and screen shots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_NO_DIRECTORY_LISTINGS

11.1.2. Test Case Description: To verify that Directory listings / Directory browsing has been deactivated in all Web server components.

11.1.3. Execution Steps:

- i. The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.
 - a. URL: *http://<IP address of DUT>*
 - b. The Webpage must show Forbidden with a HTTP status code 403.



Forbidden

You don't have permission to access this resource.

Apache/2.4.55 (Ubuntu) Server at 172.18.0.8 Port 80

c. With the proper privilege in the DUT while accessing the Log file we can see the following log info. *Securing Networks*

d. Command used: *cat /var/log/apache2/error.log*

```
anf@localhost $ cat /var/log/apache2/error.log
[Thu May 25 06:16:02.813553 2023] [autoindex:error] [pid 12:tid 139864527857344] [client 172.18.0.1:52082] AH01276: Can not serve directory /var/www/html/: No matching DirectoryIndex (index.html,index.cgi,index.pl,index.php,index.xhtml,index.htm) found, and server-generated directory index forbidden by Options directive
```

server-generated directory index forbidden by Options directive

- ii. The tester opens any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.
 - a. URL: *http://<IP address of DUT>*
 - b. (NO Directory listing/indexing should not be visible [as shown below])

Index of /

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	conf/	2023-05-25 05:51	-	
	configuration.conf	2023-05-25 05:50	15	
	image.png	2023-05-25 05:49	15	
	main.html	2023-04-26 21:58	10K	
	main.py	2023-05-25 05:49	15	

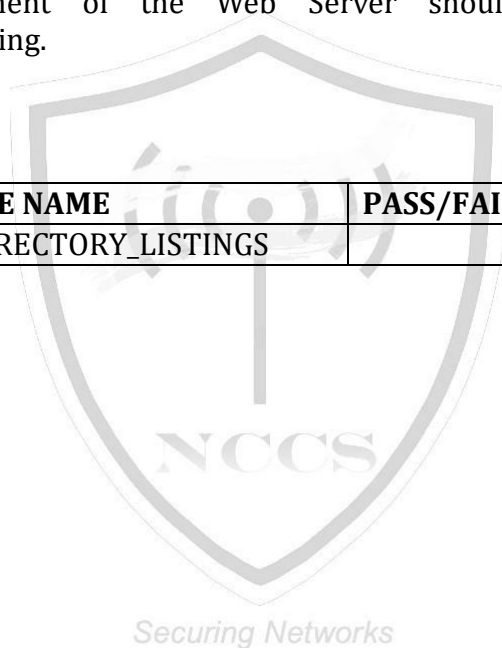
Apache/2.4.55 (Ubuntu) Server at 172.18.0.8 Port 80

- iii. The tester repeats the above steps to verify that directory listing is disabled for all directories and subdirectories accessible by the web server.

11.1.4. **Test Observations:** It should be ensured that any path in the Web Server or any Component of the Web Server should not allow Directory Listing/Indexing.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_DIRECTORY_LISTINGS		



2.11.12 TSTP for Evaluation of Web Server information in HTTPS headers

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.12
--	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 1.11: Web Interface
2. <Security Requirement No & Name > 1.11.12: Web server information in HTTPS headers
3. **Requirement Description:** The HTTPS header shall not include information on the version of the ONU/ONT webserver and the modules/add-ons used.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.11]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
 - ii. Use command to get Application No/Version No & Kernel Info
- Command used: `ifconfig -a` (To find IP information and all interfaces)

```

dot@kali: ~
pwd
clear
#ONT/system/shell>ifconfig -a
br0    Link encap:Ethernet  HWaddr 00:1F:E6:2B:B3:48
       inet addr:192.168.1.251  Bcast:192.168.1.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
       TX packets:306996 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0    Link encap:Ethernet  HWaddr 00:1F:E6:2B:B3:48
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
       TX packets:306996 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
       BROADCAST MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
       inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
       BROADCAST MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3    Link encap:Ethernet  HWaddr 00:00:00:00:00:00
       BROADCAST MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0    Link encap:UNSPEC  HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
       NOARP  MTU:1476  Metric:1
  
```

- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer  : R2.0.9.6
#ONT/system>
```

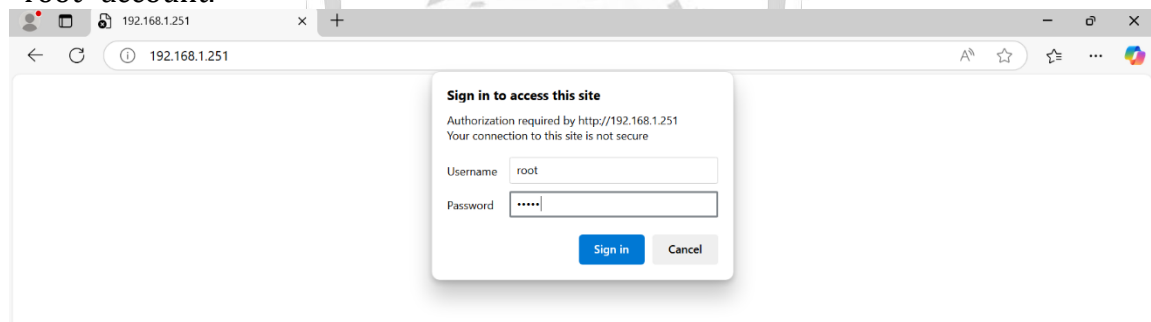
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

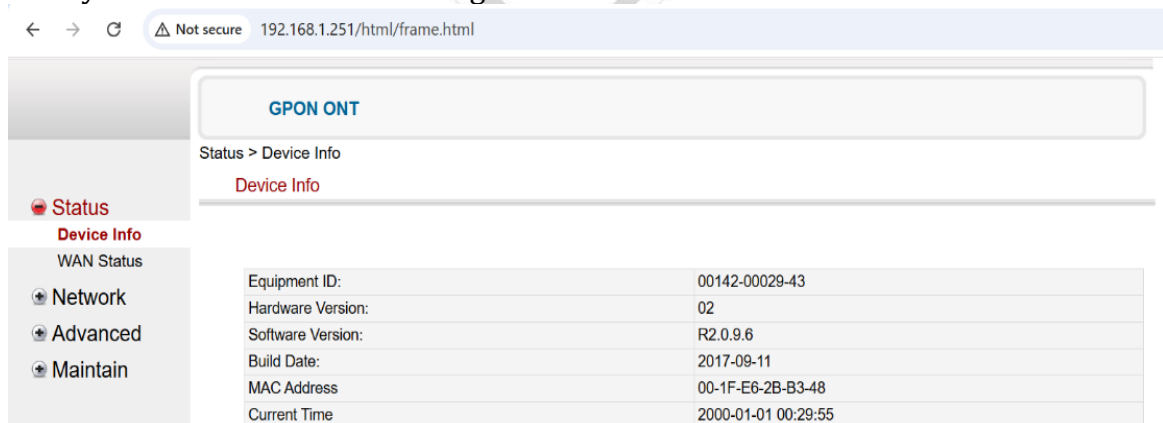
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

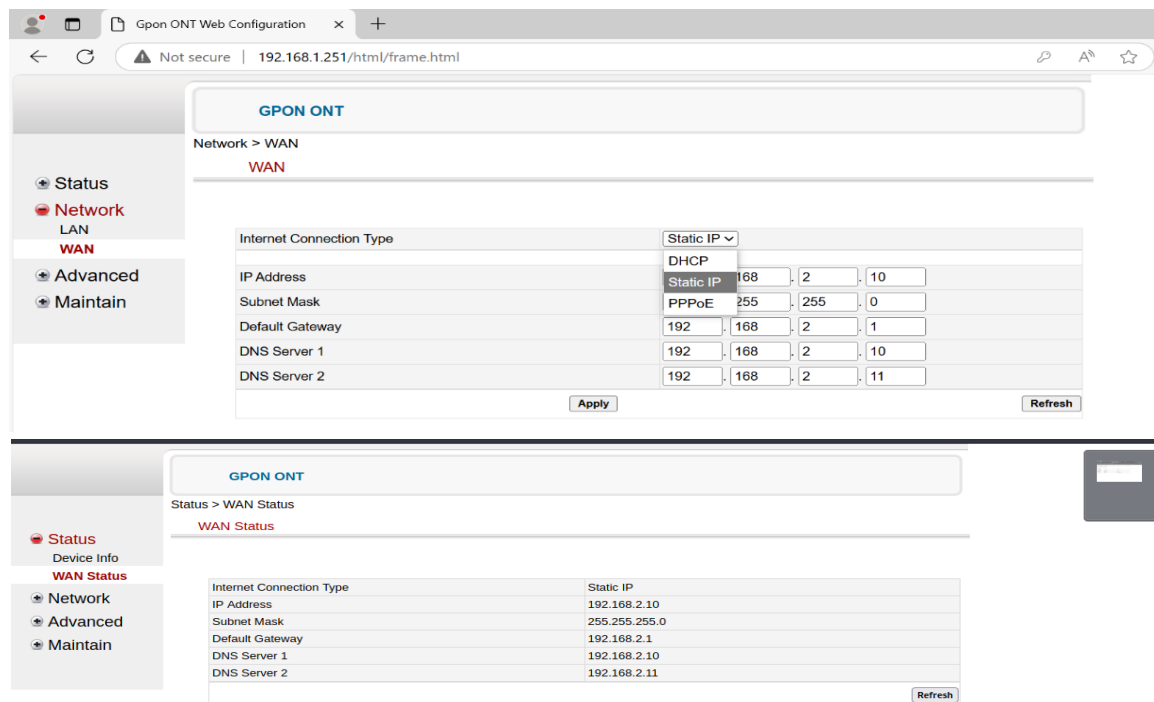
- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address



6. Preconditions:

- The tester has administrative privileges
- A tester machine is available.
- Test environment with a Terminal.

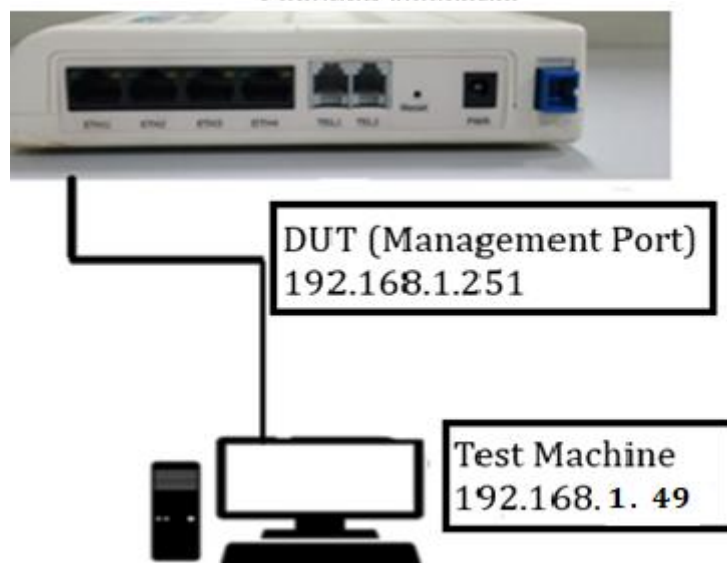
7. **Test Objective:** To verify that HTTP headers do not include information on the version of the web server and the modules/add-ons used.

8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for Apache: This test scenario is regarding Apache Web Server

8.2 **Test-bed setup Diagram:**



8.3 **Tools Used:** Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 **Test Objective:** To Verify that HTTP headers do not include information on the version of the web server and the modules/add-ons used.

8.5 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Header of Web Server.
- iii. The tester manually verifies that HTTP headers do not include information on the version of the web server.
- iv. The tester will run some web scanning tools like Nikto, to get the detailed information and verify that the HTTP headers do not include information on the version of the web server.

9. **Expected Results for Pass:** Evidence that HTTP headers do not include information on the version of the web server and the modules/addons used.

10. **Expected Format of Evidence:** Log files and screen short of test executions.

11. **Test Execution:**

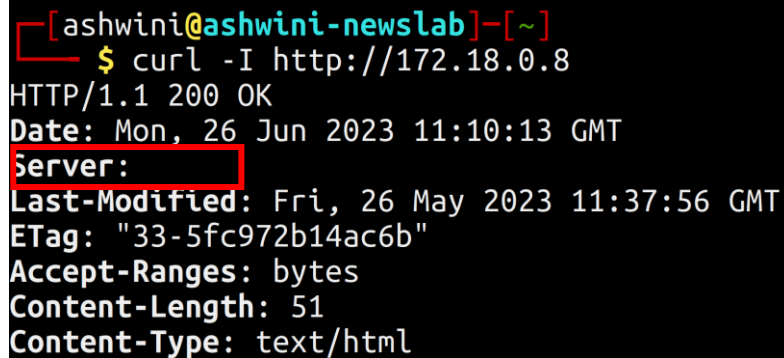
11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_NO_WEB_SERVER_HEADER_INFORMATION

11.1.2. Test Case Description: To verify that HTTP headers do not include information on the version of the web server and the modules/add-ons used.

11.1.3. Execution Steps:

- i. The tester shall open any terminal emulator and use the following command.
 - Command used: *curl -I http://< IP address of DUT >*



```
[ashwini@ashwini-news1ab]~$ curl -I http://172.18.0.8
HTTP/1.1 200 OK
Date: Mon, 26 Jun 2023 11:10:13 GMT
Server:
Last-Modified: Fri, 26 May 2023 11:37:56 GMT
ETag: "33-5fc972b14ac6b"
Accept-Ranges: bytes
Content-Length: 51
Content-Type: text/html
```

- We can see that the HTTP headers do not include information on the version of the web server and the modules/addons used.
- ii. The tester shall open any terminal emulator and use the following command.
 - Command used: *curl -I http://< IP address of DUT >*

```

[ashwini@ashwini-news1ab]-[~]
$ curl -I http://172.18.0.8
HTTP/1.1 200 OK
Date: Fri, 26 May 2023 11:45:35 GMT
Server: Apache/2.4.55 (Ubuntu)
Last-Modified: Fri, 26 May 2023 11:37:56 GMT
ETag: "33-5fc972b14ac6b"
Accept-Ranges: bytes
Content-Length: 51
Content-Type: text/html

```

- We can see that the HTTP headers do include information on the version of the web server and the modules/addons used.
- (This should not be present)

11.1.4. **Test Observations:** It should be ensured that the HTTP headers do not include information on the version of the web server and the modules/addons used.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_WEB_SERVER_HEADER_INFORMATION		

Securing Networks

2.11.13 TSTP for Evaluation of Web server information in error pages

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.13
--	--------------------------	-------------------

<DUT Details: > Alphon AONT100C

<DUT Software Version:> R2.0.9.6

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 11: Web Server
2. **<Security Requirement No & Name >** 2.11.13 Web server information in error pages.
3. **<Requirement Description: >**ONU/ONT to have capability to log important Security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.
[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.6.1;
2) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.5]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
- ii. Use command to get Application No/Version No & Kernel Info
 - Command used: **ifconfig -a** (To find IP information and all interfaces)


```

#ONT/system>clear
#ONT/system>show ipconfig -a
br0
  Link encap:Ethernet  HWaddr 00:1F:E6:28:B3:48
  inet addr:192.168.1.251  Bcast:192.168.1.255  Mask:255.255.255.0
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
  TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0
  Link encap:Ethernet  HWaddr 00:1F:E6:28:B3:48
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
  TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1
  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
  BROADCAST MULTICAST  MTU:1500  Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2
  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
  inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
  BROADCAST MULTICAST  MTU:1500  Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3
  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
  BROADCAST MULTICAST  MTU:1500  Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0
  Link encap:UNSPEC  HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
  NOARP  MTU:1476  Metric:1

```

- The below screenshot shows the firmware version of the DUT

```

#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>

```

- The below screenshot shows the information of the DUT

```

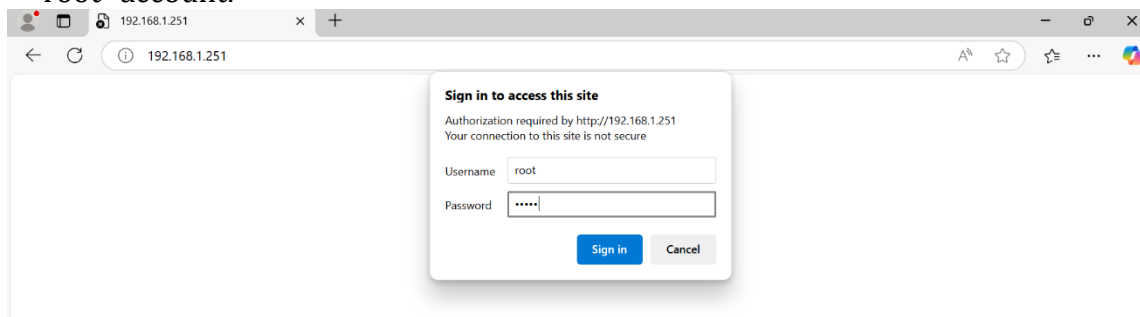
#ONT/system>custom
Customer Information

Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>

```

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info

← → ↻ ⚠ Not secure 192.168.1.251/html/frame.html

GPON ONT

Status > Device Info

Device Info

Equipment ID:	00142-00029-43
Hardware Version:	02
Software Version:	R2.0.9.6
Build Date:	2017-09-11
MAC Address	00-1F-E6-2B-B3-48
Current Time	2000-01-01 00:29:55

Status

Device Info

WAN Status

Network

Advanced

Maintain

iv. Set the static IP address

Gpon ONT Web Configuration x +

← ↻ ⚠ Not secure | 192.168.1.251/html/frame.html

GPON ONT

Network > WAN

WAN

Internet Connection Type: Static IP

IP Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server 1: 192.168.2.10

DNS Server 2: 192.168.2.11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

Status

Device Info

WAN Status

Network

Advanced

Maintain

v. Example list of Web Server may be present as per (NMAP and OEM Documentation)

- Apache httpd
- Nginx
- Lighttpd
- Microsoft IIS and more

vi. Note: We have made this TSTP for Apache httpd Web Server the tester must verify for the respective Web Server as mentioned in the OEM documentation.

a. For Apache httpd:

- Command used: **apachectl -v** (To get version information)

```
amf@localhost $ apachectl -v
Server version: Apache/2.4.55 (Ubuntu)
Server built: 2023-03-08T16:32:34
```

- Command used:
 - **apachectl -V | grep HTTPD_ROOT** (To get the Root directory of apache2)
 - **apachectl -V | grep SERVER_CONFIG_FILE** (To get the config file name)
 - Using that we found the Apache config file is in: **"/etc/apache2/apache2.conf"**

```
amf@localhost $ apachectl -V | grep HTTPD_ROOT
-D HTTPD_ROOT="/etc/apache2"

amf@localhost $ apachectl -V | grep SERVER_CONFIG_FILE
-D SERVER_CONFIG_FILE="apache2.conf"
```

- Command used: **grep -I "Server Signatures" /etc/apache2/apache2.conf** (To check Apache will suppresses the footer line which contain Server information in error pages)
 - The Server Signature directive allows the configuration of a trailing footer line under server-generated documents (error messages, mod_proxy ftp directory listings, mod_info output, ...).
 - The **Off setting**, which is the default, suppresses the footer line. The **On setting** simply adds a line with the server version number and Server Name of the serving virtual host, and the **Email setting** additionally creates a "mailto:" reference to the Server Admin of the referenced document.

```
amf@localhost $ grep -I "ServerSignature" /etc/apache2/apache2.conf
ServerSignature Off
```

- (Above result states that ServerSignatures should be set to off not anything else)

6. Preconditions

- The tester has administrative privileges
- A tester machine is available.
- Test environment with a Terminal.

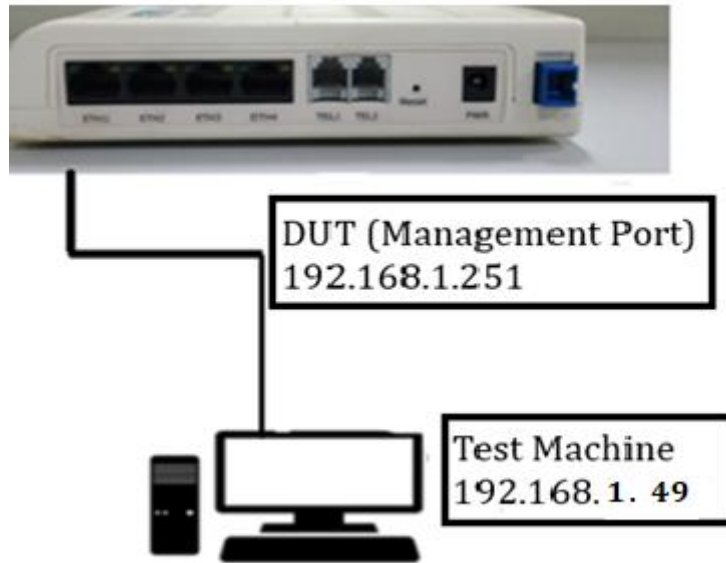
7. **Test Objective:** To verify that error pages and error messages do not include information about the web server.

8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for Apache: This test scenario is regarding Apache Web Server

8.2 Test Setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Header of Web Server.
- iii. The tester verifies that generated error pages and error messages do not include information about the web server.
- iv. Tester checks for any other Error case like 5XX, 4XX errors.
- v. Tester checks for one more error scenario randomly.
- vi. If the tester does not have access to the web server configuration files on the DUT, then the test is to be performed for all the Http error scenarios (5XX, 4XX).

9. **Expected Results for Pass:** Evidence that generated error pages and error messages do not include information about the web server.

10. **Expected Format of Evidence:** Log files and screenshots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. **Test Case Name:** TC_NO_WEB_SERVER_ERROR_PAGES_INFORMATION

11.1.2. **Test Case Description:** To verify that error pages and error messages do not include information about the web server.

11.1.3. Execution Steps:

- i. The tester shall open any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.
 - URL: ***http://<IP address of DUT>/<random text>***
 - (Random text is used so that we can get the Http 404 error)



Not Found

The requested URL was not found on this server.

- ii. We can see that the error page does not include information on the version of the web server and the modules/addons used.
- iii. The tester opens any Web Browser (Mozilla Firefox, Google Chrome) and go to the web address/IP of the DUT.
 - a. URL: `http://<IP address of DUT>/ <random text>`
 - b. (Random text is used so that we can get the Http 404 error)
 - c. (NO Directory listing/indexing should not be visible)



Not Found

The requested URL was not found on this server.

Apache/2.4.55 (Ubuntu) Server at 172.18.0.8 Port 80

- d. We can see that the error page does include information on the version of the web server and the modules/addons used.
 - e. (This should not be present)
 - f. Tester checks for any other Error case like 5XX, 4XX errors.
 - g. Tester checks for one more error scenario randomly.
 - h. If the tester does not have access to the web server configuration files on the DUT, then the test is to be performed for all the Http error scenarios (5XX, 4XX).
- 11.1.4. **Test Observations:** It should be ensured that the error page does not include information on the version of the web server and the modules/addons used.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_WEB_SERVER_ERROR_PAGES_INFORMATION		

2.11.14 TSTP for Minimized file type mappings (not there in Wi Fi)

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.14
--	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

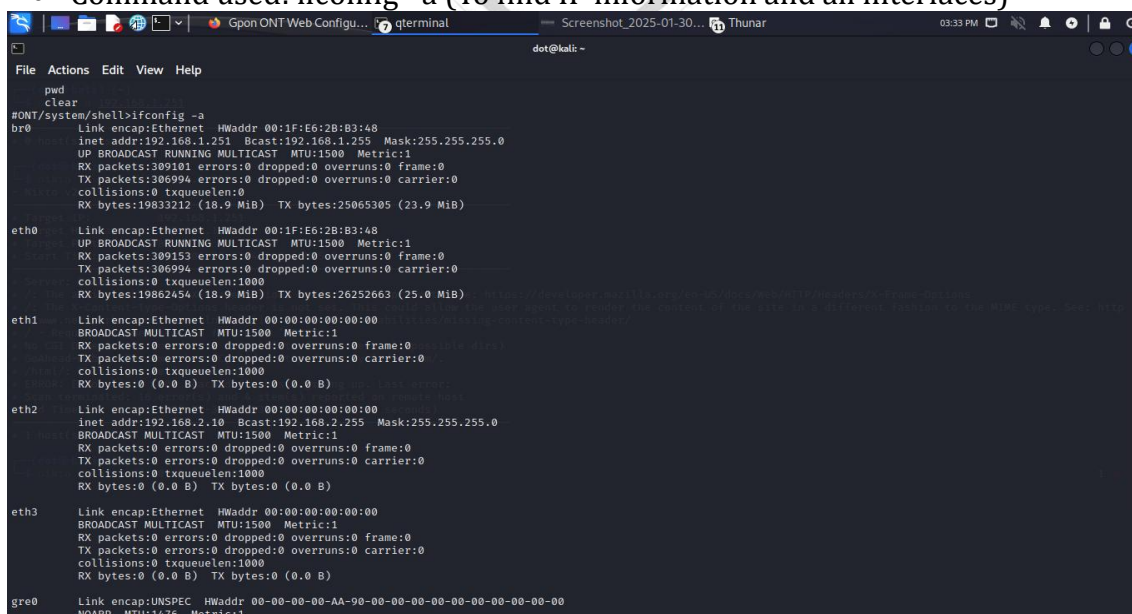
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 1.11: Web Servers
2. <Security Requirement No & Name > 1.11.14: Minimized file type mappings (not there in Wi Fi)
3. <Requirement Description:> File type or script-mappings that are not required for ONU/ONT operation shall be deleted.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- i. Use command to get Interfaces details
 - ii. Use command to get Application No/Version No & Kernel Info
- Command used: ifconfig -a (To find IP information and all interfaces)



```
dot@kali: ~  
File Actions Edit View Help  
pwd  
clear  
#ONT/system/shell$ifconfig -a  
br0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:389101 errors:0 dropped:0 overruns:0 frame:0  
TX packets:386994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:19833212 (18.9 MiB) TX bytes:25065305 (23.9 MiB)  
  
eth0: Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:389153 errors:0 dropped:0 overruns:0 frame:0  
TX packets:386994 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:19862454 (18.9 MiB) TX bytes:26252663 (25.0 MiB)  
  
eth1: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth2: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
eth3: Link encap:Ethernet HWaddr 00:00:00:00:00:00  
BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
gre0: Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00  
NOARP MTU:1476 Metric:1
```

- The below screenshot shows the firmware version of the DUT


```
#ONT/system>ontver
OntSwVer N:R2.0.9.6
#ONT/system>
```

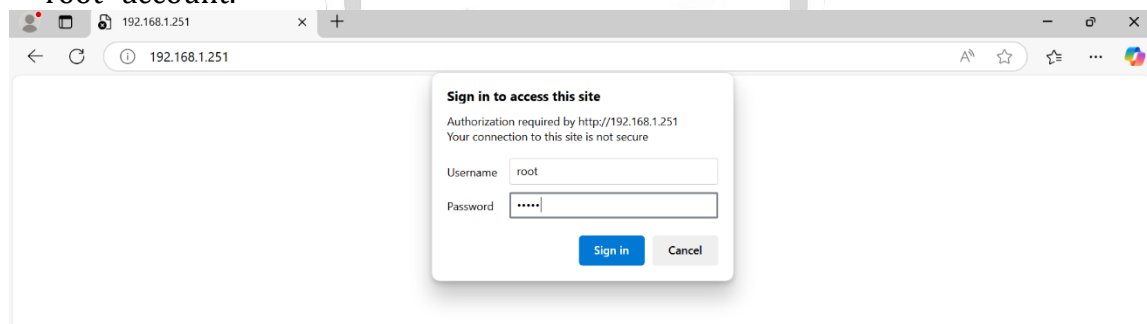
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

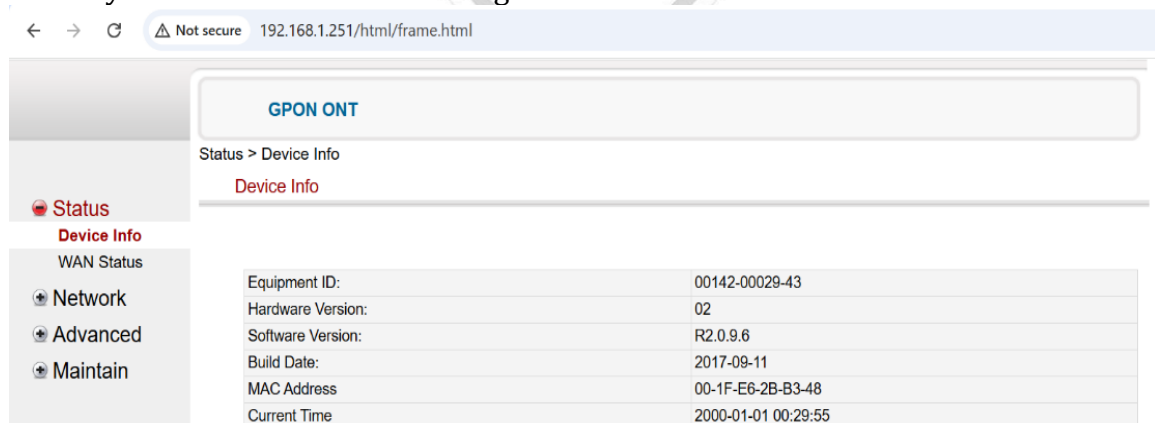
Customer Name      : UUAP
Customer Full Name : Alphon
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

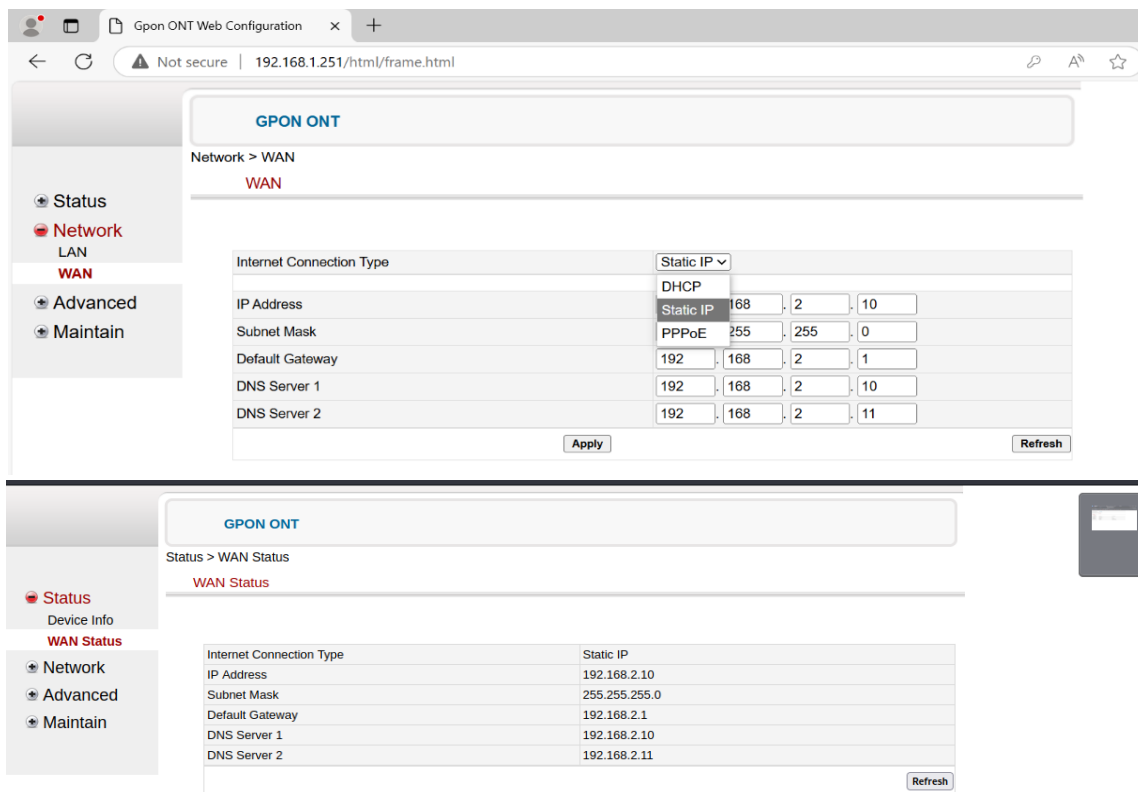
- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address



6. Preconditions

- The tester has administrative privileges
- The web server is configured according to the manual
- The vendor must provide the list of necessary file types.
- A tester machine is available.

7. Test Objective: To verify that file type- or script-mappings that are not required have been deleted.

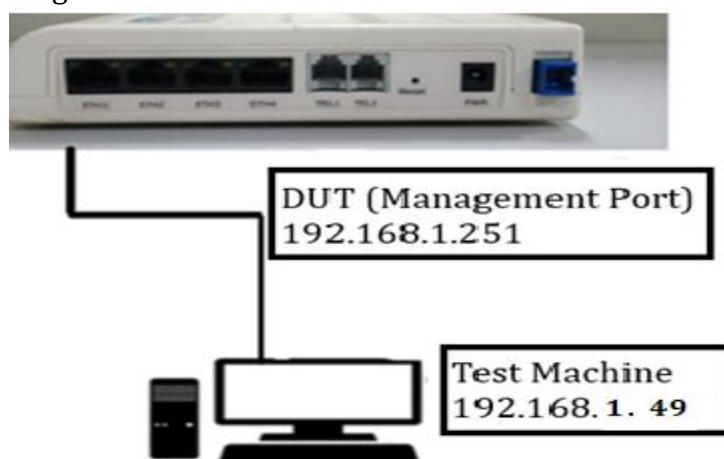
8. Test Plan:

8.1 Number of Test Scenarios: *Securing Networks*

8.1.1 Test Scenario for Apache

8.1.2 This test scenario is regarding Apache Web Server

8.2 Test Setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester manually verifies that the file type- or script-mappings that are not required have been deleted.

9. Expected Results for Pass: Evidence that all file type- or script-mappings, that are not required, have been deleted.

10. Expected Format of Evidence: Log files and screen shots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_NO_WEB_SERVER_FILE_TYPE MAPPINGS

11.1.2. Test Case Description: To verify that file type- or script-mappings that are not required have been deleted.

11.1.3. Execution Steps:

- i. With the proper privilege in the DUT access the shell to see the file types that are commented out.

a. Command used: *grep -I "AddType" <path of configuration file>*

```
amf@localhost $ grep -I "AddType" /etc/apache2/apache2.conf
AddType text/html .html
# AddType image/gif .gif
# AddType application/x-httpd-php .php
# AddType application/x-httpd-php .phtml
# AddType application/x-httpd-php .php3
# AddType text/javascript .js
# AddType application/x-sh .sh
# AddType application/x-csh .csh
# AddType application/vnd.microsoft.portable-executable .exe
# AddType application/x-perl .pl
# AddType text/x-vb .vbe
# AddType text/vbscript .vbs
```

b. Here we can see that the File type that has been added in the server using AddType Directive.

c. The File Types have been commented out using "#"

d. The tester will compare the list by the Vendor and the output of the command any filetype left the test case will fail.

- ii. With the proper privilege in the DUT access the shell to see the which File types are been removed.

a. Command used: *grep -I "RemoveType" <path of configuration file>*

```
amf@localhost $ grep -I "RemoveType" /etc/apache2/apache2.conf
RemoveType .gif
RemoveType .php
RemoveType .phtml
RemoveType .php3
RemoveType .js
RemoveType .sh
RemoveType .csh
RemoveType .exe
RemoveType .pl
RemoveType .vbe
RemoveType .vbs
```

- b. (Here we can see that the unnecessary file types are removed using *Remove Type Directive*)
- 11.1.4. Test Observations: Hence we verified that the unnecessary file types are removed in the web server.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_NO_WEB_SERVER_FILE_TYPE MAPPINGS		



2.11.15 TSTP for Evaluation of Restricted file access

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.15
--	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 11: Web Server

2. <Security Requirement No & Name > 1.11.15 Restricted file access

3. <Requirement Description: > Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the ONU/ONT webserver's document directory. In particular, the ONU/ONT webserver shall not be able to access files which are not meant to be delivered.

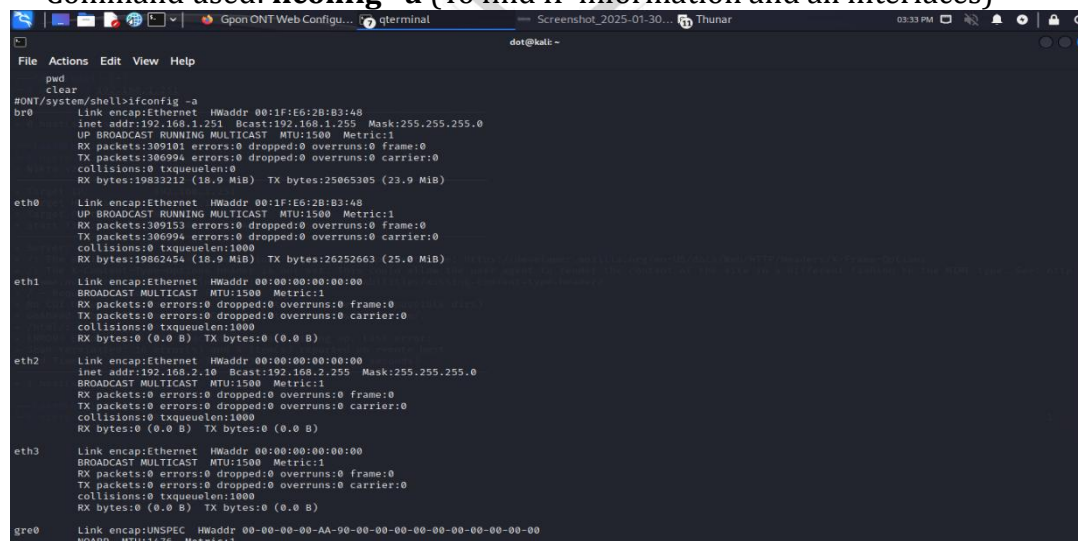
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0 section 4.3.4.14]

4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

- Use command to get Interfaces details
- Use command to get Application No/Version No & Kernel Info

• Command used: **ifconfig -a** (To find IP information and all interfaces)



```
dot@kali: ~
File Actions Edit View Help
pwd
clear
#ONT/system/shell>ifconfig -a
brw      Link encap:Ethernet  HWaddr 00:1F:E6:2B:83:48
        inet addr:192.168.1.251  Bcast:192.168.1.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
        TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0     Link encap:Ethernet  HWaddr 00:1F:E6:2B:83:48
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
        TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1     Link encap:Ethernet  HWaddr 00:00:00:00:00:00
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2     Link encap:Ethernet  HWaddr 00:00:00:00:00:00
        inet addr:192.168.2.10  Bcast:192.168.2.255  Mask:255.255.255.0
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3     Link encap:Ethernet  HWaddr 00:00:00:00:00:00
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0     Link encap:UNSPEC  HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00-00
        NOARP  MTU:1476  Metric:1
```

• The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>
```

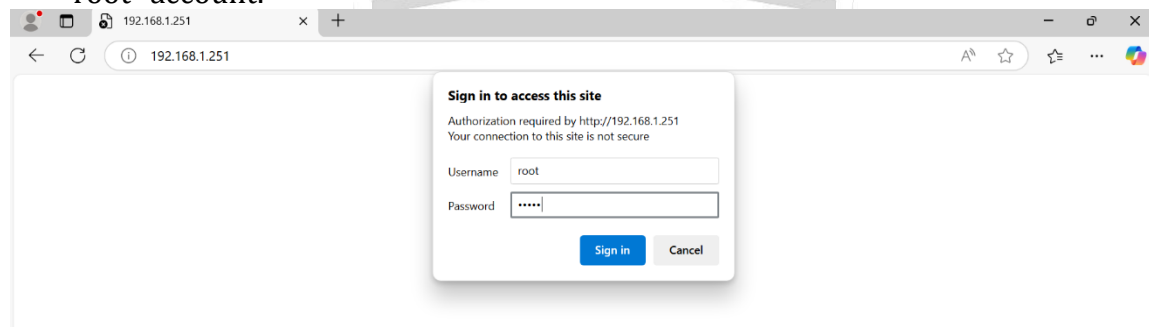
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

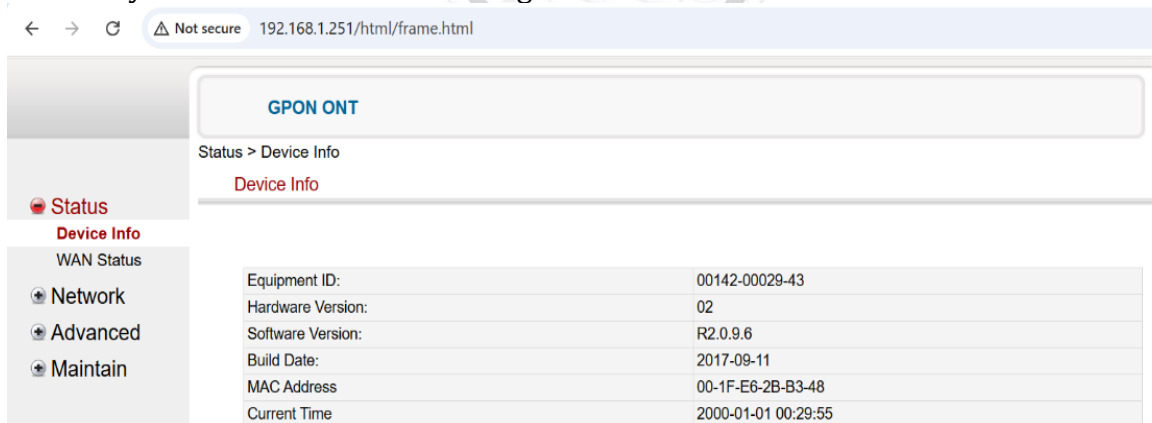
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address

The image shows two screenshots of the GPON ONT Web Configuration interface. The top screenshot displays the 'Network > WAN' configuration page. The left sidebar has 'Status', 'Network' (selected), 'LAN', 'WAN', 'Advanced', and 'Maintain'. The main area shows the 'WAN' configuration with a dropdown menu open for 'Internet Connection Type', showing options: DHCP, Static IP (selected), and PPPoE. Below the dropdown are input fields for IP Address (192.168.2.10), Subnet Mask (255.255.255.0), Default Gateway (192.168.2.1), DNS Server 1 (192.168.2.10), and DNS Server 2 (192.168.2.11). There are 'Apply' and 'Refresh' buttons at the bottom. The bottom screenshot shows the 'Status > WAN Status' page. The left sidebar has 'Status' (selected), 'Device Info', 'WAN Status', 'Network', 'Advanced', and 'Maintain'. The main area shows the 'WAN Status' with a table displaying the same configuration values as the top screenshot. There is a 'Refresh' button at the bottom right.

GPON ONT

Network > WAN

WAN

Internet Connection Type: Static IP

IP Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server 1: 192.168.2.10

DNS Server 2: 192.168.2.11

Apply Refresh

GPON ONT

Status > WAN Status

WAN Status

Internet Connection Type	Static IP
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server 1	192.168.2.10
DNS Server 2	192.168.2.11

Refresh

6. Preconditions

- The tester has administrative privileges
- The web server is configured according to the manual
- A tester machine is available.
- Test environment with a Web Browser.

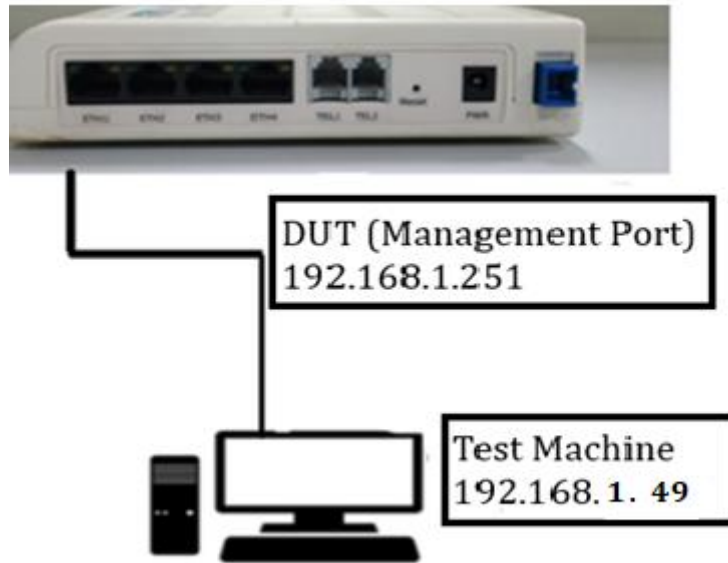
7. Test Objective: To test whether the restrictive access rights are assigned to all files which are directly or indirectly in the web server's document directory and to verify whether path traversal is made improbable.

8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for Apache: This test scenario is regarding Apache Web Server

8.2 Test Setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester verifies that access rights on the servable content (meaning directories and files) is set to the following:
 - o The files are owned by the user that runs the web server;
 - o The files are not writable to others, except the web server's account;
- iii. The tester verifies that the user running the web server is an unprivileged account;(Refer the TSTP for clause 2.11.4 - No system privileges)
- iv. For Operating Systems that have chrooted environments, the tester verifies that the web server runs inside a jail or chrooted environment.
- v. The tester then sets access rights such that only a particular directory and file are accessible from port 80 of the server. Others will be denied.

9. Expected Results for Pass:

- i. Name of user running the web server with the privileges of the account;
- ii. Access rights of files and directories that the web server serves;
- iii. Configuration that shows that the web server is in a chrooted environment

10. Expected Format of Evidence: Log files and screen shots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_RESTRICTED_FILE_ACCESS

11.1.2. Test Case Description: To test whether the restrictive access rights are assigned to all files which are directly or indirectly in the web server's document directory and to verify whether path traversal is made improbable.

11.1.3. Execution Steps:

- i. With the proper privilege in the DUT access the shell to see the owner and group of the files and directories.

a. Command used: **ls -la <path of the directory where the files are hosted>**

```
amf@localhost $ ls -la
total 20
drwxr-xr-x 1 www-data www-data 4096 Jun 19 12:07 .
drwxr-xr-x 1 www-data www-data 4096 Apr 26 21:58 ..
drwxr-xr-x 2 www-data www-data 4096 Jun 19 12:08 cgi-enabled
-rw-rw-r-- 1 www-data www-data  51 May 26 11:37 index.html
```

- b. (Here we can see that both the owner and group of the files are of the www-data that is a special User and Group under Apache)
- ii. With the proper privilege in the DUT access the shell to see the owner and group of the files and directories.

a. Command used: **id**

```
amf@localhost $ id
uid=1001(amf) gid=1001(amf) groups=1001(amf)
```

- b. (Here we can see the USERID is **1001** and the USERNAME is **amf**)
- c. Command used: **echo " " >> <path of the directory where the files are hosted>/<any available file>**

```
amf@localhost $ echo " " >> /var/www/html/index.html
bash: /var/www/html/index.html: Permission denied
```

- d. (Here we can see that the permission is denied cause the user is not the same user as the web server user.)
- iii. With the proper privilege in the DUT access the shell to see the owner and group of the files and directories.

a. Command used: **ps aux | grep apache2**

```
amf@localhost $ ps aux | grep apache2
root      181560  0.0  0.0  6836  5560 ?        Ss   13:50   0:00 /sbin/chroot /chroot/httpd usr/sbin/apache2 -DFOREGROUND -k start
www-data  181561  0.0  0.0  6496  2964 ?        Ss   13:50   0:00 /sbin/chroot /chroot/httpd usr/sbin/apache2 -DFOREGROUND -k start
www-data  181562  0.0  0.0  1997952 4108 ?       Sl   13:50   0:00 /sbin/chroot /chroot/httpd usr/sbin/apache2 -DFOREGROUND -k start
www-data  181563  0.0  0.0  1997952 4132 ?       Sl   13:50   0:00 /sbin/chroot /chroot/httpd usr/sbin/apache2 -DFOREGROUND -k start
root      184505  0.0  0.0   6768  4740 ?        Ss   14:03   0:00 /sbin/chroot /chroot/httpd usr/sbin/apache2 -k start
www-data  184506  0.0  0.0  1998248 5468 ?       Sl   14:03   0:00 /sbin/chroot /chroot/httpd usr/sbin/apache2 -k start
www-data  184507  0.0  0.0  1998176 4528 ?       Sl   14:03   0:00 /sbin/chroot /chroot/httpd usr/sbin/apache2 -k start
amf       188296  0.0  0.0  17864  2528 pts/4    S+   14:28   0:00 grep --colour=auto apache2
```

- b. (We can see every process starts with **/sbin/chroot/** this shows that the Apache server is running in chrooted environment.)
- c. (Anything other than that the test case will fail)
- iv. Additionally, Tester can set Document Root (root folder of web server as a new folder For Example- var/www/secure with it's own html file - Tester will create this directory and index.html inside it)
- v. Then tester will ensure access rights are such that from port 80 externally only index.html of var/www/secure is accessible. Nor is var/www/html accessible

not is any other file in var/www/secure accessible. The settings are change in
vi /etc/apache2/sites-available/000-default.conf

```
<VirtualHost *:80>
```

```
# The ServerName directive sets the request scheme, hostname and port that  
# the server uses to identify itself. This is used when creating  
# redirection URLs. In the context of virtual hosts, the ServerName  
# specifies what hostname must appear in the request's Host: header to  
# match this virtual host. For the default virtual host (this file) this  
# value is not decisive as it is used as a last resort host regardless.  
# However, you must set it for any further virtual host explicitly.
```

```
#ServerName www.example.com
```

```
ServerAdmin webmaster@localhost
```

```
DocumentRoot /var/www/secure
```

```
# Adding another directory
```

```
Alias /secure /var/www/html
```

```
<Directory /var/www/html>
```

```
Options Indexes FollowSymLinks
```

```
AllowOverride All
```

```
Require all granted
```

```
</Directory>
```

```
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
# error, crit, alert, emerg.
```

```
# It is also possible to configure the loglevel for particular  
# modules, e.g.
```

```
#LogLevel info ssl:warn
```

```
ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
# For most configuration files from conf-available/, which are  
# enabled or disabled at a global level, it is possible to  
# include a line for only one particular virtual host. For example the  
# following line enables the CGI configuration for this host only  
# after it has been globally disabled with "a2disconf".
```

```
#Include conf-available/serve-cgi-bin.conf
```

```
</VirtualHost>
```

```
<Directory />
```

```
Order Deny,Allow
```

```
Deny from all
```

```
Options None
```

```
AllowOverride None
```

```
</Directory>
```

```
<Directory /var/www/secure>
```

```
# Deny first, then allow
```

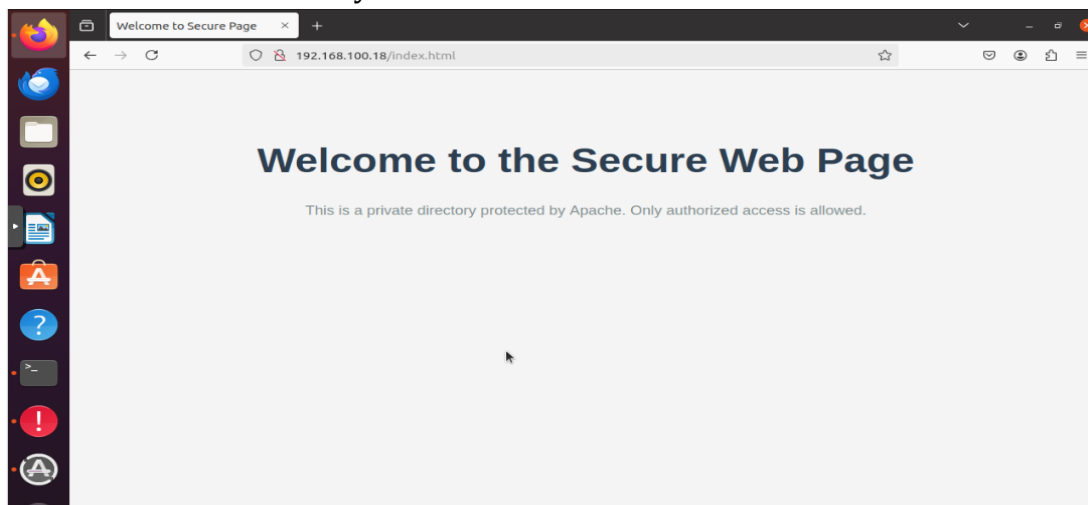
```
Order deny,allow
```



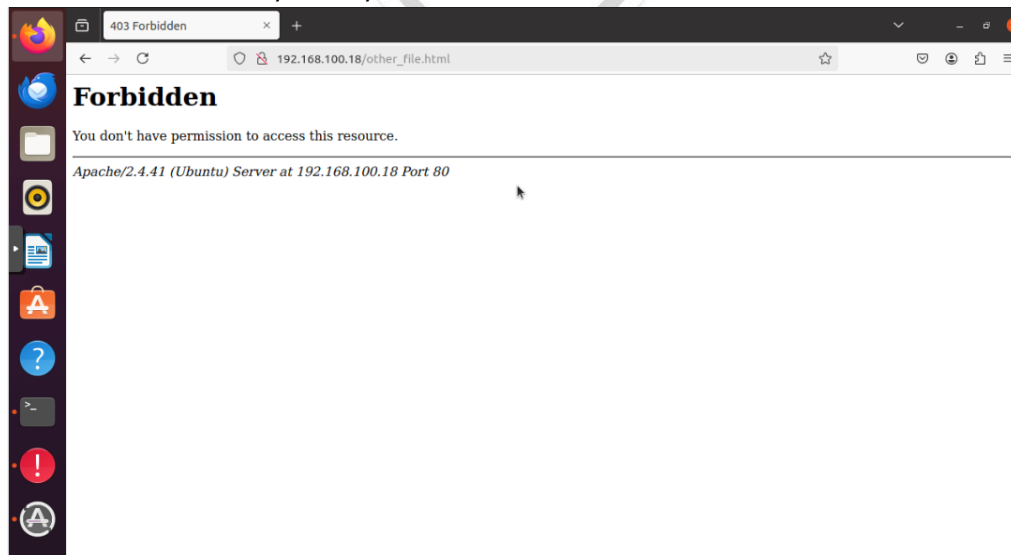
```
# Deny everyone from everything
Deny from all
<FilesMatch index\.html>
# but allow index.html
Allow from all
</FilesMatch>
</Directory>
```

- vi. Then tester tries to access the files and except index.html of var/www/secure everything should be inaccessible.

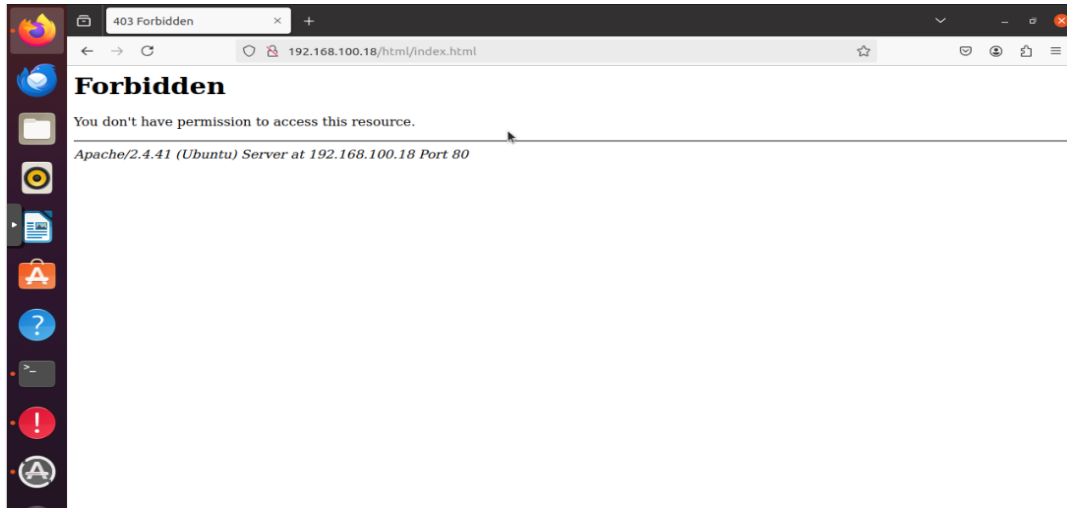
11.1.4. **Test Observations:** Hence we verified that the restrictive access rights are assigned to all files which are directly or indirectly in the web server's document directory.



- a. index.html of var/www/secure is accessible



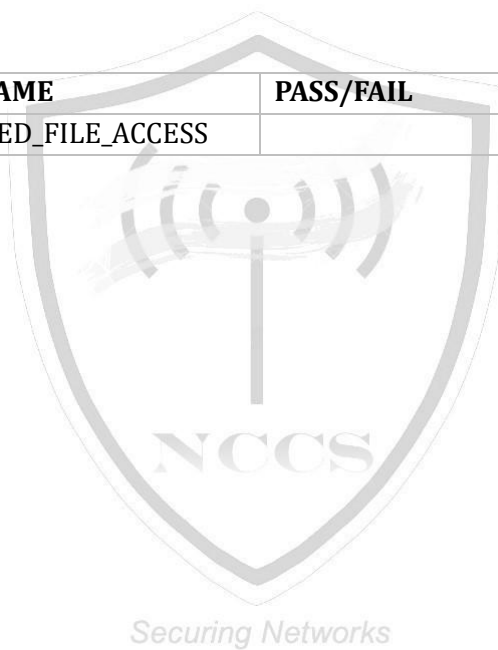
- b. other_file in var/www/secure is inaccessible



c. index.html of var/www/html also not accessible

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_RESTRICTED_FILE_ACCESS		



2.11.16 TSTP for Execute rights exclusive for CGI/Scripting directory

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.11.16
--	--------------------------	-------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 11: Web Server

2. <Security Requirement No & Name >1.11.16 Execute rights exclusive for CGI/Scripting directory

3. <Requirement Description: >If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V1.0.0. section 4.3.4.15]

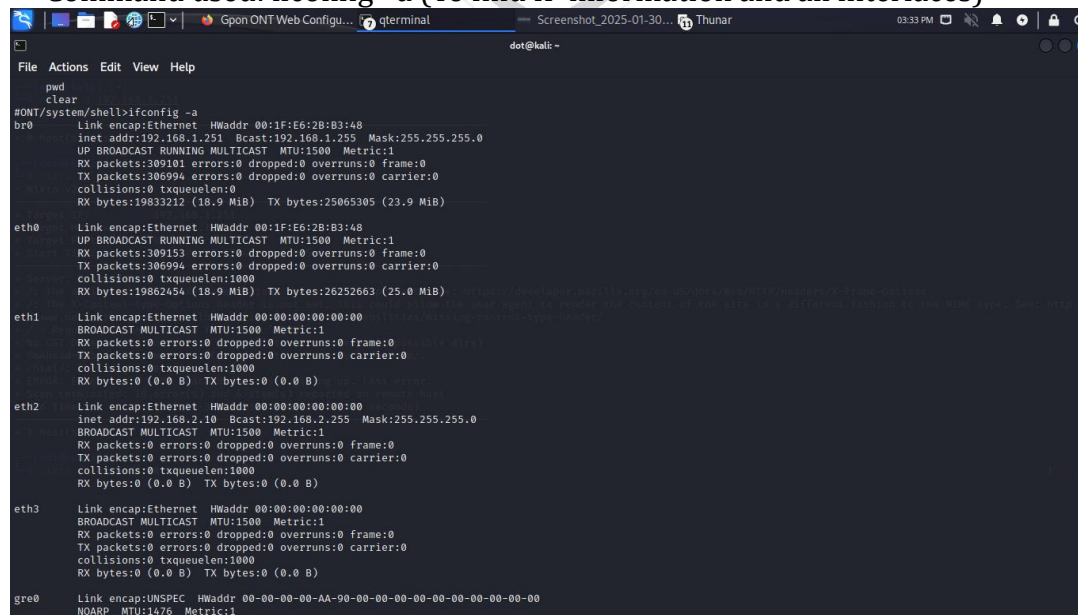
4. DUT Confirmation Details:

Use the command line interface to get details of the machine on which test is conducted.

i. Use command to get Interfaces details

ii. Use command to get Application No/Version No & Kernel Info

- Command used: `ifconfig -a` (To find IP information and all interfaces)



```
File Actions Edit View Help
pwd
clear
#ONT/system/shell>ifconfig -a
br0    Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48
       inet addr:192.168.1.251 Bcast:192.168.1.255 Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:309101 errors:0 dropped:0 overruns:0 frame:0
       TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:19833212 (18.9 MiB)  TX bytes:25065305 (23.9 MiB)

eth0    Link encap:Ethernet HWaddr 00:1F:E6:2B:B3:48
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:309153 errors:0 dropped:0 overruns:0 frame:0
       TX packets:306994 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:19862454 (18.9 MiB)  TX bytes:26252663 (25.0 MiB)

eth1    Link encap:Ethernet HWaddr 00:00:00:00:00:00
       BROADCAST MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth2    Link encap:Ethernet HWaddr 00:00:00:00:00:00
       inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.255.0
       BROADCAST MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth3    Link encap:Ethernet HWaddr 00:00:00:00:00:00
       BROADCAST MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gre0    Link encap:UNSPEC HWaddr 00-00-00-00-AA-90-00-00-00-00-00-00-00-00-00-00
       NOARP  MTU:1476  Metric:1
```

- The below screenshot shows the firmware version of the DUT

```
#ONT/system>ontver
OntSwVer : R2.0.9.6
#ONT/system>
```

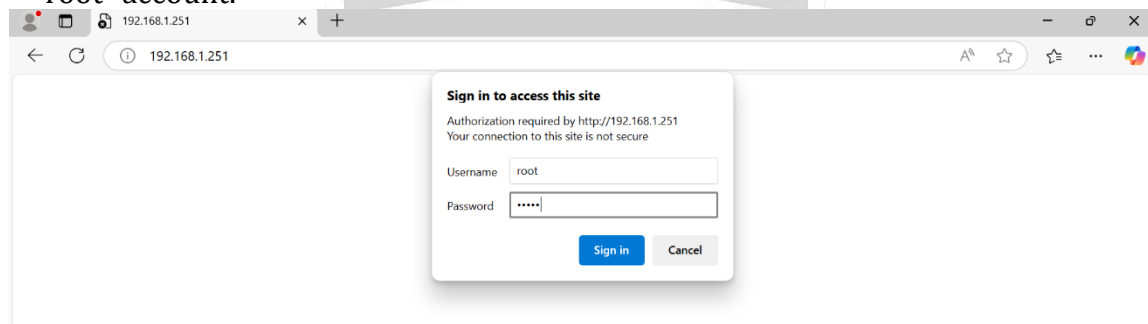
- The below screenshot shows the information of the DUT

```
#ONT/system>custom
Customer Information

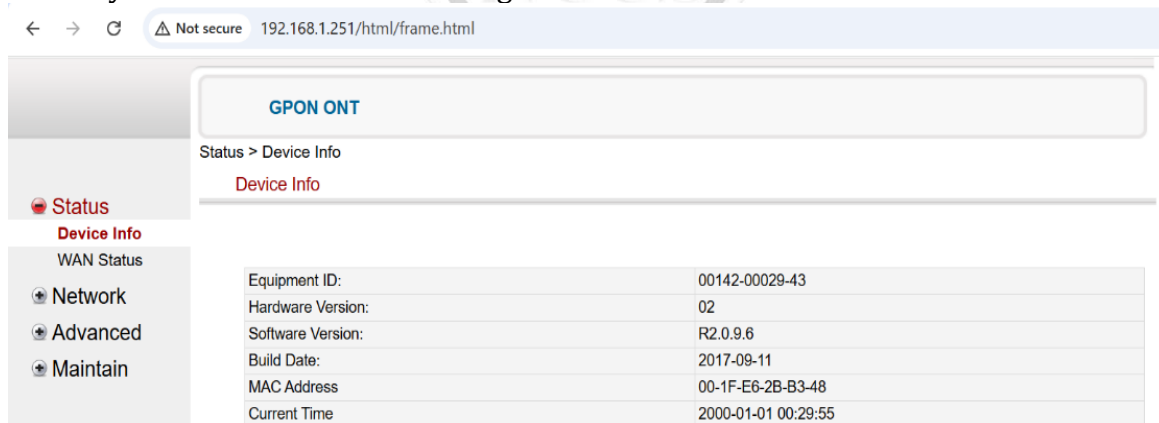
Customer Name      : UUAP
Customer Full Name : Alphion
System Config file : /etc/sys.cfg.alp
#ONT/system>
```

5. DUT Configuration

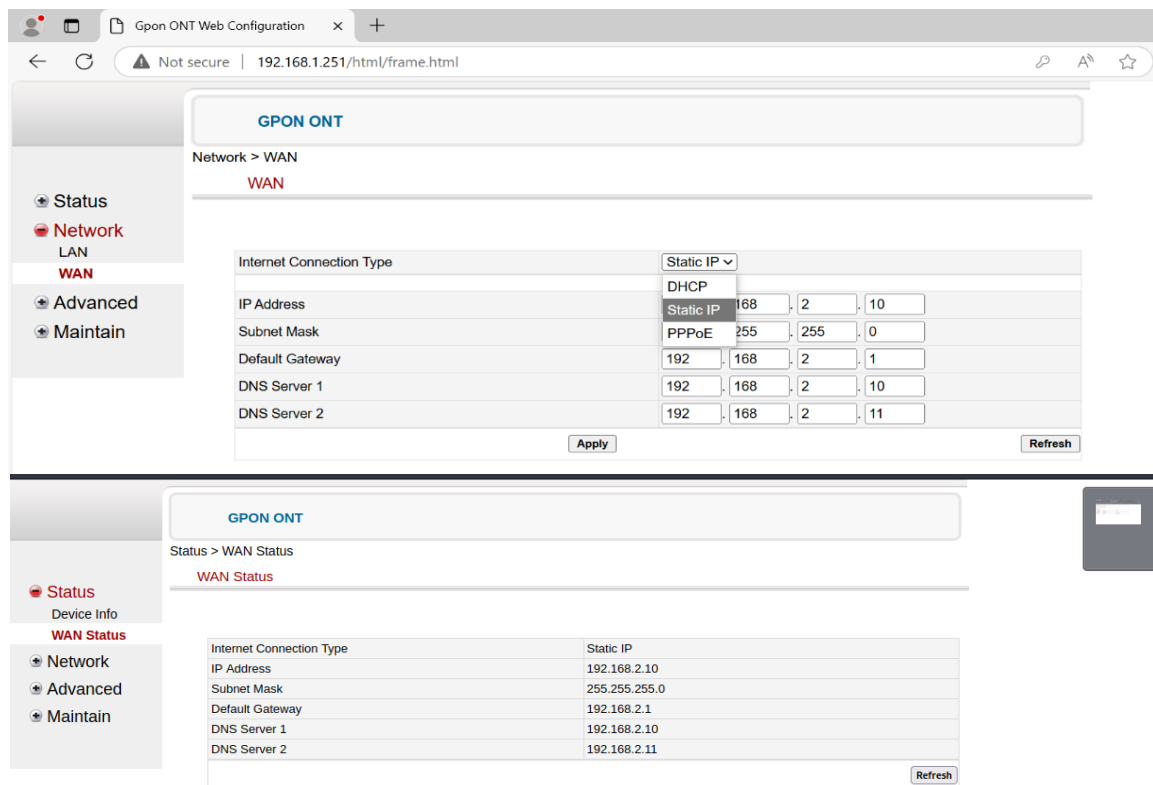
- The Tester opens GUI (webpage) of DUT (192.168.1.251) in tester machine
- The Tester attempts to open GUI using IP address of the DUT and login DUT using “root” account.



- Verify the DUT information through device info



- Set the static IP address



6. Preconditions

- The tester has administrative privileges
- A tester machine is available.
- Test environment with a Terminal.
- Test Environment with a Browser
- If the web server is configured with CGI/Scripting on, this test applies

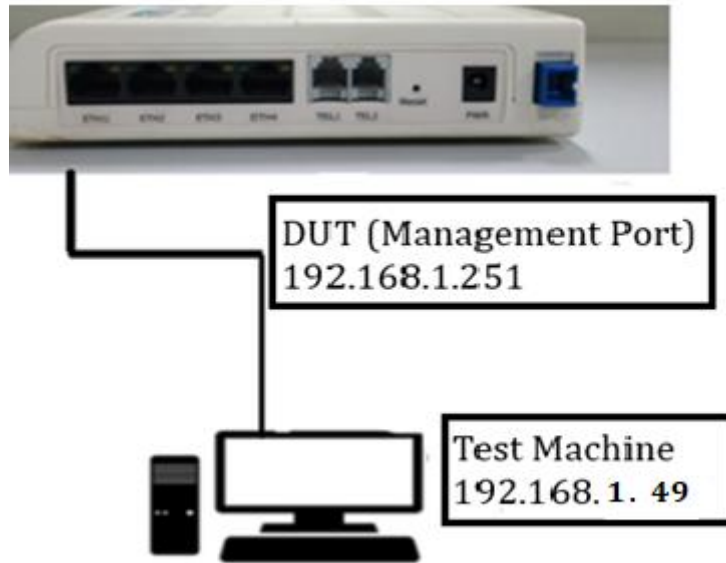
7. **Test Objective:** To test whether the web server only has execute permissions on the CGI/Scripting directory.

8. Test Plan:

8.1 Number of Test Scenarios:

8.1.1 Test Scenario for Apache: This test scenario is regarding Apache Web Server

8.2 Test Setup Diagram:



8.3 Tools Used: Default DUT configuration tool for Web Server as per vendor. It can be command line, GUI or any other interface as specified in vendor documentation.

8.4 Test Execution Steps

- i. Power up the testbed
- ii. The tester tries to access the Shell of Web Server.
- iii. Consult the web server configuration to identify all directories used for CGI or other scripting components.
- iv. The tester manually checks the permission of the CGI directory and verifies it by checking it in the browser.
- v. The tester will run some web scanning tools like Nikto, to get the detailed information and verify that the only executable CGI are working.
- vi. The tester should ensure that the static content directory does not have execute permissions to prevent it from executing scripts.
- vii. The tester should create a test CGI script in the CGI directory to verify that it executes correctly and also in the static directory to ensure it does not execute.

9. Expected Results for Pass: The web server is configured such that only the CGI/Scripting directory has execute permissions in the web server

- **NOTE:** Generally, it is insufficient to set operating system permissions file rights to avoid that the web server executes code from a particular location. If only operating system access rights are used, additional documentation, e.g. a best practice guide or OS manual, that this is sufficient should be provided.

10. Expected Format of Evidence: Log files and screenshots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_EXCLUSIVE_EXECUTE_RIGHTS_FOR_CGI

11.1.2. Test Case Description: To test whether the web server only has execute permissions on the CGI/Scripting directory.

11.1.3. Execution Steps:

- i. The tester shall open any terminal emulator to access the DUT shell and use the following command.
- a. Command used: ***ls -la <path of the CGI-BIN directory>/<available file name>***

```
amf@localhost $ ls -la test.py
-rwxr-xr-x 1 www-data www-data 245 Jun 21 11:20 test.py
```

- b. (Here we can see that owner of the file is allowed execution rights)
- c. We will open any browser and verify the following
- d. URL: ***http://<IP address of the DUT>/<CGI-BIN Directory>/<available file name>***

← → ↻ ⚠ Not secure | 172.18.0.8/cgi-enabled/test.py

CGI Script Test Page

- ii. The tester shall open any terminal emulator and use the following command.
- a. Command used: ***ls -la <path of the CGI-BIN directory>/<available file name>***

```
amf@localhost $ ls -la test.py
-rw-r--r-- 1 www-data www-data 245 Jun 21 11:20 test.py
```

- b. (Here we can see that owner of the file does not have execution rights)
- c. We will open any browser and verify the following
- d. URL: ***http://<IP address of the DUT>/<CGI-BIN Directory>/<available file name>***

← → ↻ ⚠ Not secure | 172.18.0.8/cgi-enabled/test.py

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator at webmaster@localhost to inform them of the time this error occurred, and the actions you performed just before this error.

More information about this error may be available in the server error log.

Apache/2.4.55 (Ubuntu) Server at 172.18.0.8 Port 80

- e. With proper authorization in the DUT we will access the DUT shell to view the logs

```
amf@localhost $ cat /var/log/apache2/error.log
[Wed Jun 21 11:24:27.784194 2023] [cgid:error] [pid 3150:tid 140511222773632] (13)Permission denied: AH01241: exec of '/var/www/html/cgi-enabled/test.py' failed
```

- f. (Here we can see the error permission denied when the executable bit is off)
- iii. The tester should create two directories: one for CGI scripts and one for static content. For example:
- a. CGI directory: ***/var/www/cgi-bin***
- b. Static content directory: ***/var/www/static***
- c. Command: ***\$sudo mkdir -p /var/www/cgi-bin***
- d. ***\$sudo mkdir -p /var/www/static***
- iv. The tester should set execute permissions on the CGI directory to ensure that CGI scripts can run. This can be done with: ***sudo chmod 755 /var/www/cgi-bin***

- v. The tester should ensure that the static content directory does not have execute permissions to prevent it from executing scripts. This can be done with:
sudo chmod 644 /var/www/static
- vi. The tester should configure Apache to allow CGI script execution in the CGI directory.
- vii. Ensure that the CGI module is enabled: *sudo a2enmod cgi*
- viii. Modify the Apache configuration file: *sudo vi /etc/apache2/sites-available/000-default.conf*
- ix. **Following should be in between: <VirtualHost *:80></VirtualHost *:80> tags**
Alias /cgi-bin /var/www/cgi-bin
<Directory "/var/www/cgi-bin">
Options +ExecCGI
AddHandler cgi-script .cgi
Require all granted
</Directory>
Alias /static /var/www/static
- x. **The** tester should create a test CGI script in the CGI directory to verify that it executes correctly. For example:

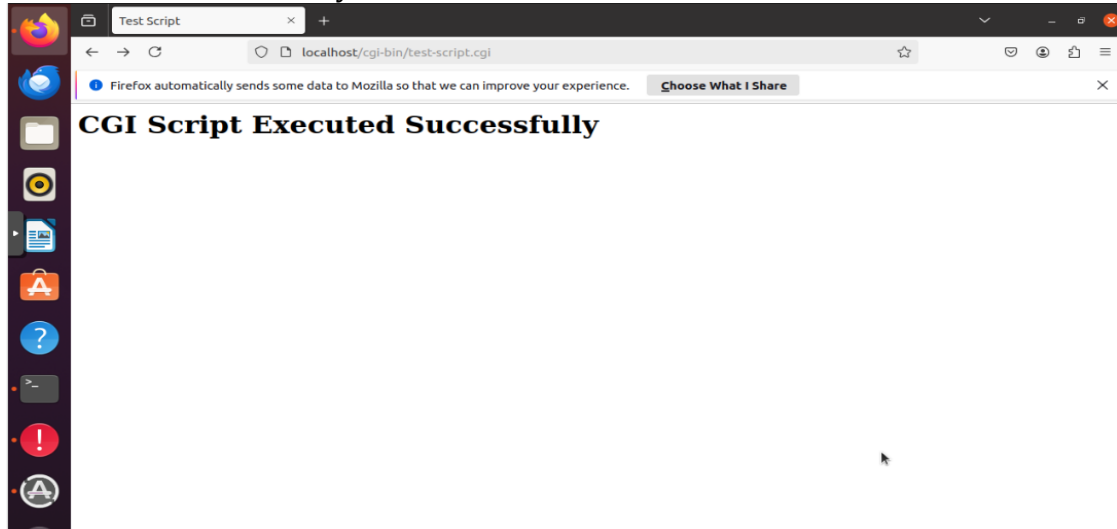
```
>sudo bash -c 'cat > /var/www/cgi-bin/test-script.cgi <<EOL
>#!/bin/bash
>echo "Content-type: text/html"
>echo ""
>echo "<html><head><title>Test Script</title></head><body>"
>echo "<h1>CGI Script Executed Successfully</h1>"
>echo "</body></html>"
>EOL'
>sudo bash -c 'cat > /var/www/static/test-script.cgi <<EOL
>#!/bin/bash
>echo "Content-type: text/html"
>echo ""
>echo "<html><head><title>Test Script</title></head><body>"
>echo "<h1>CGI Script Executed Successfully</h1>"
>echo "</body></html>"
>EOL'
```

Make both the test script executable with:
sudo chmod 755 /var/www/cgi-bin/test-script.cgi
sudo chmod 755 /var/www/static/test-script.cgi
- xi. The tester should restart Apache to apply the changes: *sudo systemctl restart apache2*
- xii. The tester should verify the setup by visiting the following URL in a web browser:
<http://localhost/cgi-bin/test-script.cgi>
<http://localhost/static/test-script.cgi>

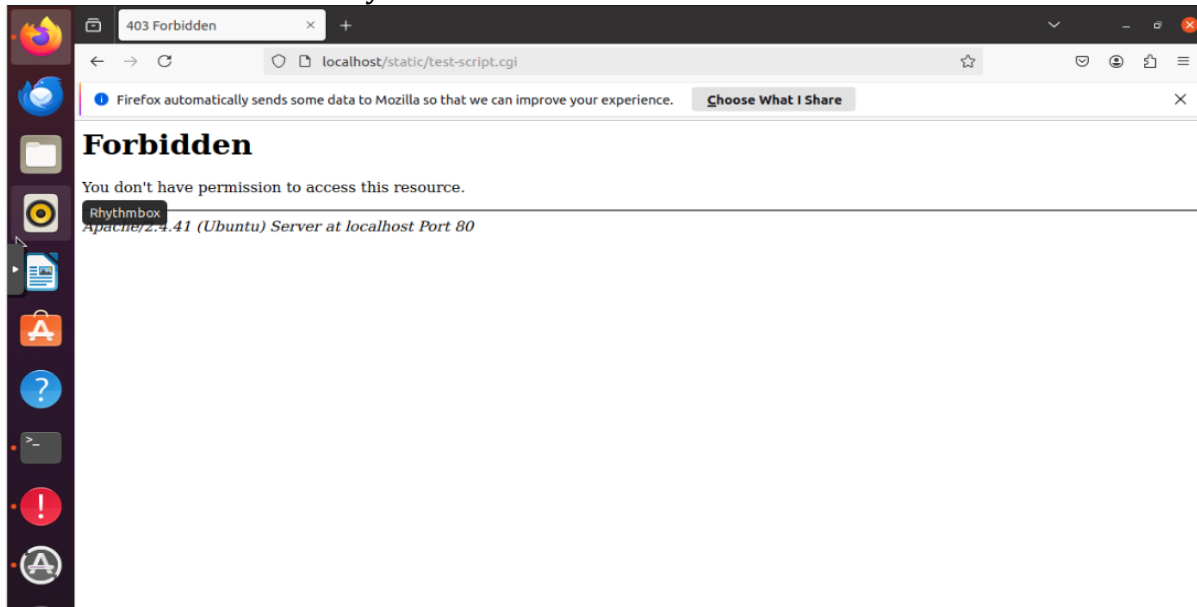
11.1.4. Test Observations:

- i. When the executable bit is on, the CGI script run with no error.
- ii. When the executable bit is set to off, the CGI script gave a 500 error.
- iii. For step 3 onwards:

iv. For CGI-BIN directory:



v. For STATIC Directory:



Securing Networks

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	TC_EXCLUSIVE_EXECUTE_RIGHTS_FOR CGI		

Section 12: Other Security requirements

2.12.1 TSTP for Evaluation of No System / Root Password Recovery

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.12.1
---	--------------------------	------------------

<DUT Details: > Syrotech SY-GPON-1110-WDONT (HGU)

<DUT Software Version:> 1.0.38-230104

<Digest Hash of OS>D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

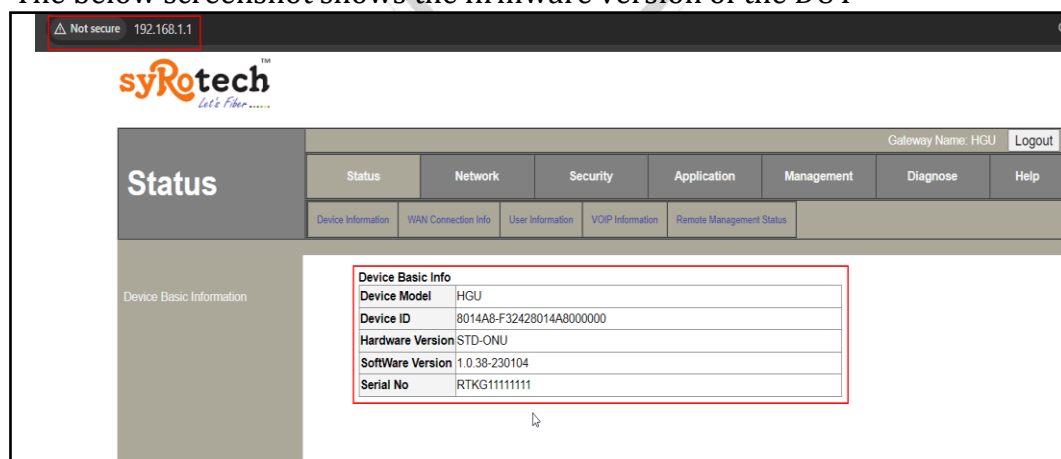
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 12: Other Security requirements
2. **<Security Requirement No & Name >** 2.12.1 No System / Root Password Recovery
3. **<Requirement Description: >** No provision shall exist for ONT/ONU System / Root password recovery. In the event of system password reset (e.g., through press of Hard-reset button), the entire configuration of the ONT/ONU shall be irretrievably deleted

4. DUT Confirmation Details:

Use the command line/GUI interface to get details of the machine on which test is conducted.

- i. Use GUI to get Application No/Version No & hardware Info
- ii. The below screenshot shows the firmware version of the DUT





Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
FXS	1 Port(s)	Physical	FXS
GUI	-	Man-Machine	Syrotech

5. DUT Configuration:

- i. The DUT (IP:192.168.1.1) is connected with Lab's Testing Machine (IP:192.168.1.2) via LAN2.

Status

Gateway Name: HGU Logout

Status

Network

Security

Application

Management

Diagnose

Help

Device Information

WAN Connection Info

User Information

VOIP Information

Remote Management Status

WLAN Interface Information

LAN Interface Information

Gateway Info:

IP Address

192.168.1.1

MAC Address

8014a8000000

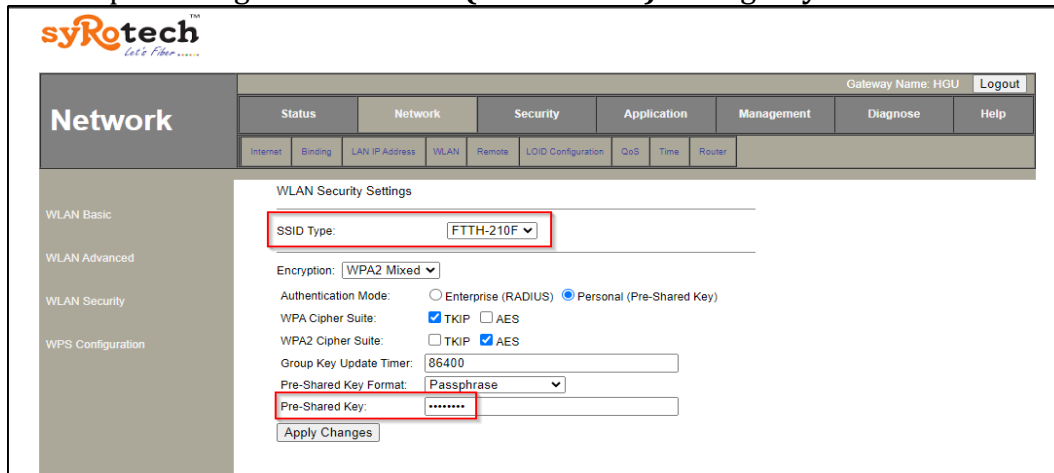
Receive/Send Info:

Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
PORT_1	43	7002	0	0	136	13196	0	0
PORT_2	1411	199188	0	0	1298	435765	0	0

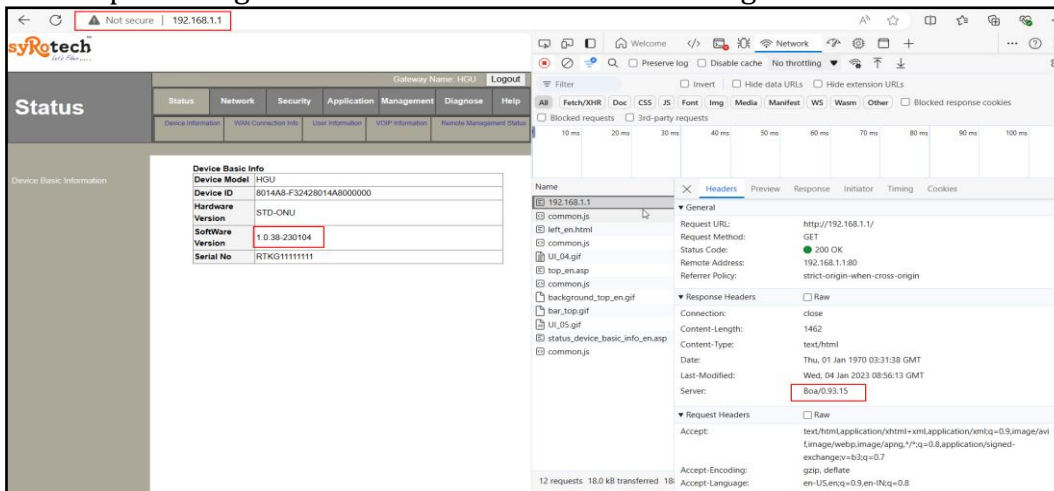
LAN Detect Status:

PORT	STATUS
LAN1	FAIL
LAN2	PASS

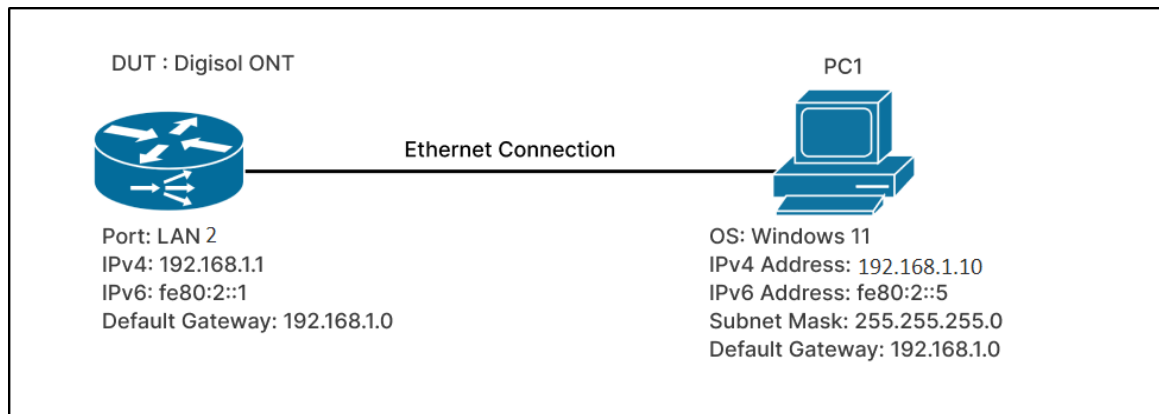
- ii. DUT is pre-configured with **SSID (FTTH-210F)** having **Key “12345678”**.



- iii. DUT is pre-configured with **Boa** as a webserver having **0.93.15** version.



6. **Precondition:** OEM documentation is required to verify the presence and functionality of password recovery options for the Device Under Test (DUT). This includes determining if password recovery is possible after a DUT reset and clarifying the specific password reset features available (if any).
7. **Test Objective:** To ensure that there is no system/root password recovery present in the DUT.
8. **Test Plan:**
- 8.1 Number of Test Case Scenarios : 2
- 8.1.1 **Test Case 01:** Verify that the DUT does not have System/Root password recovery
- 8.1.2 **Test Case 02:** Verify that the DUT does not have configured Password /Configuration after resetting DUT via CLI/GUI Mode
- 8.2 Test Setup Diagram



8.3 Tools Used:- CLI/GUI of DUT

8.4 Test Execution Steps

- a. **For TC 8.1.1:** Verify that the DUT does not have System/Root password recovery
 - i. Login to the DUT
 - ii. Save all the current DUT configuration by navigating to **Management > Device Management > Config File management** and click on **SaveCurrDef. Download to your local tester machine**
 - iii. Check the System/Root password in the DUT configuration file
- b. **For TC 8.1.2** Verify that the DUT does not have configured Password /Configuration after resetting DUT via CLI/GUI Mode
 - i. Launch the Browser and enter the DUT's IP address (e.g., 198.168.1.1). And enter the username **admin** and password **Syro@43210\$** in the login page.
 - ii. To change the current user account password refer to precondition
 - iii. To set the firewall Level high to **Low** in IPv4 refer to precondition.
 - iv. To verify WLAN Basic Configuration after reset, Set the DUT WLAN Basic Configuration refer to precondition
 - v. To verify WLAN Security Configuration after reset, Set the DUT WLAN Security Configuration refer to precondition
 - vi. To verify all Configuration after reset, Save the current DUT configuration. navigate Management > Device Management > Config File management and click on SaveCurrDef
 - vii. Reset the DUT for the default configuration check. There is no option in DUT to reset the password, so to reset the password we need to reset DUT to the factory default.
 - viii. The DUT prompts for password login, post reset. Provide old password (admin - Default password "Syro@43210\$" for DUT) and new password (Syro@123). Click on Save.
 - ix. To verify the configuration change to defaults after reset, navigate to Security > Firewall > Firewall Level
 - x. To verify the configuration change to defaults after reset, navigate to Network > WLAN > WLAN Basic
 - xi. To verify the configuration change to defaults after reset, navigate to Network > WLAN > WLAN Security

9. Expected Results for Pass:

- i. There should not be password recovery option available in the DUT
- ii. There should not be configured configuration available in the DUT after reset

13.1.22.

10. Expected Format of Evidence: - Screenshots of CLI

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

11.1.2. **Test Case Description:** Verify that the DUT does not have System/Root password recovery

11.1.3. Execution Steps:

- i. Verify that the DUT does not have System/Root password recovery
 - a. Login to the DUT
 - b. Save all the current DUT configuration by navigating to **Management > Device Management > Config File management** and click on **SaveCurrDef. Download to your local tester machine**
 - c. Check the System/Root password in the DUT configuration file

11.2 Test Case Number: 02

11.2.1. Test Case Name: 8.1.2

11.2.2. **Test Case Description:** Verify that the DUT does not have configured Password /Configuration after resetting DUT via CLI/GUI Mode

11.2.3. Execution Steps:

- i) Launch the Browser and enter the DUT's IP address (e.g., 198.168.1.1). And enter the username **admin** and password **Syro@43210\$** in the login page.

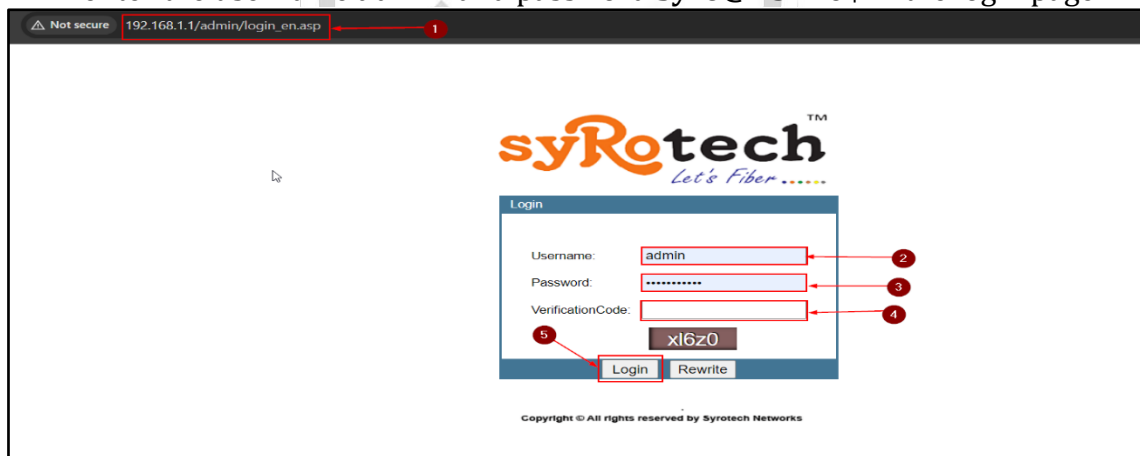
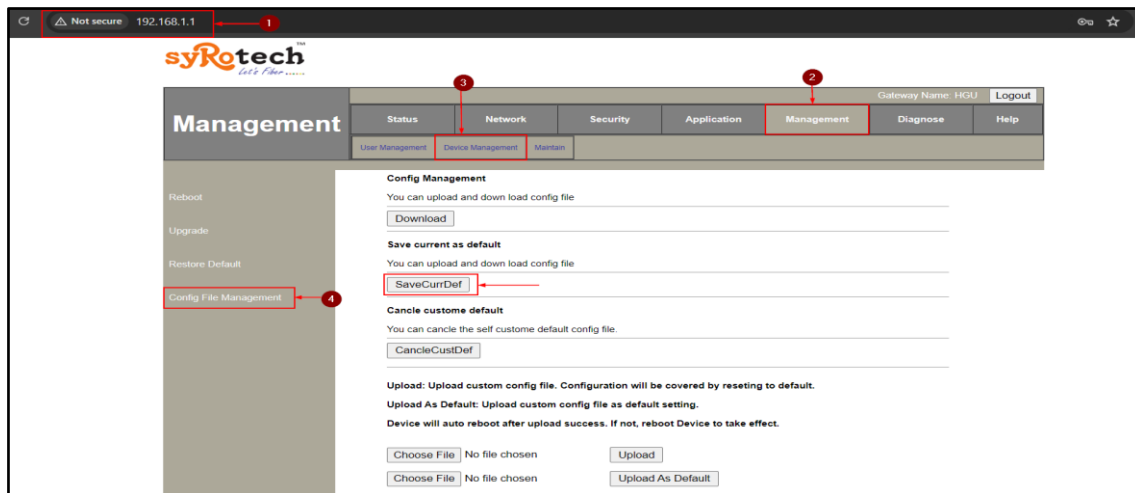


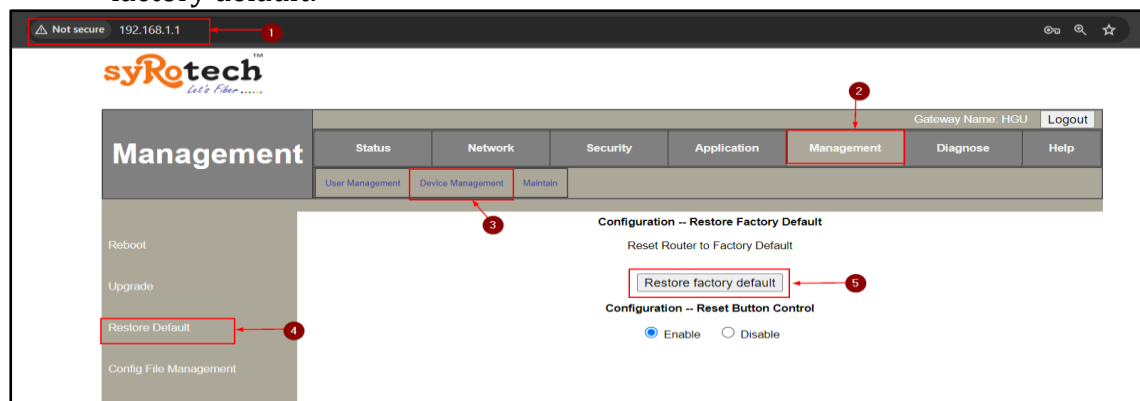
Figure: Login the DUT.

- ii) Change the current user account password, refer to precondition
- iii) Set the firewall Level from **high** to **Low** in IPv4 refer to precondition
- iv) Set the DUT WLAN Basic Configuration refer to precondition
- v) Set the DUT WLAN Security Configuration refer to precondition
- vi) Save all the current DUT configuration by navigating to **Management > Device Management > Config File management** and click on **SaveCurrDef**



Save the current DUT configuration.

- vii) Reset the DUT for the default configuration check. There is no option in DUT to reset the password, so to reset the password we need to reset DUT to the factory default.



Reset the DUT.

- viii) The DUT prompts for password login, post reset. Provide old password (**admin** - Default password "**Syro@43210\$**" for DUT) and new password (Syro@123). Click on Save.

Set password after DUT reset.

11.2.4. Test Observation:

- i. **Test Case01:** Not Tested
- ii. **Test Case02:** After factory reset, the DUT does not have any previously configured settings in the DUT. DUT requires password change after login with default user.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not Tested
2	8.1.2		Tested



2.12.2 TSTP for Evaluation of Secure System Software Revocation

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.12.2
---	--------------------------	------------------

<DUT Details: > Syrotech SY-GPON-1110-WDONT (HGU)

<DUT Software Version:> 1.0.38-230104

<Digest Hash of OS> D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 12: Other Security requirements

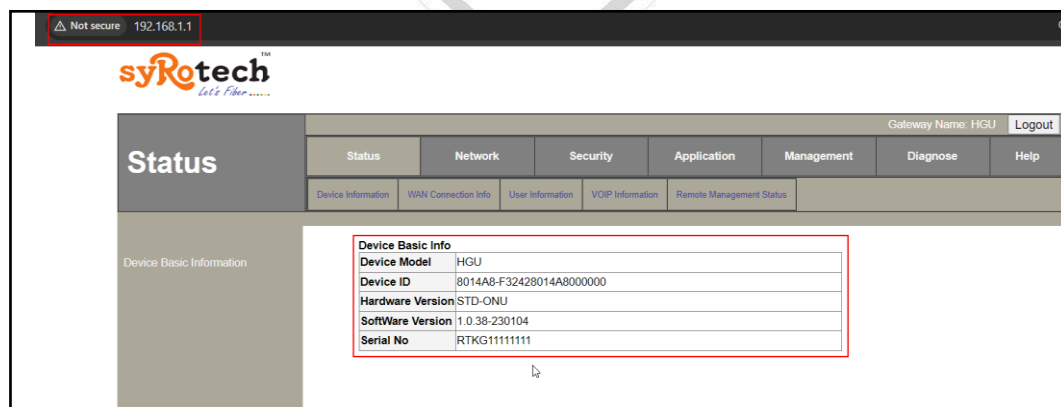
2. <Security Requirement No & Name > 2.12.2 Secure System Software Revocation

3. <Requirement Description: > Once the ONU/ONT software image is legally updated/ upgraded with New Software Image, it shall not be possible to roll back to a previous software image. In case roll back is essential, it shall be done only by the administrator with appropriate nonrepudiation controls. ONU/ONT shall support a well-established control mechanism for rolling back to previous software image

4. DUT Confirmation Details:

- Use the command line/GUI interface to get details of the machine on which test is conducted.
- Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT





Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2 Port(s)	Physical	LAN1, LAN2
FXS	1 Port(s)	Physical	FXS
GUI	-	Man-Machine	Syrotech

5. DUT Configuration:

- i. The DUT (IP:192.168.1.1) is connected with Lab's Testing Machine (IP:192.168.1.2) via LAN2.

Gateway Name: HGU Logout

Status

WLAN Interface Information

LAN Interface Information

Gateway Info:

IP Address: 192.168.1.1

MAC Address: 8014a8000000

Receive/Send Info:

Interface	Receive			Send		
	Packets	Bytes	Errors Dropped	Packets	Bytes	Errors Dropped
PORT_1	43	7002	0 0	136	13196	0 0
PORT_2	1411	199188	0 0	1298	435765	0 0

LAN Detect Status:

PORT	STATUS
LAN1	FAIL
LAN2	PASS

ii. DUT is pre-configured with **SSID (FTTH-210F)** having **Key "12345678"**.

syrotech™ Let's Fiber.....

Gateway Name: HGU Logout

Network

WLAN Basic

WLAN Advanced

WLAN Security

WPS Configuration

WLAN Security Settings

SSID Type: FTTH-210F

Encryption: WPA2 Mixed

Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

WPA Cipher Suite: ☒ TKIP ☐ AES

WPA2 Cipher Suite: ☐ TKIP ☒ AES

Group Key Update Timer: 86400

Pre-Shared Key Format: Passphrase

Pre-Shared Key: *****

Apply Changes

iii. DUT is pre-configured with **Boa** as a webserver having **0.93.15** version.

Not secure | 192.168.1.1

syrotech™ Let's Fiber.....

Gateway Name: HGU Logout

Status

Device Basic Information

Device Basic Info

Device Model: HGU

Device ID: 8014A8-F32428014A8000000

Hardware Version: STD-ONU

Software Version: 1.0.38-230104

Serial No: RTKG11111111

12 requests, 18.0 KB transferred

Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other

Blocked requests 3rd-party requests

10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 80 ms 90 ms 100 ms 110

Name X Headers Preview Response Initiator Timing Cookies

192.168.1.1

General

Request URL: http://192.168.1.1/

Request Method: GET

Status Code: 200 OK

Remote Address: 192.168.1.180

Referrer Policy: strict-origin-when-cross-origin

Response Headers

Connection: close

Content-Length: 1462

Content-Type: text/html

Date: Thu, 01 Jan 1970 03:31:38 GMT

Last-Modified: Wed, 04 Jan 2023 08:56:13 GMT

Server: Boa/0.93.15

Request Headers

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

6. Precondition: OEM documentation is needed for how to perform software revocation in the DUT. OEM should provide previous releases of DUT software.

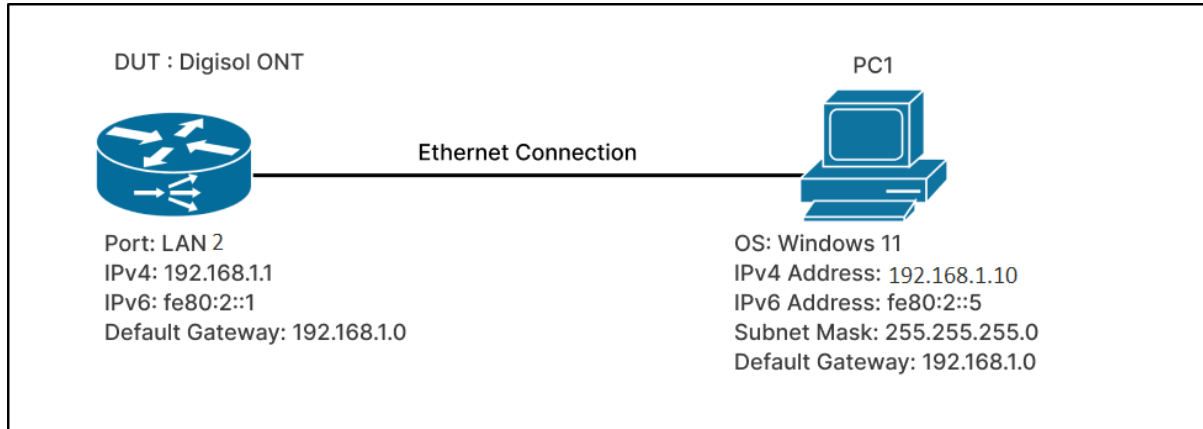
7. Test Objective: To ensure that once DUT software update/upgrade is over, it's not possible to revoke to previous version of DUT software. If software revocation possible, it should be authenticated and secure manner.

8. Test Plan:

8.1 Number of Test Case Scenarios: 1

8.1.1 Verify if it is not possible to roll back to the previous version of the exploitable software image and if possible to rollback, ensure that this action can only be performed by an admin user with secure manner.

8.2 Test Setup Diagram: <DIGISOL/Syrotech>



8.3 Tools Used:- CLI/GUI of DUT

8.4 Test Execution Steps

i. Positive Testcase:

- Log into the DUT with a high-privilege user account and navigate to the manual upgrade section. Attempt to upload the deprecated or older version of firmware.
- Ensure that the high-privilege user account can perform this action and successfully rollback to the older exploitable firmware version.

ii. Negative Testcase :

- login DUT with a low-privilege user account and navigate to the manual upgrade section in Management section. Attempt to upload the deprecated or older version of firmware.
- Verify if the low-privilege user account can perform this action.

9. **Expected Results for Pass:** If software revocation possible, it done through admin level user only with secure manner

10. Expected Format of Evidence: Screenshots of CLI/GUI

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

11.1.2. **Test Case Description:** Verify if it is not possible to roll back to the previous version of the exploitable software image and if possible, to rollback, ensure that this action can only be performed by an admin user with secure manner.

11.1.3. Execution Steps:

i. Positive Testcase:

- Log into the DUT with a high-privilege user account with username as **admin** and password as **admin123** and navigate to the manual upgrade section in Management section. Attempt to upload the deprecated or older version of firmware.

- b. To verify the High-level privilege user can perform this rollback action, navigate management > Device manage> Upgrade Image , then click on “Browse” upload The firmware file.

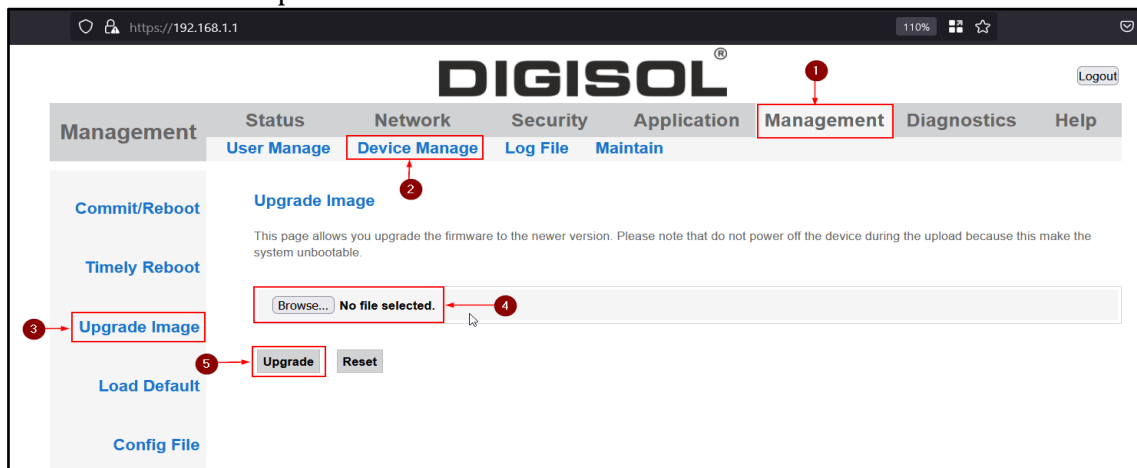
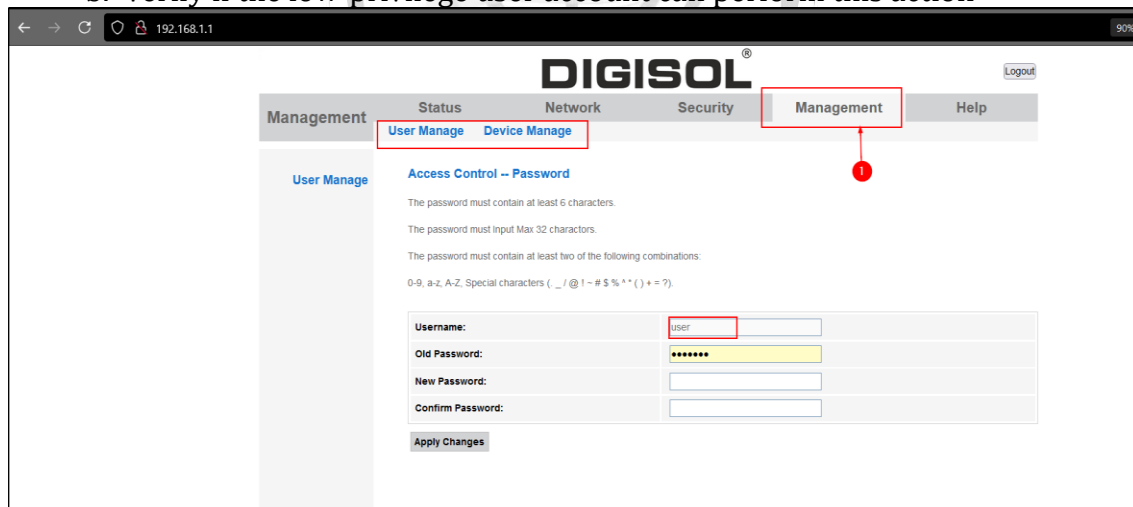


Figure: Check if low privilege user can upgrade/downgrade firmware.

ii. Negative Testcase :

- Log out DUT and login with a low-privilege user account with username as **user** and password as **user123** and navigate to the manual upgrade section in Management section. Attempt to upload the deprecated or older version of firmware.
- Verify if the low-privilege user account can perform this action



Check if low privilege user can upgrade/downgrade firmware.

11.1.4. **Test Observation:** The tester verified that the low privilege users do not have the right to upgrade/ downgrade firmware of the DUT.

12. Test Case Result:

Sl. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Tested

2.12.3 TSTP for Evaluation of Software Integrity Check – Boot

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.12.3
---	--------------------------	------------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 3: Software Security

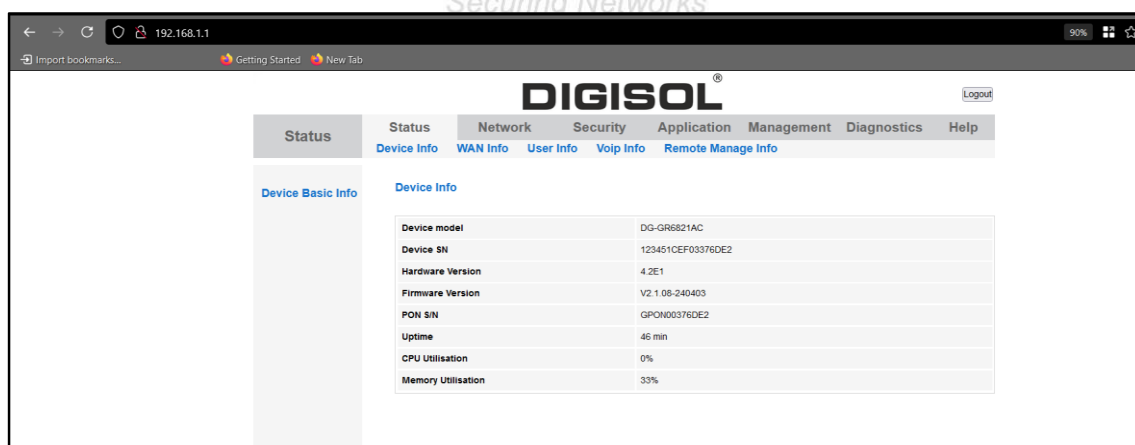
2. <Security Requirement No & Name > 2.12.3 Software Integrity Check – Boot

3. <Requirement Description: > The ONU/ONT shall verify the integrity of software component(s) at boot time by comparing the result of a standard cryptographic hash generated strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only to the expected reference value.

4. DUT Confirmation Details:

- Use the command line/GUI interface to get details of the machine on which test is conducted.
- Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT





Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

- The DUT is connected to LAN 2 – with the Lab's Testing Machine.

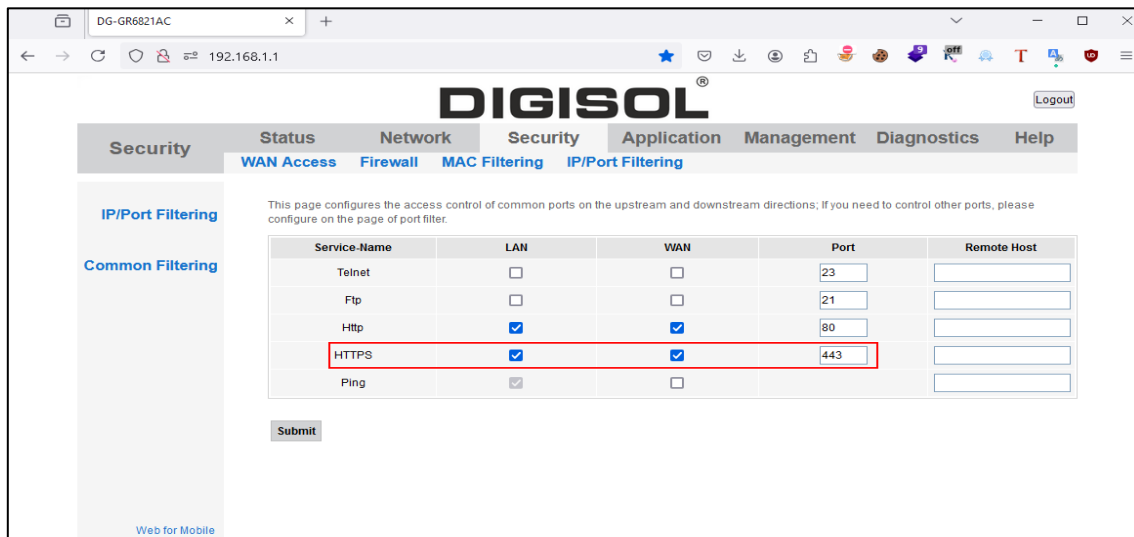
The screenshot shows the DIGISOL web management interface. The 'LAN Info' tab is selected, displaying the 'LAN Port Status' table. The table shows two ports: Port_1 (down) and Port_2 (up, 1000 M, Full duplex). The 'Send and Recv' table shows traffic statistics for both ports. The 'Active DHCP Clients' table is also visible.

Interface	State	Speed	Mode
Port_1	down	--	--
Port_2	up	1000 M	Full duplex

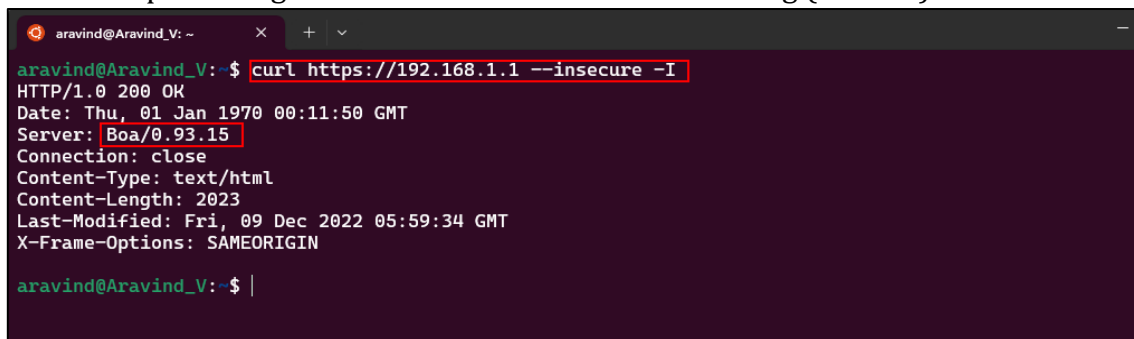
Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
Port_1	2079	467487	0	0	2204	636909	0	0
Port_2	784	171280	0	0	608	204454	0	0

Device Type	MAC Address	IP Address	Lease Time
-------------	-------------	------------	------------

ii. HTTPS is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.



iv. Configure the NTP server ip address in the ONT GUI

6. **Precondition:** OEM should provide the document related to DUT boot process.

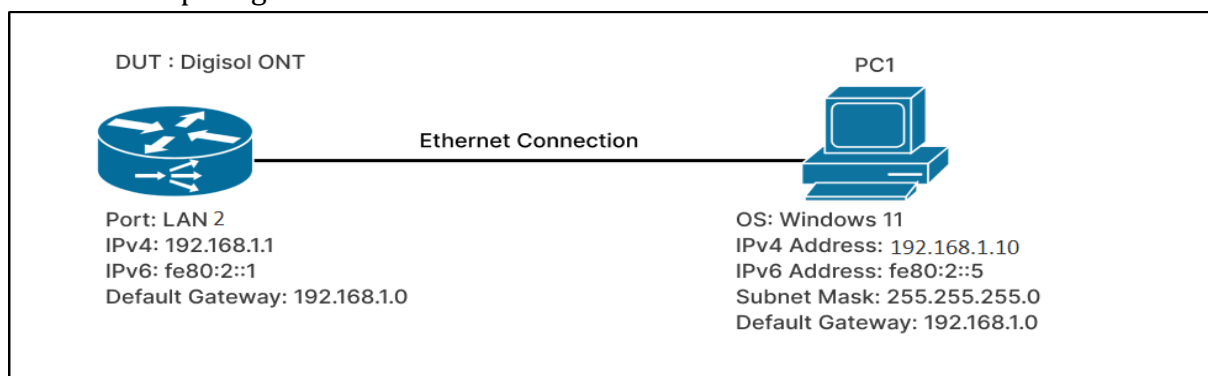
7. **Test Objective:** Verify that DUT is validate the hash of software image when booting

8. Test Plan:

8.1 Number of Test Case Scenarios: 1

8.1.1 Verify the DUT software performing a cryptographic checksum during the booting stage.

8.2 Test Setup Diagram



8.3 Tools Used: - DUT GUI/CLI (boot log),

8.4 Test Execution Steps

- a. **TC 8.1.1** Verify the DUT software performing a cryptographic checksum during the booting stage.
- To log into the web interface of the router, open a web browser and enter the default gateway address (<https://192.168.1.1>) in the address bar. Then, enter the username **admin** and password **Digisol@321** in the login dialog box.
 - To verify the current running firmware version, navigate to status > Device Basic info and find firmware version.
 - Navigate to Management > Device Manage > Commit and Reboot, and click commit and reboot, wait for the DUT to complete the reboot process.
 - After rebooting the DUT and verifying the software boot log, comparing the result of measurements such as cryptographic hashes or GRC to ensure the DUT meets the expected reference hash values.

9. Expected Results for Pass: DUT software image hash verification at booting time

10. Expected Format of Evidence: screenshot of DUT CLI/GUI

11. Test Execution:

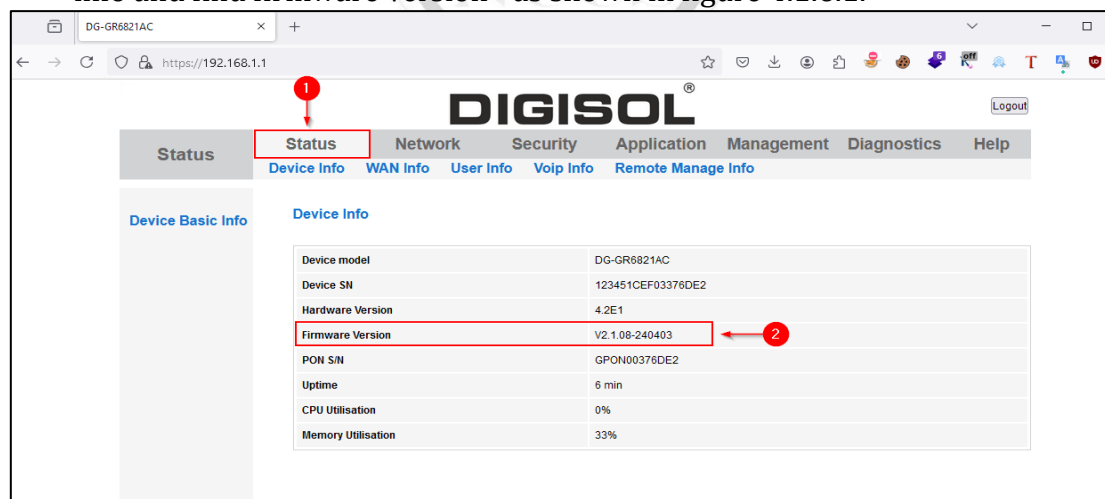
11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

11.1.2. Test Case Description: Verify the DUT software performing a cryptographic checksum during the booting stage.

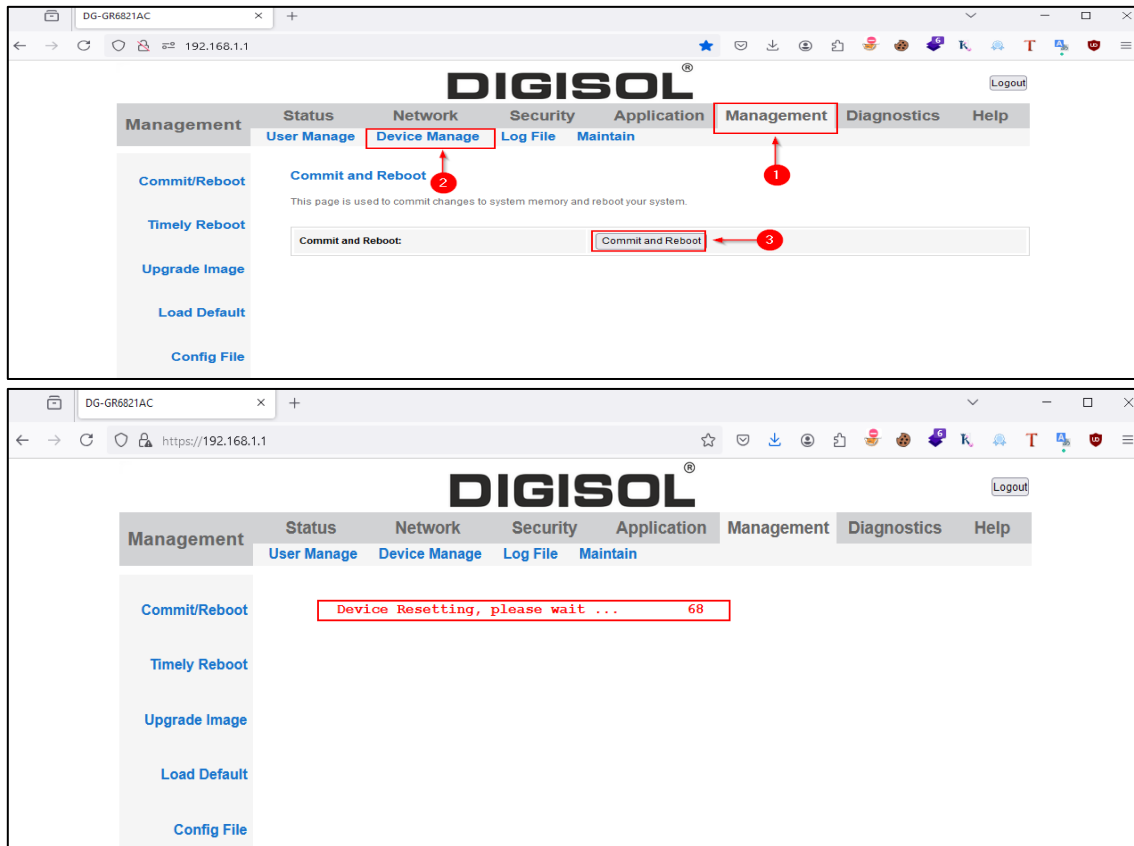
11.1.3. Execution Steps:

- To log into the web interface of the router, open a web browser and enter the default gateway address (<https://192.168.1.1>) in the address bar. Then, enter the username **admin** and password **Digisol@123** in the login dialog box.
- To verify the current running firmware version, navigate to status > Device Basic info and find firmware version - as shown in figure 4.1.6.1.



Verify the current running firmware version.

- Navigate to Management > Device Manage > Commit and Reboot, and click commit and Reboot, wait for the DUT to complete the reboot process- as shown in figure 4.1.6.2.



To verify the cryptographic checksum during booting commit and reboot the DUT.

- iv. After rebooting the DUT and verifying the software boot log, comparing the result of measurements such as cryptographic hashes or GRC to ensure the DUT meets the expected reference hash values.
- v. The below figure shows the DUT not verifying the hash of software

```

Manufacturer: DIGISOL;
ProductClass: DG-GR6821AC;
SerialNumber: ICF03-123451CEF03376DE2;
IP: 192.168.1.1;
HWVer: 4.2E1;
SWVer: V2.1.08-240403;

1970-01-01 05:49:38 [Notice] systemd: eth0 down
1970-01-01 05:49:38 [Warning] kernel: ---->rt18192cd_close
1970-01-01 05:49:38 [Warning] kernel: Error Flag: 0xffff0000
1970-01-01 05:49:38 [Notice] systemd: wlan0 down
1970-01-01 05:49:38 [Notice] systemd: wlan0 5G down
1970-01-01 05:49:38 [Warning] kernel: rt18192cd_close---->
1970-01-01 05:49:38 [Warning] kernel: TAPIDxs reboot notifier called
1970-01-01 05:49:38 [Emergency] kernel: reboot: Restarting system
1970-01-01 05:49:38 [Warning] kernel: StopHi Succeed
1970-01-01 05:49:38 [Warning] kernel: System restart.
1970-01-01 00:00:11 [Notice] systemd: br0 down
1970-01-01 00:00:11 [Notice] systemd: br0 down
1970-01-01 00:00:12 [Notice] systemd: eth0 down
1970-01-01 00:00:12 [Notice] systemd: eth0.2 down
1970-01-01 00:00:12 [Notice] systemd: eth0.3 down
1970-01-01 00:00:12 [Warning] kernel: port 0 assign to eth0.2
1970-01-01 00:00:12 [Warning] kernel: eth0.2 -> 0x1
1970-01-01 00:00:12 [Notice] systemd: eth0.3 down
1970-01-01 00:00:12 [Notice] systemd: eth0.3 down
1970-01-01 00:00:12 [Warning] kernel: port 1 assign to eth0.3
1970-01-01 00:00:12 [Warning] kernel: eth0.3 -> 0x2
1970-01-01 00:00:12 [Notice] systemd: eth0 down
1970-01-01 00:00:12 [Notice] systemd: br0 down
1970-01-01 00:00:12 [Notice] systemd: br0 down
1970-01-01 00:00:12 [Warning] kernel: re8670_open 3963
1970-01-01 00:00:12 [Notice] systemd: eth0 up
1970-01-01 00:00:12 [Notice] systemd: br0 up

```

13.1.23.

12. Test Observation: Not tested

13. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Tested

2.12.4 TSTP for Evaluation of Unused Physical and Logical Interfaces Disabling

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.12.4
---	--------------------------	------------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

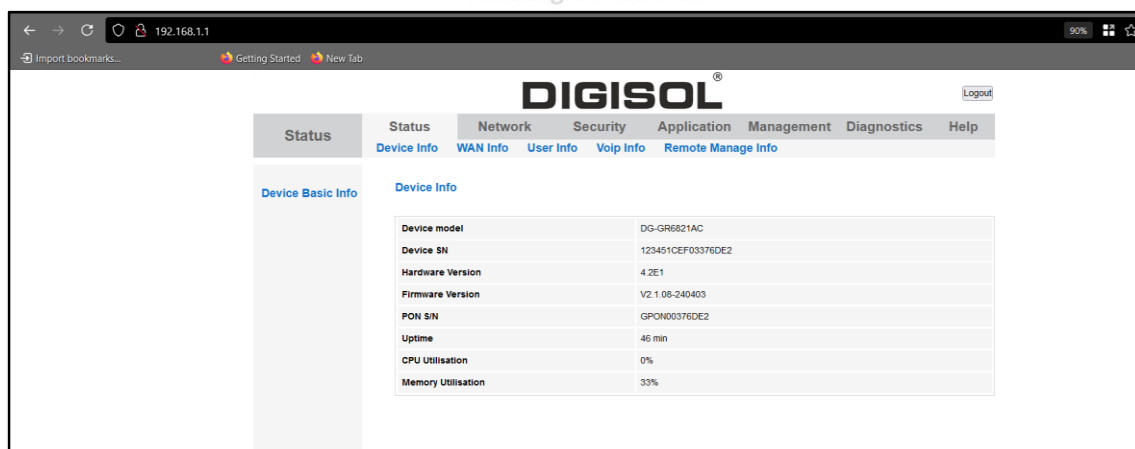
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 12: Other Security requirements
2. **<Security Requirement No & Name >** 2.12.4 Unused Physical and Logical Interfaces Disabling
3. **<Requirement Description: >** The ONU/ONT shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces (including LAN ports) which are not under use shall be disabled by configuration so that they remain inactive even in the event of a reboot.
4. **DUT Confirmation Details:**
 - i. Use the command line/GUI interface to get details of the machine on which test is conducted.
 - ii. Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT

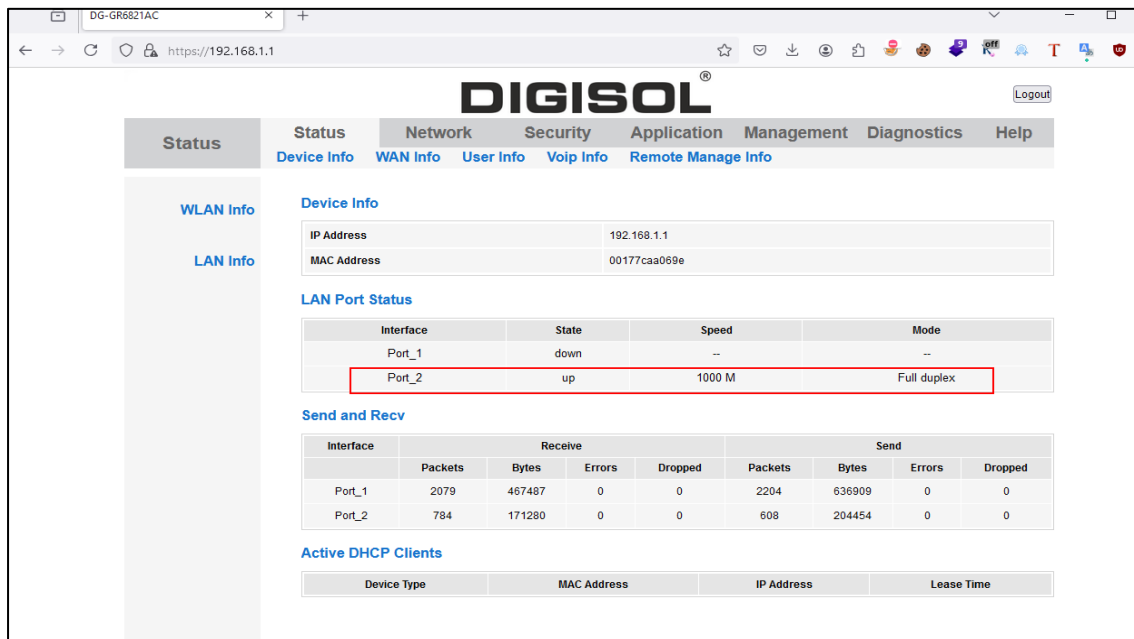




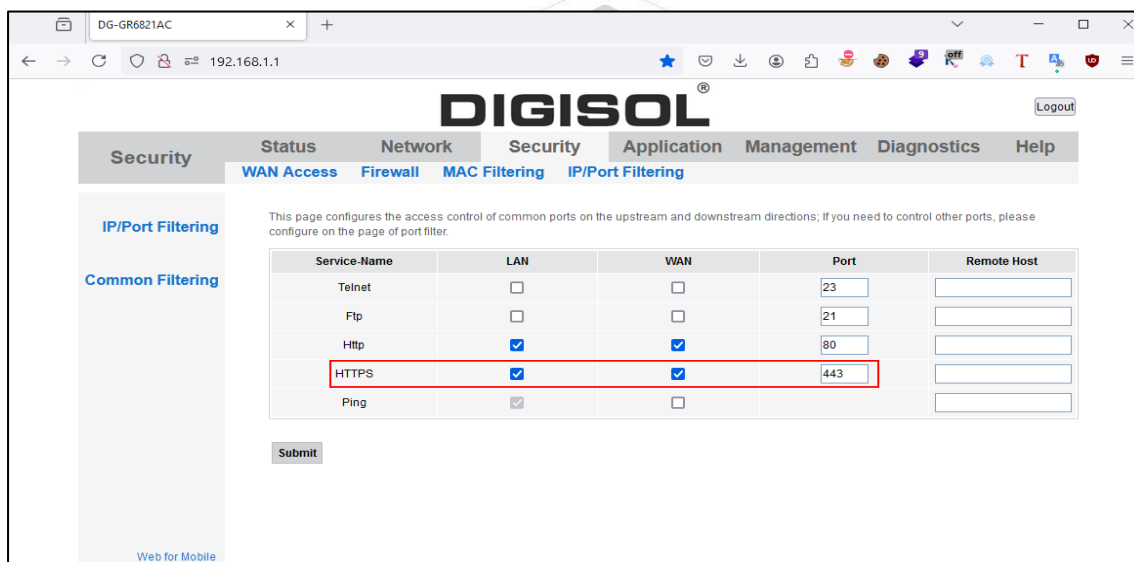
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

- The DUT is connected to LAN 2 – with the Lab's Testing Machine.



ii. HTTPS is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~
aravind@Aravind_V:~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN
aravind@Aravind_V:~$

```

6. **Precondition:** OEM document regarding disables the unused ports.

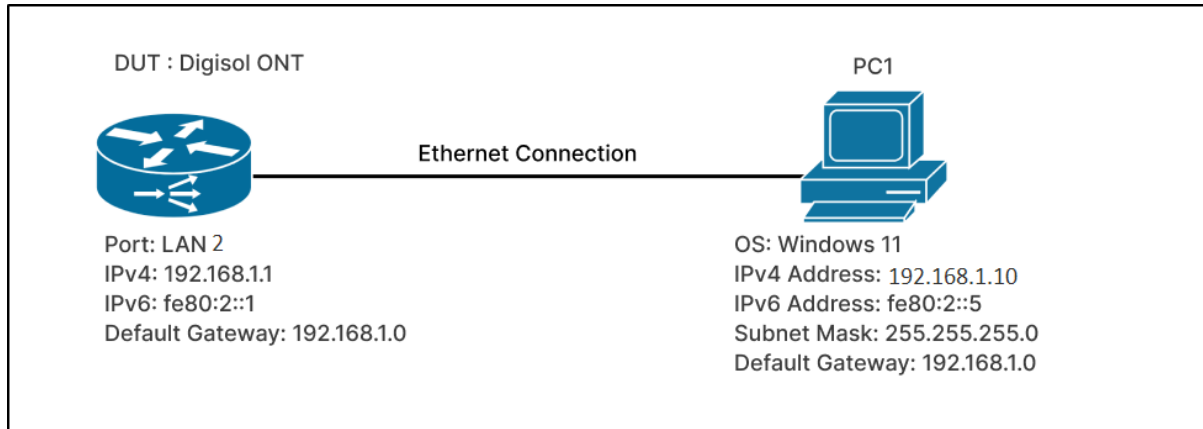
7. **Test Objective:** To verify that DUT have option to disable the unused interfaces and it even disabled after rebooting of DUT.

8. **Test Plan:**

8.1 Number of Test Case Scenarios: 1

8.1.1 Verify that the DUT have option to disable the unused interfaces

8.2 Test Setup Diagram



8.3 Tools Used:- Web browser (For access GUI of DUT)

8.4 Test Execution Steps

- a. **TC 8.1.1** Verify that the DUT have option to disable the unused interfaces
 - i. To log into the web interface of the router, open a web browser and enter the default gateway address (**192.168.1.1**) in the address bar. Then, enter the username **admin** and password **admin123** in the login dialog box.
 - ii. To verify the status of Physical ports, navigate to the Diagnostic > Self diagnostic. Start Diagnostic.
 - iii. Disable the unused interfaces in the DUT

9. **Expected Results for Pass:** Disabled interfaces should not be enabled after reboot of DUT

10. **Expected Format of Evidence:** Screenshots of GUI, log

11. Test Execution:

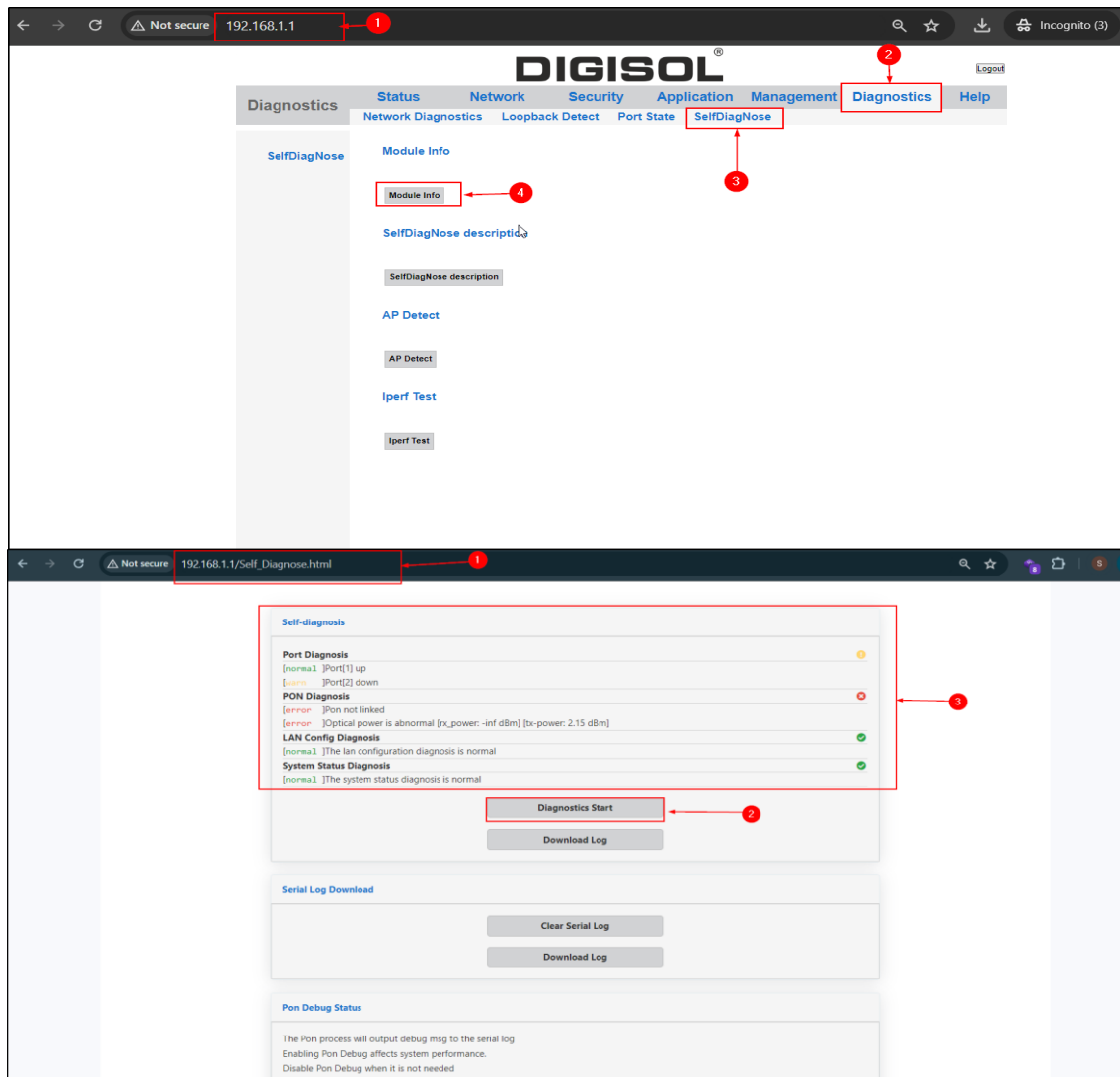
11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

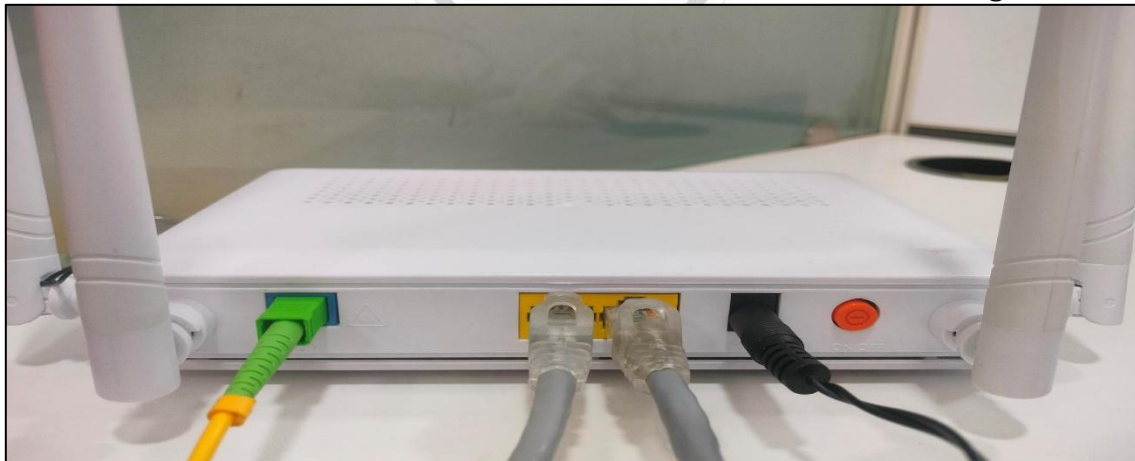
11.1.2. **Test Case Description:** To verify that DUT have option to disable the unused interfaces and it even disabled after rebooting of DUT.

11.1.3. Execution Steps:

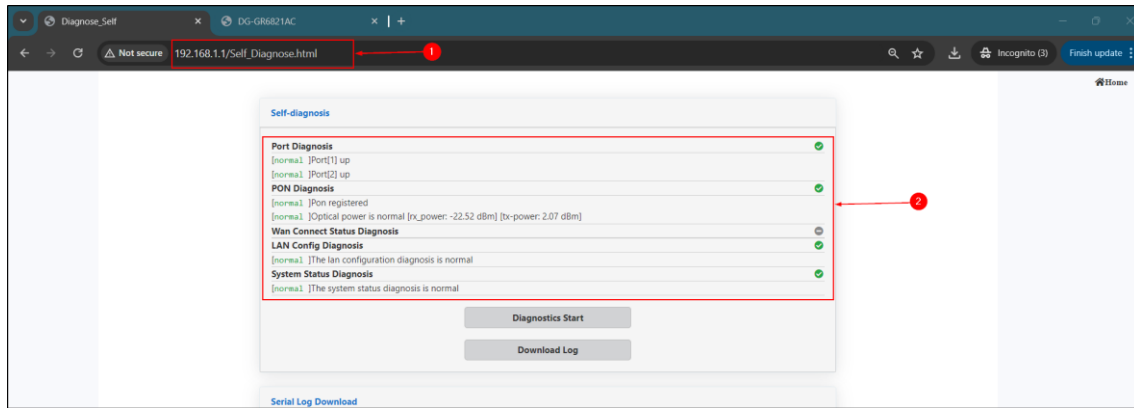
- i. To log into the web interface of the router, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **admin** and password **admin123** in the login dialog box.
- ii. To verify the status of Physical ports, navigate to the Diagnostic > Self diagnostic. Start Diagnostic – as shown in below figure



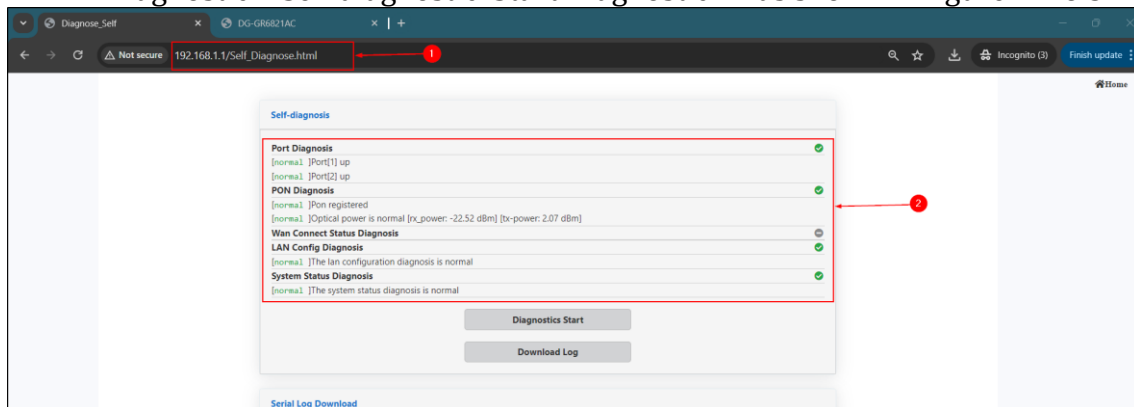
iii. Insert ethernet cable in LAN1, LAN2, PON interface – as shown in figure 4.1.6.3.



iv. To verify the status of Physical ports (after utilizing every port), navigate to the Diagnostic > Self diagnostic. Start Diagnostic – as shown in figure 4.1.6.4.



- v. Click on Reboot.
- vi. Post reboot, log into the web interface of the router, open a web browser and enter the default gateway address (**192.168.1.1**) in the address bar. Then, enter the username **admin** and password **admin123** in the login dialog box.
- vii. To verify that the status of ports remains same i.e. enabled, navigate to the Diagnostic > Self diagnostic. Start Diagnostic - - as shown in figure 4.1.6.5.



11.1.4. Test Observation:

- i. The DUT have the option to show the status of the interfaces
- ii. The DUT does not have option to configure the unused interface in the DUT

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		

2.12.5 TSTP for Evaluation of No Default Profile

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.12.5
---	--------------------------	------------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

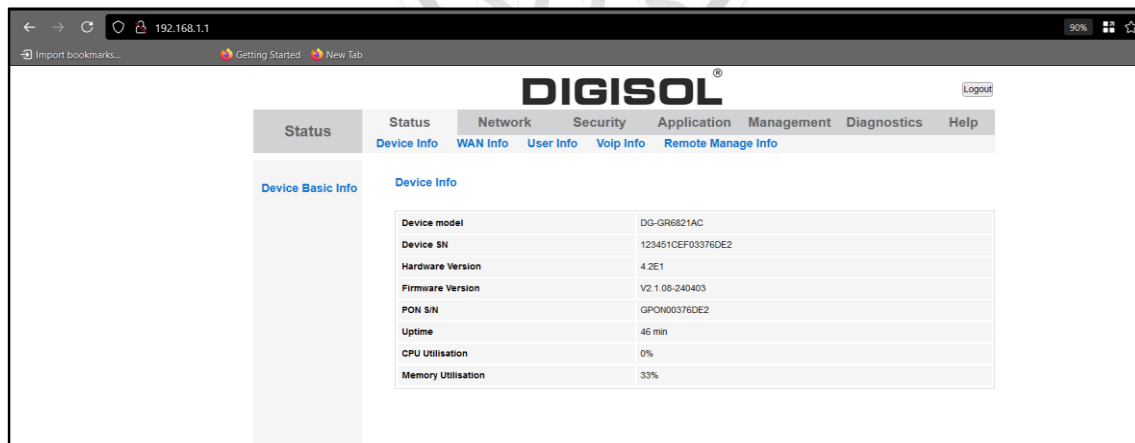
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 12: Other Security requirements
2. **<Security Requirement No & Name >** 2.12.5 No Default Profile
3. **<Requirement Description: >** No pre-defined user accounts other than Admin / Root user account would be available
4. **DUT Confirmation Details:**
 - i. Use the command line/GUI interface to get details of the machine on which test is conducted.
 - ii. Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT

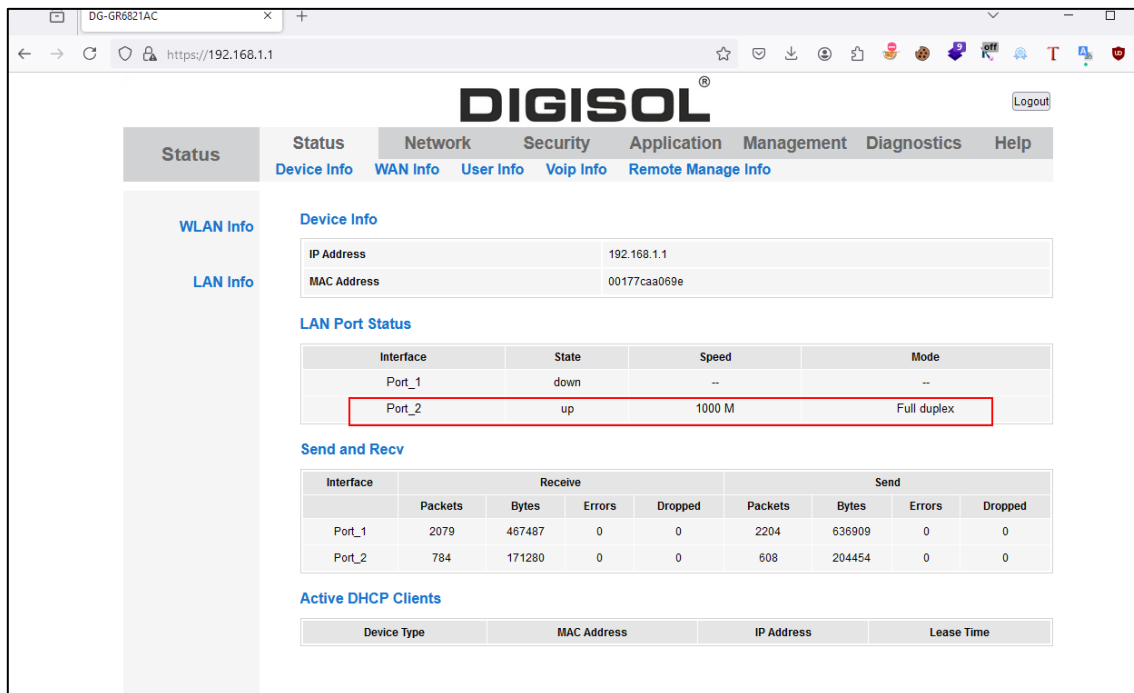




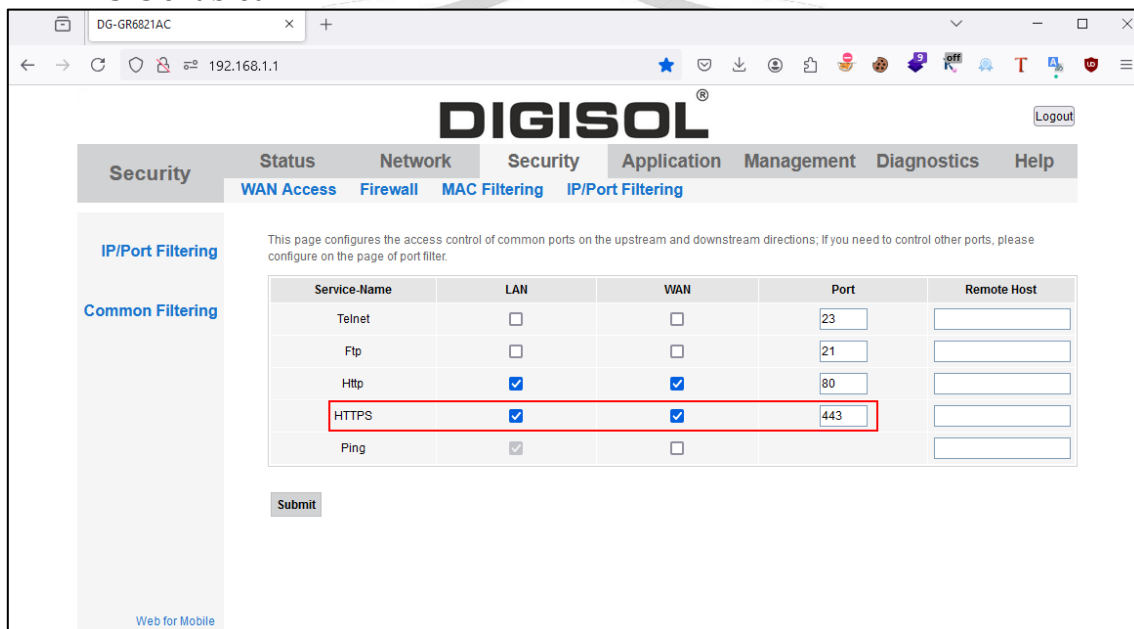
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

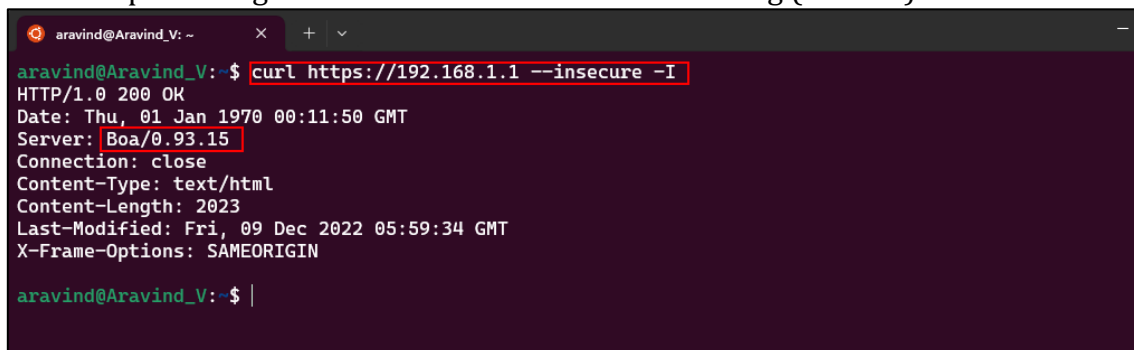
- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.



ii. HTTPS is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.



6. **Precondition:** OEM document regarding predefined accounts on the DUT.

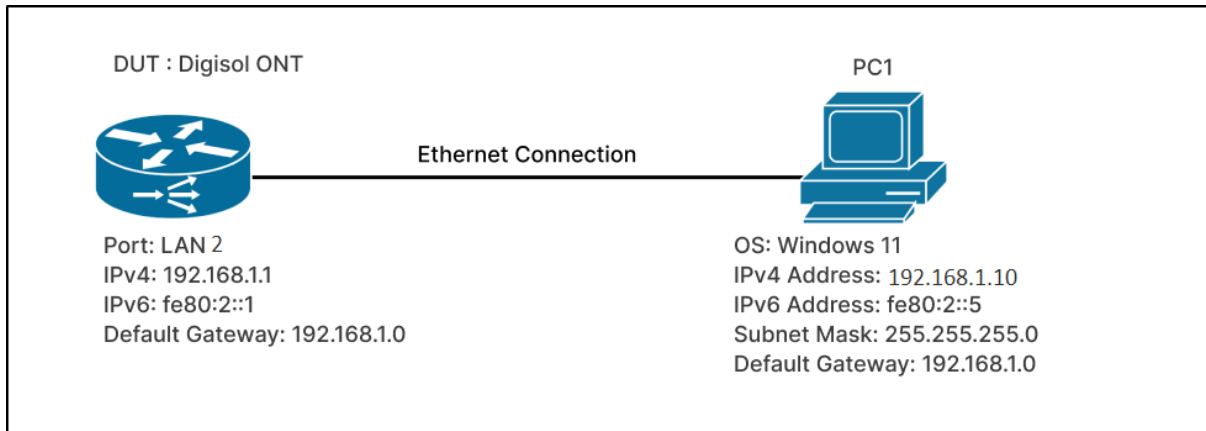
7. **Test Objective:** To verify the presence of any predefined accounts on the DUT, check both the CLI and GUI interfaces.

8. Test Plan:

8.1 Number of Test Case Scenarios : 1

8.1.1 To verify the presence of any predefined accounts on the DUT, check both the CLI and GUI interfaces.

8.2 Test Setup Diagram



8.3 Tools Used: - Web browser (For access GUI of DUT), SSH client (CLI of DUT)

8.4 Test Execution Steps

a. **TC 8.1.1** To verify the presence of any predefined accounts on the DUT, check both the CLI and GUI interfaces.

b. GUI:

- Reset the ONT by physically pressing the reset button.
- To log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **admin** and password **admin123** in the login dialog box.
- Navigate to the **Management** tab > Device manage > Config file. Obtain the DUT's configuration file by clicking the download button.
- Verify that there is presence of any predefined accounts on the DUT, open notepad and locate if any predefined account.

c. CLI:

- Reset the ONT by physically pressing the reset button.
- To log into the CLI of DUT, open putty enters IP address 192.168.1.1 in hostname field, select connection type "telnet" and click on "Open".
- Login into DUT by entering Username "**admin**" and password "**admin123**".
- Enter the following command to access DUT configuration file,
 - enterlinuxshell
 - cd /var
 - ls
 - cd /config
 - ls
- Verify that presence of any predefined accounts on the DUT, by entering following command:
 - cat lastgood.xml | grep ssh
 - cat lastgood.xml | grep ftp
 - cat lastgood.xml | grep admin
 - cat lastgood.xml | grep user

9. **Expected Results for Pass:** Default accounts should not be present in the DUT other than admin or root accounts

10. **Expected Format of Evidence:** Screenshots of GUI/CLI, log

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. Test Case Name: 8.1.1

11.1.2. **Test Case Description:** To verify the presence of any predefined accounts on the DUT, check both the CLI and GUI interfaces.

11.1.3. Execution Steps:

a. GUI:

- i. Reset the ONT by physically pressing the reset button.
- ii. To log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username **admin** and password **admin123** in the login dialog box. - as shown in figure 4.1.6.1.

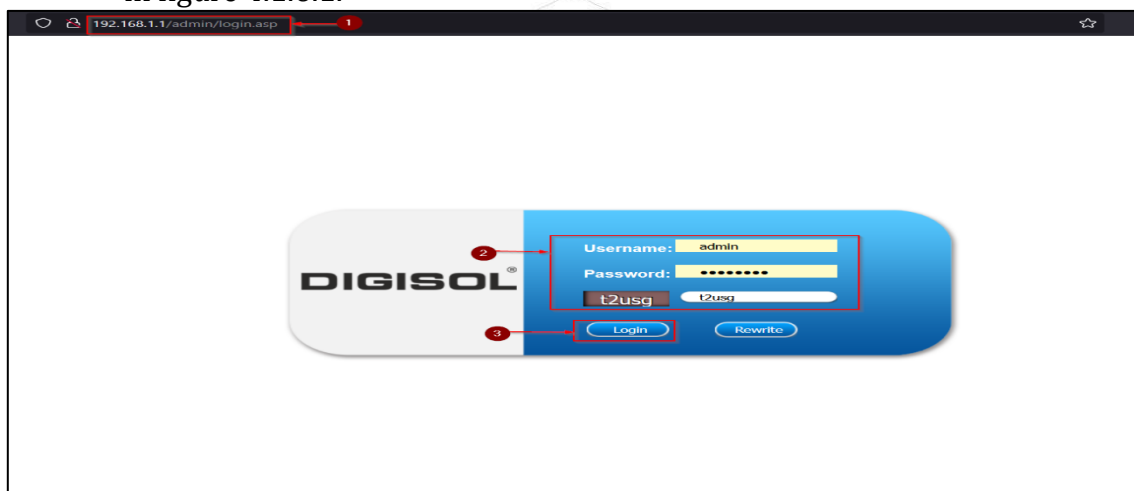


Figure 4.1.6.1: Login using default credentials.

- iii. Navigate to the Management tab > Device manage > Config file. Obtain the DUT's configuration file by clicking the download button. - as shown in figure 4.1.6.2.

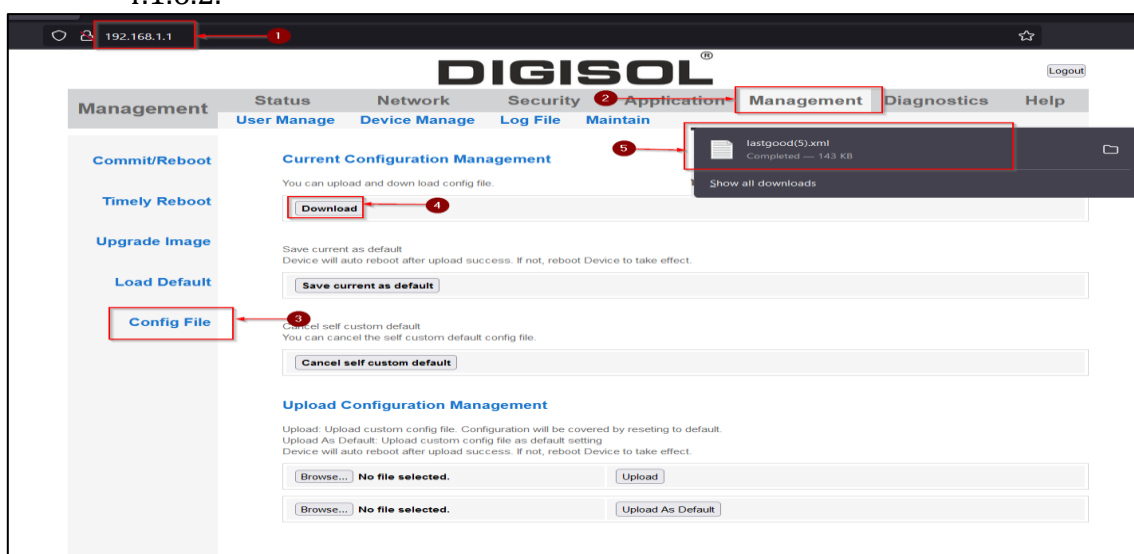


Figure 4.1.6.2: download config file

iv. Open notepad, to verify that there is presence of any predefined accounts on the DUT.

b. CLI:

- i. Reset the ONT by physically pressing the reset button.
- ii. To log into the CLI of DUT, open putty enters IP address 192.168.1.1 in hostname field, select connection type “telnet” and click on “Open”. - as shown in figure 4.1.6.3.

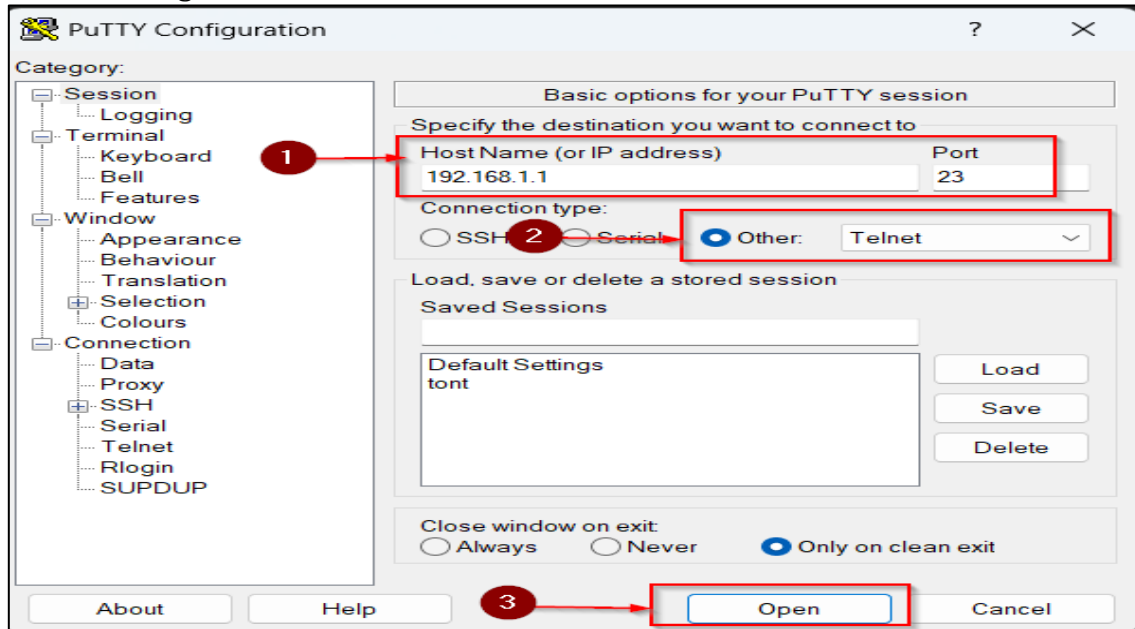


Figure 4.1.6.3: Access CLI by using Putty

- iii. Login into DUT by entering Username “admin” and password “admin123”- as shown in figure 4.1.6.4.
- iv. Enter the following command to access DUT configuration file, - as shown in figure 4.1.6.4 and figure 4.1.6.5.
 - enterlinuxshell
 - cd /var
 - ls
 - cd /config
 - ls

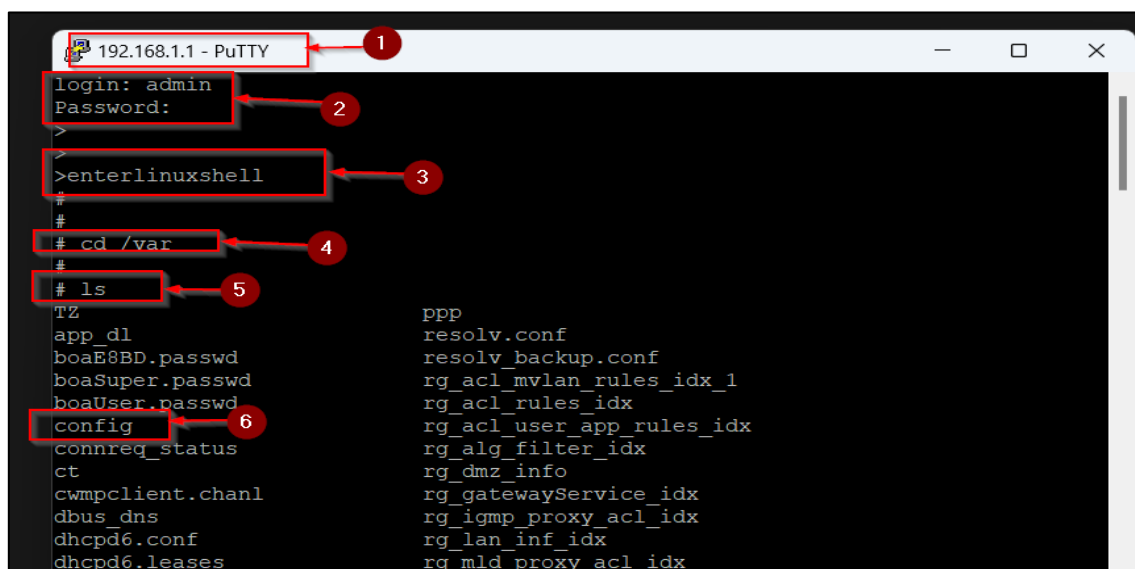


Figure 4.1.6.4: Login credentials and steps to access config file

```
#
# cd config
#
# ls
config_def_c.xml      lastgood_hs.xml_bak      rtkbosa_k.bin
lastgood.xml          lastgood_mp_hs2.xml      run_customized_sdk.sh
lastgood.xml_bak      lost+found               syslogd.txt
lastgood_hs.xml       omci_custom_opt.conf
#
```

Figure 4.1.6.5: steps to access config file

v. Verify that presence of any predefined accounts on the DUT, by entering following command:

- `cat lastgood.xml | grep ssh`
- `cat lastgood.xml | grep ftp`
- `cat lastgood.xml | grep admin`
- `cat lastgood.xml | grep user`

A. GUI:

i. Predefined user accounts other than Admin / Root user account were present in the DUT.

```
<Value Name="PROVINCE_SICHUAN_TFTP_PASSWD" Value="e8tftp"/>
<Value Name="PROVINCE_SICHUAN_TFTP_USER" Value="e8tftp"/>
<Value Name="PROVINCE_SICHUAN_SSH_PASSWD" Value="e8ssh"/>
<Value Name="PROVINCE_SICHUAN_SSH_USER" Value="e8ssh"/>
<Value Name="FTP_PASSWD" Value="e8ftp"/>
<Value Name="FTP_USER" Value="e8ftp"/>
<Value Name="TELNET_PASSWD" Value="admin123"/>
<Value Name="TELNET_USER" Value="admin"/>
<Value Name="PON_CUSTOM_SDK" Value="0"/>
<Value Name="OMCI_LOGFILE_MASK" Value="0"/>
<Value Name="OMCI_TM_OPT" Value="2"/>
<Value Name="OMCC_VER" Value="128"/>
<Value Name="OMCI_SW_VER2" Value="V3.2.02-221128"/>
<Value Name="OMCI_SW_VER1" Value="V3.2.02-221128"/>
<Value Name="OMCI_OLT_MODE" Value="0"/>
<Value Name="VLAN_MANU_TAG_PRI" Value="255"/>
<Value Name="VLAN_MANU_TAG_VID" Value="65535"/>
<Value Name="VLAN_MANU_MODE" Value="0"/>
<Value Name="VLAN_CFG_TYPE" Value="0"/>
<Value Name="RTK_IGMP_TAGDECISION" Value="0"/>
<Value Name="RTK_IGMP_VIDTYPE" Value="0"/>
<Value Name="RTK_IGMP_DROPV1" Value="1"/>
<Value Name="RTK_IGMP_DBGGEN" Value="0"/>
<Value Name="OMCI_VEIP_SLOT_ID" Value="255"/>
<Value Name="OMCI_FAKE_OK" Value="1"/>
<Value Name="OMCI_VENDOR_PRODUCT_CODE" Value="0"/>
<Value Name="OMCI_CUSTOM_ME" Value="262144"/>
<Value Name="OMCI_CUSTOM_MCAST" Value="0"/>
<Value Name="OMCI_CUSTOM_RDP" Value="0"/>
<Value Name="OMCI_CUSTOM_BDP" Value="128"/>
<Value Name="DUAL_NIGHT_MODE" Value="0"/>
```

```
<value Name="CWMP_CURRENT_USERNAME" Value="tums" />
<Value Name="CWMP_INFORM_TIME" Value="0"/>
<Value Name="CWMP_INFORM_INTERVAL" Value="43200"/>
<Value Name="CWMP_INFORM_ENABLE" Value="1"/>
<Value Name="CWMP_ACS_PASSWORD" Value="admin"/>
<Value Name="CWMP_ACS_USERNAME" Value="admin"/>
<Value Name="CWMP_ACS_URL_OLD" Value="http://devacs.edatahome.com:9090/ACS-server/ACS"/>
<Value Name="CWMP_ACS_URL" Value="http://devacs.edatahome.com:9090/ACS-server/ACS"/>
<Value Name="CWMP_PROVISIONINGCODE" Value="" />
<Value Name="DIRECT_BRIDGE_MODE" Value="1"/>
<Value Name="E8BDUSER_PASSWORD" Value="" />
<Value Name="E8BDUSER_NAME" Value="" />
<Value Name="PROVINCE_SICHUAN_FUNCTION_MASK" Value="0"/>
<Value Name="PROVINCE_SICHUAN_RESET_PASSWORD" Value="SCDX189"/>
<Value Name="SUSER_PASSWORD" Value="digisol@321#"/>
<Value Name="SUSER_NAME" Value="admin"/>
<Value Name="SYSLOG_SERVER_PORT" Value="0"/>
<Value Name="SYSLOG_SERVER_IP" Value="0.0.0.0"/>
<Value Name="SYSLOG_MODE" Value="1"/>
<Value Name="SYSLOG_DISPLAY_LEVEL" Value="5"/>
<Value Name="SYSLOG_LOG_LEVEL" Value="6"/>
<Value Name="WIFI_MAP_LOG_LEVEL" Value="0"/>
<Value Name="WIFI_MAP_DEVICE_NAME" Value="EasyMesh_Device"/>
<Value Name="WIFI_MAP_CONFIGURED_BAND" Value="0"/>
<Value Name="WIFI_MAP_CONTROLLER" Value="0"/>
<Value Name="WIFI_STA_CONTROL" Value="0"/>
<Value Name="WLAN_BANDST_STALOATHRESHOLD2G" Value="75"/>
<Value Name="WLAN_BANDST_STEERINGINTERVAL" Value="30"/>
<Value Name="WLAN_BANDST_CHANNELUSETHRD" Value="80"/>
<Value Name="WLAN_BANDST_RSSTHRDLW" Value="-80"/>
<Value Name="WLAN_BANDST_RSSTHRDHIGH" Value="-40"/>
<Value Name="WLAN_BANDST_ENABLE" Value="0"/>
<Value Name="WLAN_SITE_SURVEY_TIME" Value="0"/>
<Value Name="WLAN1_APSD_ENABLE" Value="0"/>
<Value Name="WLAN1_QoS" Value="0"/>
<Value Name="WLAN1_VAP3_ITF_GROUP" Value="0"/>
<Value Name="WLAN1_VAP2_ITF_GROUP" Value="0"/>

<Value Name="QOS_UPRATE" Value="0"/>
<Value Name="DIFFSERV_PHBCLASS" Value="0"/>
<Value Name="QOS_DIFFSERV" Value="0"/>
<Value Name="MP_MODE" Value="12"/>
<Value Name="BR_STP_ENABLED" Value="0"/>
<Value Name="BR_AGEING_TIME" Value="300"/>
<Value Name="SNMP_SYS_NAME" Value="Modem/Router"/>
<Value Name="SNMP_SYS_DESCR" Value="System Description"/>
<Value Name="INIT_SCRIPT" Value="1"/>
<Value Name="INIT_LINE" Value="1"/>
<Value Name="DEVICE_TYPE" Value="1"/>
<Value Name="USER_PASSWORD" Value="user123"/>
<Value Name="USER_NAME" Value="user"/>
<Value Name="DMZ_IP" Value="0.0.0.0"/>
<Value Name="DMZ_ENABLE" Value="0"/>
<Value Name="PORT_FW_ENABLE" Value="0"/>
<Value Name="MACF_IN_ACTION" Value="1"/>
<Value Name="MACF_OUT_ACTION" Value="1"/>
<Value Name="IPF_IN_ACTION" Value="0"/>
<Value Name="IPF_OUT_ACTION" Value="1"/>
<Value Name="RIP_VERSION" Value="1"/>
<Value Name="RIP_ENABLE" Value="1"/>
<Value Name="ADSL_OLR" Value="3"/>
<Value Name="DHCP_MODE" Value="2"/>
<Value Name="DHCP_S" Value="172.19.31.4"/>
<Value Name="DNS3" Value="0.0.0.0"/>
<Value Name="DNS2" Value="0.0.0.0"/>
<Value Name="DNS1" Value="0.0.0.0"/>
```

B. CLI:

- i. Predefined user accounts other than Admin / Root user account were present in the DUT.


```

#
# cd config
#
# ls
config_def_c.xml      lastgood_hs.xml_bak    rtkbosa_k.bin
lastgood.xml          lastgood_mp_hs2.xml    run_customized_sdk.sh
lastgood.xml_bak      lost+found             syslogd.txt
lastgood_hs.xml       omci_custom_opt.conf
#
#
# cat lastgood.xml | grep ftp
<Value Name="PROVINCE_SICHUAN_TFTP_PASSWD" Value="e8tftp"/>
<Value Name="PROVINCE_SICHUAN_TFTP_USER" Value="e8tftp"/>
<Value Name="TFTP_PASSWD" Value="e8ftp"/>
<Value Name="TFTP_USER" Value="e8ftp"/>
<Value Name="TFTP_SERVER_ADDR" Value="tftp://0.0.0.0"/>
<Value Name="tftp_specific_ip" Value=""/>
<Value Name="ftp_specific_ip" Value=""/>
<Value Name="tftp_port" Value="0"/>
<Value Name="ftp_port" Value="21"/>
<Value Name="tftp" Value="0"/>
#
#
# cat lastgood.xml | grep ssh
<Value Name="PROVINCE_SICHUAN_SSH_PASSWD" Value="e8ssh"/>
<Value Name="PROVINCE_SICHUAN_SSH_USER" Value="e8ssh"/>
<Value Name="ssh_specific_ip" Value=""/>
<Value Name="ssh_port" Value="0"/>
<Value Name="ssh" Value="0"/>
#
#
# cat lastgood.xml | grep telnet
<Value Name="telnet_specific_ip" Value=""/>
<Value Name="telnet_port" Value="23"/>
<Value Name="telnet" Value="2"/>
#
#
# cat lastgood.xml | grep telnet
<Value Name="telnet_specific_ip" Value=""/>
<Value Name="telnet_port" Value="23"/>
<Value Name="telnet" Value="2"/>
#
#
# cat lastgood.xml | grep admin
<Value Name="TELNET_PASSWD" Value="admin123"/>
<Value Name="TELNET_USER" Value="admin"/>
<Value Name="CWMP_ACS_PASSWORD" Value="admin"/>
<Value Name="CWMP_ACS_USERNAME" Value="admin"/>
<Value Name="SUSER_PASSWORD" Value="admin123"/>
<Value Name="SUSER_NAME" Value="admin"/>
<Value Name="password" Value="useradmin"/>
<Value Name="username" Value="useradmin"/>
#
#
#
# cat lastgood.xml | grep user
<Value Name="USER_PASSWORD" Value="user123"/>
<Value Name="USER_NAME" Value="user"/>
<Value Name="password" Value="useradmin"/>
<Value Name="username" Value="useradmin"/>

```

11.1.4. Test Observation:

- i. The DUT have the predefined accounts other than admin/root accounts in CLI
- ii. The DUT does not have option to configure the unused interface in the DUT

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1	FAIL	

Section 13 Specific Requirement

2.13.1 TSTL Report for Evaluation Registration with ONT

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.1
---	--------------------------	------------------

Applicant Name: **SyroTech**

Application Number: **GE-BE-1103240001**

DUT Details: **GPON-ONT**

TSTL Document ID: **GE-BE-1103240001 v001**

DUT Make: **SyroTech**

DUT Model no: **SY-GPON-2010-WADONT**

DUT Serial Number: **5447E8-123455447E8541A97**

DUT Software Version: **V 3.2.02-231205**

Applicable ITSAR: **ONT ITSAR403012311**

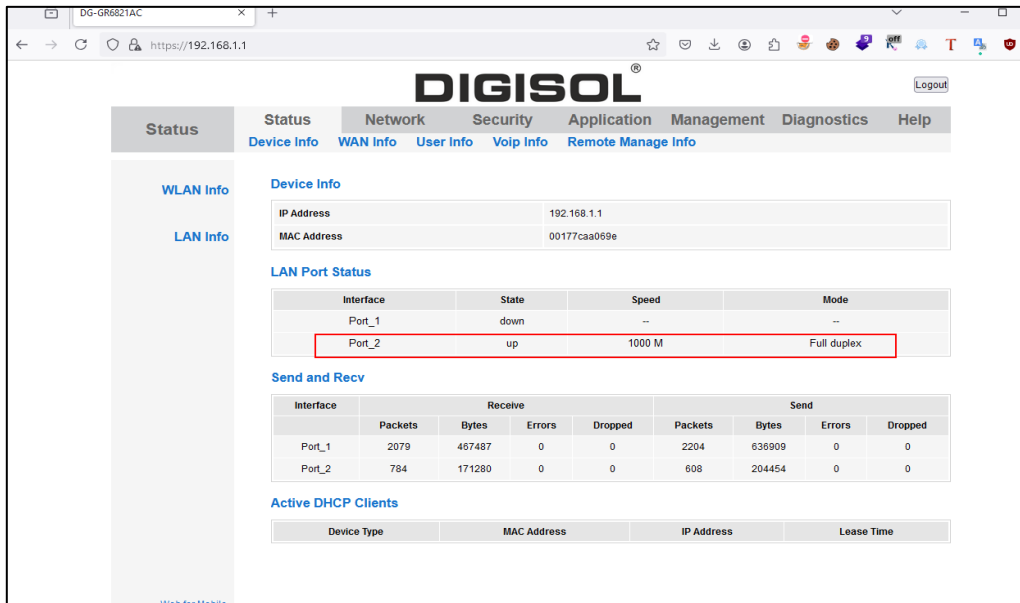
Version No: **1.0.1**

OEM Supplied Document list: **NA**

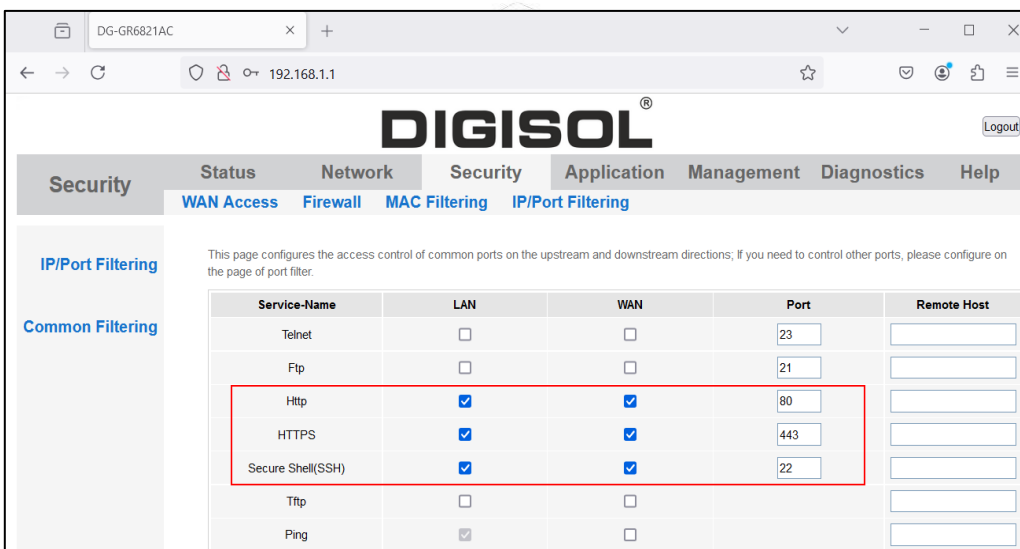
1. **<ITSAR Section No & Name>** Section13: Specific Requirement
2. **<Security Requirement No & Name >** 2.13.1 Registration with ONT
3. **Requirement Description:** The ONT must support transmitting serial No, registration ID, logical ONU ID, credentials for mutual authenticating with OLT
OLT should support this mutual authentication
 - i. Pre-shared secret A compliant G-PON system shall support a pre-shared secret key (PSK) that is associated with a particular ONU and is stored at that ONU and in the operator infrastructure. On the operator side, the pre-shared secret for a particular ONU might be stored in the physically connected OLT, or at a central server that the OLT accesses during authentication. The PSK is a 128-bit value. It may be provisioned into the ONU and into the operator infrastructure in any manner that satisfies these requirements.
 - ii. Master session key OLT and ONU may execute a mutual authentication procedure, in the course of which both the OLT and the ONU compute the 128-bit master session key (MSK), a session-specific shared secret. Whenever the ONU is successfully authenticated MSK is used to encrypt data encryption keys that are transmitted upstream. For the duration of the execution of the secure mutual authentication procedure, the OLT refrains from initiating data encryption key exchanges. OLT and ONT mutually authenticate based on pre-shared key or master session key.

[Reference Annex B Enhanced security capabilities 9.13.11 of ITU-T G.988]

4. DUT Confirmation Details:



ii. HTTPS and SSH is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~
aravind@Aravind_V:~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN
aravind@Aravind_V:~$

```

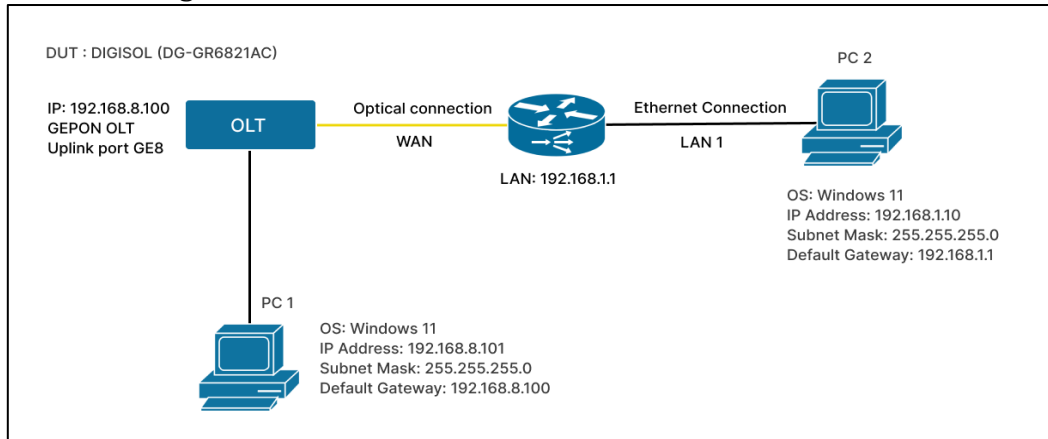
6. **Pre-Condition:** OEM shall documentation stating the supported access methods into DUT

7. **Test Objective:** To verify that minimum two of the above authentication attributes shall be mandatorily combined for protecting all the accounts from misuse and for local access and machine accounts, at least one authentication attribute shall be supported

8. Test Plan

8.1 Test Cases: To verify ONT must support transmitting its serial number, registration ID, logical ONU ID, and credentials for mutual authentication with the OLT, which should support both pre-shared keys (PSK) and master session keys (MSK) for secure mutual authentication.

8.2 Test Bed Diagram



8.3 Tools Required

9. Expected Results for Pass

- To capture the traffic (data encryption) between ONT and OLT, enable the OMCI logs
- To log into the web interface of the OLT, open a web browser and enter the default gateway address (192.168.8.100) in the address bar. Then, enter the username admin and password Xpon@Olt9417# in the login dialog box.
- Physically connect the ONT to the OLT over PON port.
- To enforce authentication between OLT and ONU for registration, log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username admin and password admin123 in the login dialog box.
- Navigate to Network > LOID register, to create a new LOID, provide the LOID name as Deltaphi and password as admin123.
- To add a LOID in the OLT, navigate to Authentication > LOID List, ONU LOID select for PON1 as add LOID username Deltaphi and password admin123 and submit
- To verify if the registration of the ONU is done with the ONT (post enforcing authentication) and check the connection status in the OLT, navigate to ONU configuration > ONU list > set Port ID as PON1 > Refresh.
- Verify that the ONU sends its serial number, registration ID, and logical ONU ID with credentials to the OLT, and that the DUT supports mutual authentication with a pre-shared key and encryption using the master session key.

10. Expected format of evidence

11. Test Execution

11.1 Test Case Number: 1

- 11.1.1. **Test case Name:** To verify ONT must support transmitting its serial number, registration ID, logical ONU ID, and credentials for mutual authentication with the OLT, which should support both pre-shared keys (PSK) and master session keys (MSK) for secure mutual authentication.

11.1.2. **Test Case Description:** To verify ONT must support transmitting its serial number, registration ID, logical ONU ID, and credentials for mutual authentication with the OLT, which should support both pre-shared keys (PSK) and master session keys (MSK) for secure mutual authentication.

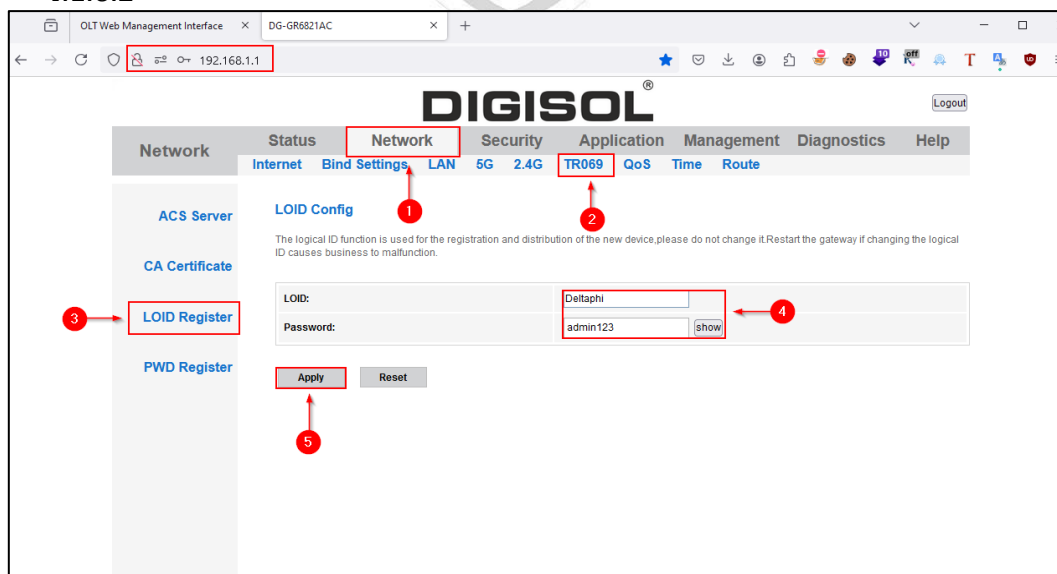
11.1.3. **Tool Used:** Manual

11.1.4. **Execution Steps:**

- i. To capture the traffic (data encryption) between ONT and OLT, enable the OMCI logs. Refer precondition.
- ii. To log into the web interface of the OLT, open a web browser and enter the default gateway address (**192.168.8.100**) in the address bar. Then, enter the username **admin** and password **Xpon@Olt9417#** in the login dialog box.
- iii. Physically connect the ONT to the OLT over PON1 port-



- iv. To enforce authentication between OLT and ONU for registration, log into the web interface of the ONT, open a web browser and enter the default gateway address (**192.168.1.1**) in the address bar. Then, enter the username **admin** and password **admin123** in the login dialog box.
- v. Navigate to Network > LOID register, to create a new LOID, provide the LOID name as Deltaphi and password as admin123, apply changes- as shown in figure 4.1.6.2



- vi. To add a LOID in the OLT, navigate to Authentication > LOID List, ONU LOID select for **PON1** as add LOID username **Deltaphi** and password **admin123** and submit -as shown in figure 4.1.6.3

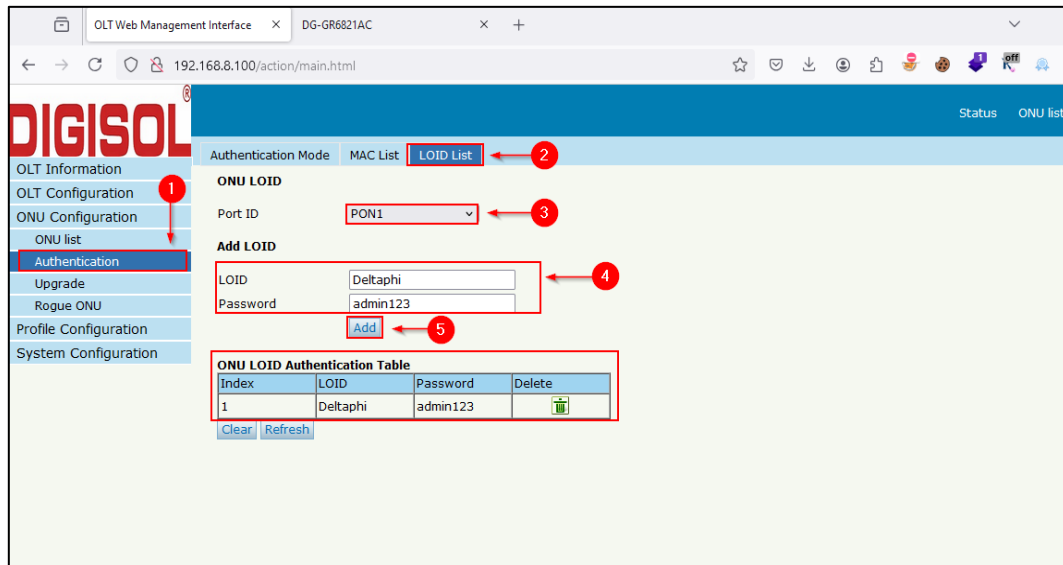


Figure no. 4.1.6.3: Configuring the LOID in the OLT

- vii. To verify if the registration of the ONU is done with the OLT (post enforcing authentication) and check the connection status in the OLT, navigate to ONU configuration > ONU list > set Port ID as PON1 > Refresh – as shown in figure 4.1.6.4

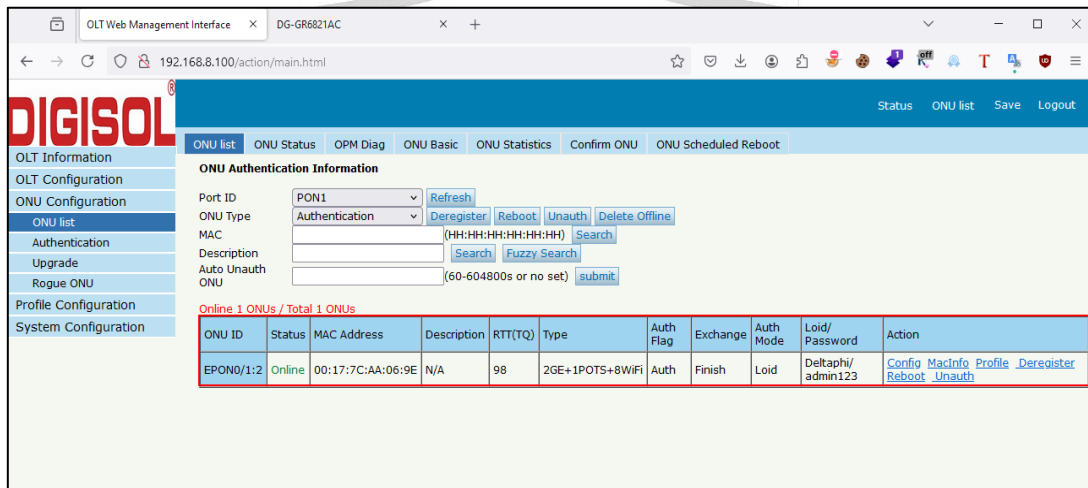


Figure no. 4.1.6.4: Registration verifying in the OLT

- viii. Verify that the ONU sends its serial number, registration ID, and logical ONU ID with credentials to the OLT, and that the DUT supports mutual authentication with a pre-shared key and encryption using the master session key.
- **Note:** The OEM should provide documentation required for the master session key (MSK) and confirm that DUT supports mutual authentication using a pre-shared key and encryption with the master session key.

11.1.5. Evidence Provided:

a.Screenshot from OLT after ONU registration below:

- i. Serial number – GPON006376DE2
- ii. Registration ID - MONU
- iii. Logical ONU ID – 00177caa069e
- iv. Credentials – Deltaphi/admin123

OLT Web Management Interface

192.168.8.100/action/main.html

Status ONU list Save Logout

System Log Alarm Threshold Alarm Syslog Server Syslog Server IPv6 Save Syslog

Alarm Log Table

Select Counts: 200

Alarm Type: ALL

Description: [Search]

Download Log: [Download]

No.1 Page/Total 2 Page 20 Item per page/Total 21 Item First, Previous, Next, Last No.1 Go Clear All Refresh

No.	Time	Level	Event	Message
1	1999/12/31 00:08:00	major	ONU AUTH Success	PON 0/1 ONU 1 1C:EF:03:37:6D:E2.
2	1999/12/31 00:07:59	major	PON LOS Recovery	PON 0/1 Link-Up
3	1999/12/31 00:07:59	major	ONU Register	PON 0/1 ONU 1 lid 0 1C:EF:03:37:6D:E2.
4	1999/12/31 00:07:33	major	ONU Deregister	PON 0/1 ONU 1 lid 0 1C:EF:03:37:6D:E2 MPCP TIMEOUT.
5	1999/12/31 00:07:31	major	PON LOS	PON 0/1 Link-Down
6	1999/12/31 00:06:44	major	ONU DEAUTH Success	PON 0/1 ONU 3 00:17:7C:AA:06:9E.
7	1999/12/31 00:06:44	major	ONU DEAUTH Success	PON 0/1 ONU 2 00:17:7C:A9:D0:6E.
8	1999/12/31 00:06:03	major	ONU Finish	PON 0/1 ONU 1 1C:EF:03:37:6D:E2.
9	1999/12/31 00:06:00	major	ONU AUTH Success	PON 0/1 ONU 1 1C:EF:03:37:6D:E2.
10	1999/12/31 00:06:00	major	ONU Register	PON 0/1 ONU 1 lid 0 1C:EF:03:37:6D:E2.
11	1999/12/31 00:06:00	major	PON LOS Recovery	PON 0/1 Link-Up
12	1999/12/31 00:05:59	major	PON LOS	PON 0/1 Link-Down
13	1999/12/31 00:05:59	major	PON LOS Recovery	PON 0/1 Link-Up
14	1999/12/31 00:05:59	major	ONU Deregister	PON 0/1 ONU 1 lid 0 1C:EF:03:37:6D:E2 MPCP ONU initiates DEREG.
15	1999/12/31 00:05:59	major	PON LOS	PON 0/1 Link-Down
16	1999/12/31 00:05:59	major	PON LOS Recovery	PON 0/1 Link-Up
17	1999/12/31 00:05:59	major	ONU Register	PON 0/1 ONU 1 lid 0 1C:EF:03:37:6D:E2.
18	1999/12/31 00:05:58	major	PON LOS	PON 0/1 Link-Down
19	1999/12/31 00:05:58	major	PON LOS Recovery	PON 0/1 Link-Up
20	1999/12/31 00:05:58	major	ONU Deregister	PON 0/1 ONU 1 lid 0 1C:EF:03:37:6D:E2 MPCP ONU initiates DEREG.

OLT Web Management Interface

DG-GR6821AC

https://192.168.8.100/action/main.html

Status ONU list Save Logout

ONU list ONU Status OPM Diag ONU Basic ONU Statistics Confirm ONU ONU Scheduled Reboot

Information Bandwidth Port VLAN QoS IGMP VoIP SIP POTS Alarm WAN WiFi DHCP Server

MAC Info Security Tr069 Misc Advance

EPON 0/1:3 00:17:7C:AA:06:9E Go Back

Basic Information

Description: [Submit]

Basic Information			
Vendor ID	MONU	Model ID	H423
ONU ID	00177caa069e	Hardware Version	V4.1
Software Version	V3.2.02-221128	Firmware Version	1.1.2 Nov 28 2022 14:49:39
Optical Module Information			
Temperature	37.05 °C	Supply Voltage	3.27 V
Bias Current	9.80 mA	Transmit Power	1.60 mW (2.04 dBm)
Receive Power	0.53 mW (-2.73 dBm)		
CAP2 Information			
ONU Type	HGU	Multi LLID	unsupport
Protection Type	unsupport	PONIF Count	1
Slot Count	0	Interface Type Count	5
Interface Type Port	GE(2); FE(0); POTS(1); USB(0); WLAN(2);		
VoIP Information			
MAC Address	00:17:7C:AA:06:9E	Protocol Support	SIP
Software Version	V3.2.02-221128	Software Time	20221128144306
User Count	1		

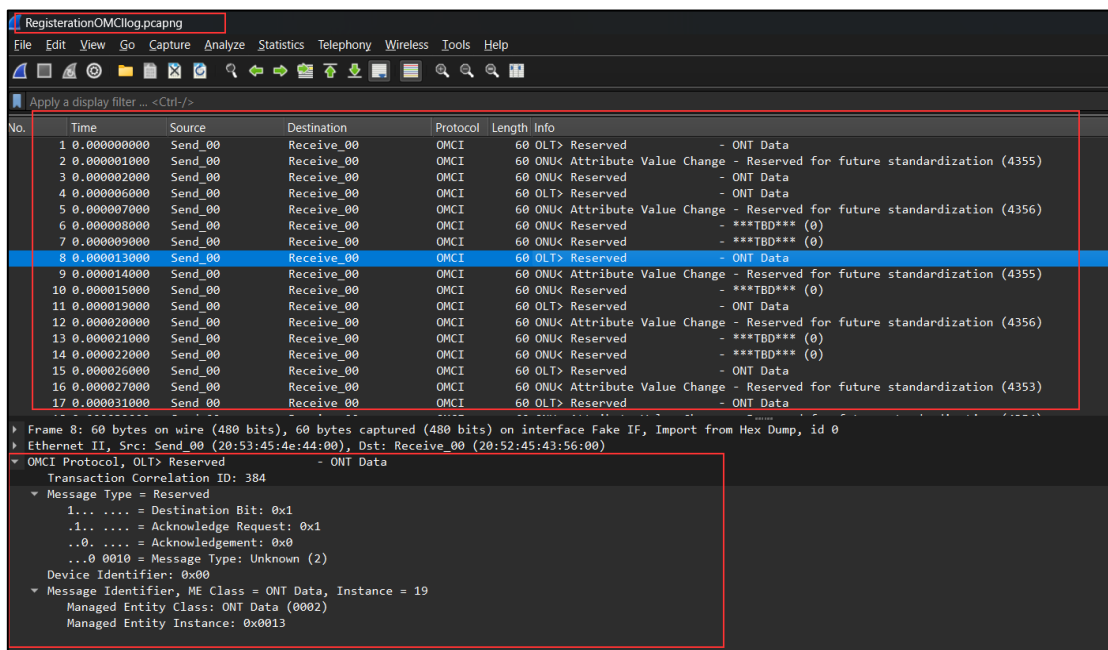
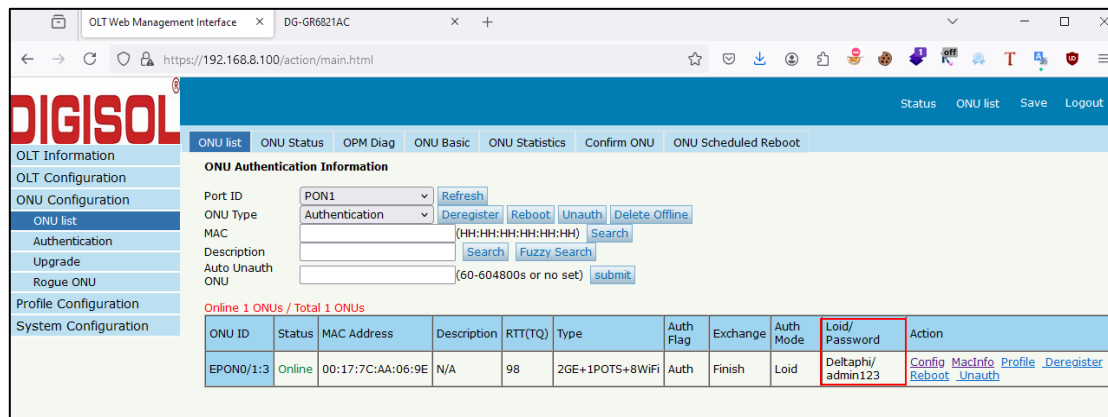
OLT Web Management Interface

ONU list ONU Status ONU Optical Information ONU Version Information ONU Manual Add ONU Allowlist ONU Statistics

Detail Information

Submit Back

Detail Information		Device Capability	
Description	GPON0/1:2	TCONT number:	31
Main software version	V2.1.08	GEM port number:	127
Standby software version	V2.1.08	Total priority queue number:	127
Vendor ID:	MONU	up priority queue number:	103
Version:	4.2E1	down priority queue number:	24
SN:	GPON00376de2	Traffic scheduler number:	31
Admin Status:	unlock	Traffic management option:	priority&rate controlled
Battery monito:	false	Total UNI number:	4
Security mode:	aes	Chip info:	2
Product code:	0	40GE number:	0
Total priority queue num:	127	25GE number:	0
Total traffic schedule num:	31	10GE number:	0
Traffic management option:	priority&rate controlled	5GE number:	0
Operate status:	enable	2.5GE number:	0



- **Note:** The OMCI logs captured on the DUT are transmitted in a Wireshark-compatible format. However, we are unable to interpret or decode these logs. To obtain the encryption and authentication keys used by the OLT and ONT during registration and properly analyze the OMCI logs, the OEM's documentation is necessary.

11.1.6. Test Observation: The tester observed that the ONT was transmitting its serial number, registration ID, logical ONU ID, and credentials while performing mutual authentication with the OLT.

- a. OEM dependent is required for the following points:
 - i. To check the data encryption between OLT and ONT, analysis of OMCI logs is required.
 - **Note:** The OEM should provide documentation explaining the process to convert the OMCI logs from hex dump format to binary data, which is the actual format required for a PCAP file to analyze the cryptographic controls used in the DUT during key exchange.
 - ii. The OEM should provide documentation detailing how the ONT and OLT mutually authenticate, compute a 128-bit master session key (MSK), and exchange session-specific shared secrets and data encryption keys.

12. **Test Case Result:** The ONT transmitted credentials during mutual authentication with the OLT. OEM-dependent documentation is required for converting OMCI logs to binary for PCAP analysis and for details on the session key and shared secrets exchange.

Note: OMCI logs are OEM proprietary. hence required OEM support to decode



2.13.2 TSTL Report for Evaluation Secure data Communication on wireless media (Ex: Wi-Fi) for ONT

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.2
---	--------------------------	------------------

Applicant Name: SyroTech

Application Number: GE-BE-1103240001

DUT Details: GPON-ONT

TSTL Document ID: GE-BE-1103240001 v001

DUT Make: SyroTech

DUT Model no: SY-GPON-2010-WADONT

DUT Serial Number: 5447E8-123455447E8541A97

DUT Software Version: V 3.2.02-231205

Applicable ITSAR: ONT ITSAR403012311

Version No: 1.0.1

OEM Supplied Document list: NA

1. **<ITSAR Section No & Name>** Section 13: Specific Requirement
2. **<Security Requirement No & Name >** 2.13.2. Secure data Communication on wireless media (Ex: Wi-Fi) for ONT
3. **Requirement Description:** ONU/ONT should support, WPA2- PSK or later version with AES standard in wireless networks which has strong encryption for Wi-Fi standard

4. DUT Confirmation Details:

DIGISOL[®]

Logout

Status

Status

Network

Security

Application

Management

Diagnostics

Help

Device Info

WAN Info

User Info

Voip Info

Remote Manage Info

Device Basic Info

Device Info

Device model	DG-GR6821AC
Device SN	123451CEF03376DE2
Hardware Version	V4.2
Firmware Version	V2.1.08-230602
PON S/N	GPON00376DE2



5. DUT Configuration

51. The DUT is configured with authentication credentials mentioned in DUT Confirmation Details.
52. The DUT (IP:192.168.1.1) is connected to the Lab's Testing Machine (IP:192.168.1.2) via LAN2.

Status

Gateway Name: HGU [Logout](#)

Status

Network

Security

Application

Management

Diagnose

Help

[Device Information](#)
[WAN Connection Info](#)
[User Information](#)
[VOIP Information](#)
[Remote Management Status](#)

Gateway Info:
IP Address: 192.168.1.1
MAC Address: 8014a8000000

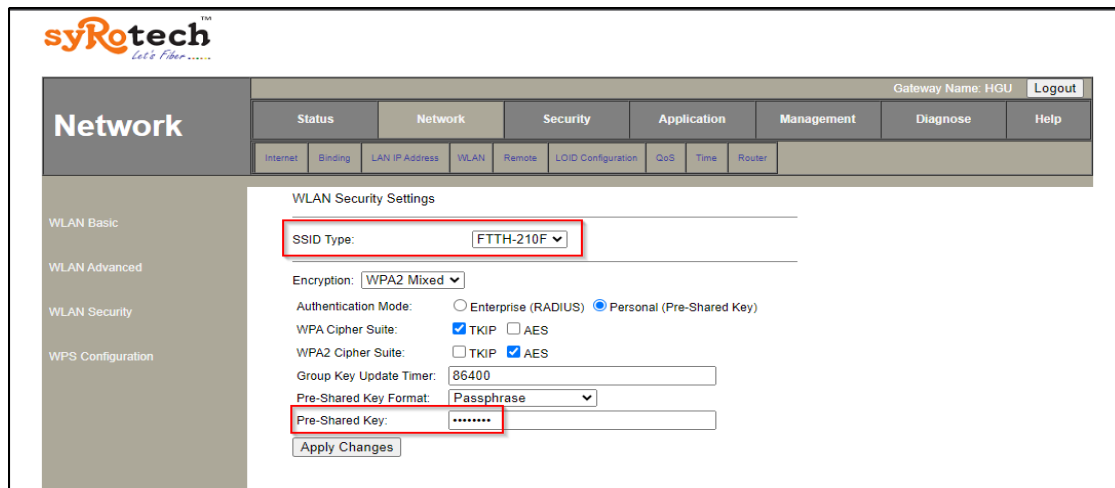
Receive/Send Info:

Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
PORT_1	43	7002	0	0	136	13195	0	0
PORT_2	1411	199188	0	0	1298	435765	0	0

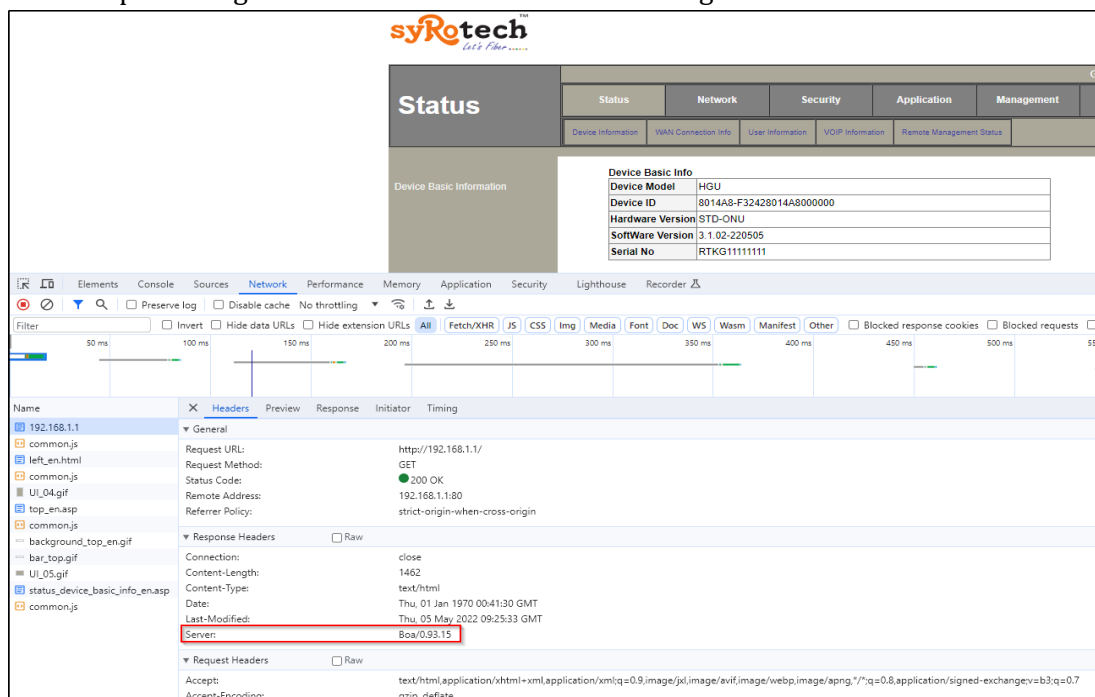
LAN Detect Status:

PORT	STATUS
LAN1	FAIL
LAN2	PASS

53. DUT is pre-configured with **SSID (FTTH-210F)** having Key "12345678".



54. DUT is pre-configured with Boa as a webserver having 0.93.15 version.



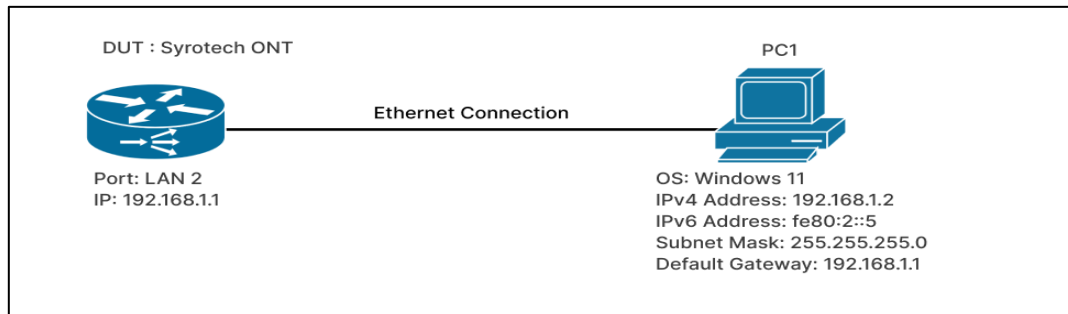
6. **Pre-Condition:** OEM shall documentation stating the supported access methods into DUT

7. **Test Objective:** To verify that minimum two of the above authentication attributes shall be mandatorily combined for protecting all the accounts from misuse and for local access and machine accounts, at least one authentication attribute shall be supported

8. Test Plan

8.1 Test Cases: To verify that the DUT supports WPA2-PSK or later version with AES standard in wireless networks which has strong encryption for Wi-Fi standard

8.2 Test Bed Diagram



8.3 Tools Required

9. Expected Result for pass

- To reset the DUT, long-press the physical rest button on the DUT.
- Open a web browser and enter the default address (192.168.1.1) in the address bar and enter the username '**admin**' and password '**Syro@43210\$**' in the login page.
- To verify that DUT supports WPA2-PSK with AES as default per standard, Navigate to Network > WLAN > WLAN Security.

10. Expected format of evidence: The DUT uses the standard WPA2-PSK with AES

11. Test Execution

Test Case Number	Test case name
01	To verify that the DUT supports WPA2-PSK or later version with AES standard in wireless networks which has strong encryption for Wi-Fi standard

11.1.1. Test Case Description: To verify that the DUT supports WPA2-PSK or later version with AES standard in wireless networks which has strong encryption for Wi-Fi standard

11.1.2. Execution Steps

- To reset the DUT, press the physical rest button on the DUT.
- Open a web browser and enter the default address (192.168.1.1) in the address bar and enter the username '**admin**' and password '**Syro@43210\$**' in the login page - as shown in figure 4.1.6.1.



Figure 4.1.6.1 – Login page of DUT

iii. To verify that DUT supports WPA2-PSK with AES as default per standard, Navigate to Network > WLAN > WLAN Security - as shown in figure 4.1.6.2.

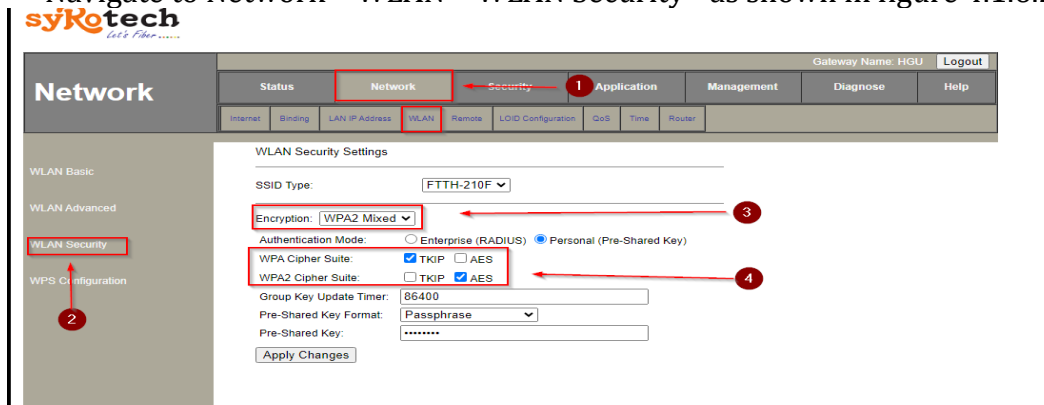
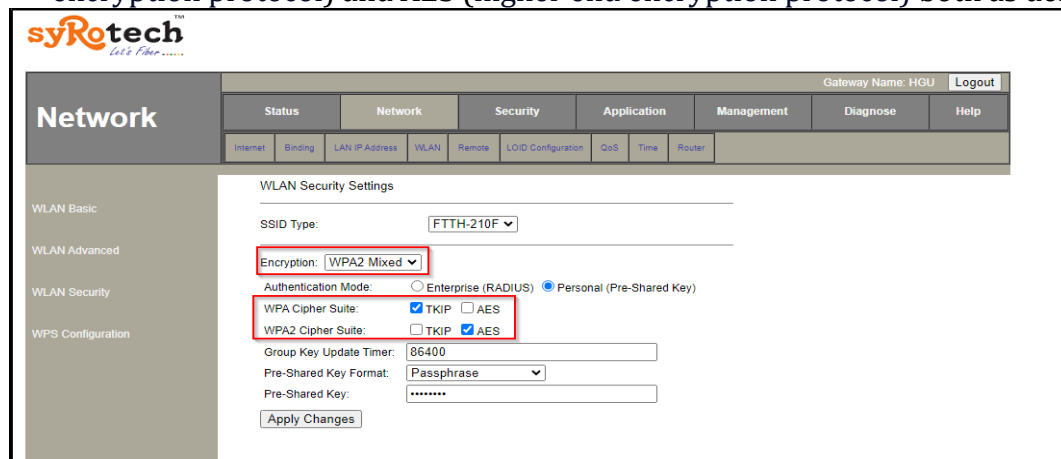


Figure 4.1.6.2 – Default encryption setting of DUT.

11.1.3.Evidence Provided: DUT supports WPA2- Mixed with TKIP (lower end encryption protocol) and AES (higher end encryption protocol) both as default.



11.1.4.Test Observation: The tester observed, that the DUT supports WPA2-Mixed with TKIP (lower end encryption protocol) and AES (higher end encryption protocol) both as default, not as per ITSAR, hence the testcase failed.

Securing Networks

12. Test Case Result

SL. No	TEST CASE NAME	PASS/FAIL	Remarks
1	DUT supports WPA2-PSK		

2.13.3 TSTP for Evaluation of MAC address filtering

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.3
---	--------------------------	------------------

<DUT Details: > Alphon AONT100C

<DUT Software Version:> R2.0.9.6

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

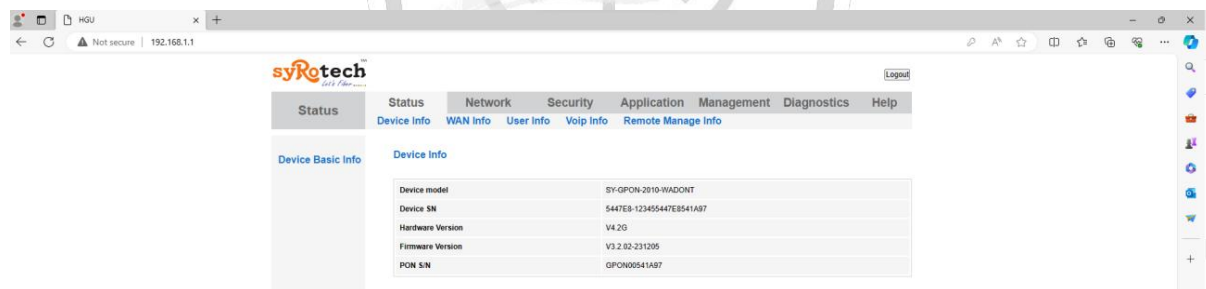
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 13: Specific Security Requirements

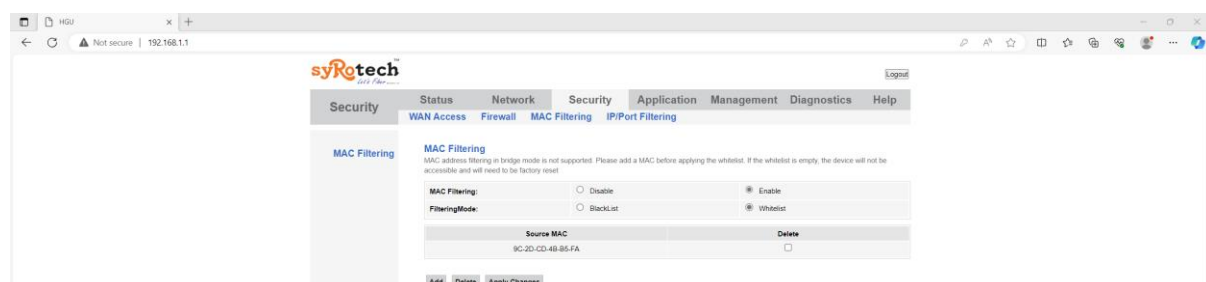
2. <Security Requirement No & Name > 2. 13.3: MAC Address Filtering

3. <Requirement Description: ONT/ONU should have capability for MAC address filtering, access is granted to matched address only.

4. DUT Confirmation Details:



5. DUT Configuration



6. Preconditions

- OEM document regarding blacklisting and whitelisting of terminal device based upon their MAC address.
- The tester has administrative privileges

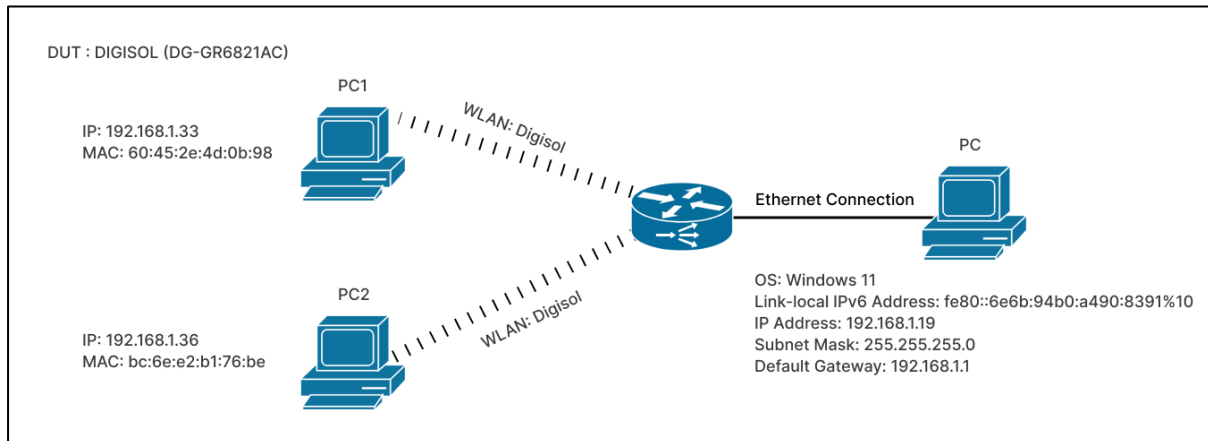
7. **Test Objective:** To verify the whitelisting configuration of DUT.

8. Test Plan

8.1. Number of Test Scenarios

8.1.1. Testing of whitelisting of MAC address

8.2. Test Bed Diagram



8.3. Tools Required: Any web browser

8.4. Test Execution Steps

- Tester shall enable MAC filtering feature and use whitelist for MAC address filtering.
- Tester will whitelist PC1 MAC Address. (Consequently , by default PC2 gets blacklisted)
- Try to access the DUT from PC1 and PC2.

9. Expected Results: PC1 should be able to access DUT while PC2 should not be able to access DUT.

10. Expected Form of Evidence: The screenshots of the web browser from where DUT is being access and after black listing DUT is not responding.

11. Test Execution

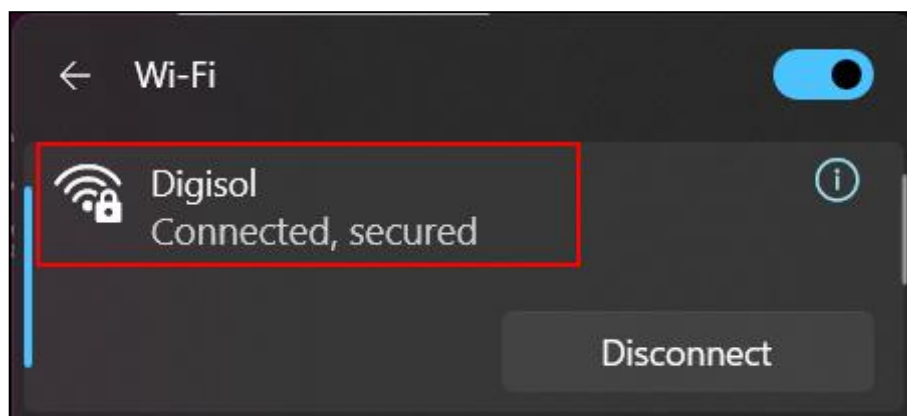
11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_WHITELIST_MAC

11.1.2. Test Case Description: To verify the whitelisting configuration of DUT.

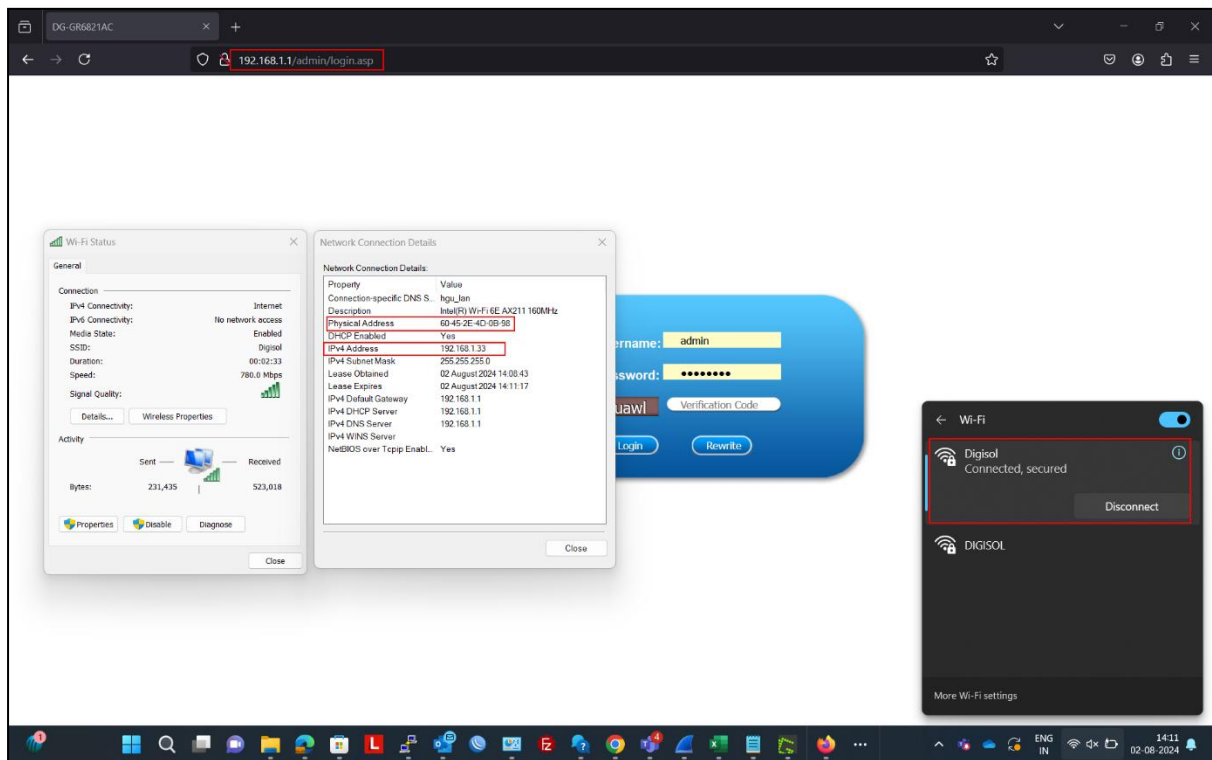
11.1.3. Execution Steps:

55. To verify that the PC1 is able to access the DUT, on system navigate to WIFI and enter the credentials



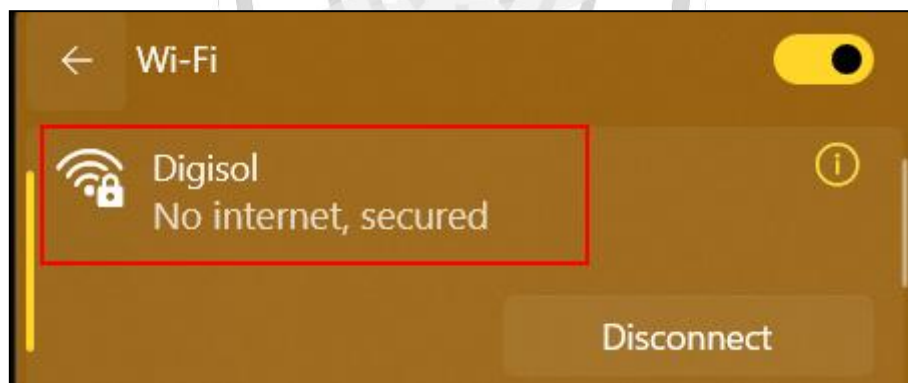
56.

PC1 connected to DUT via WIFI

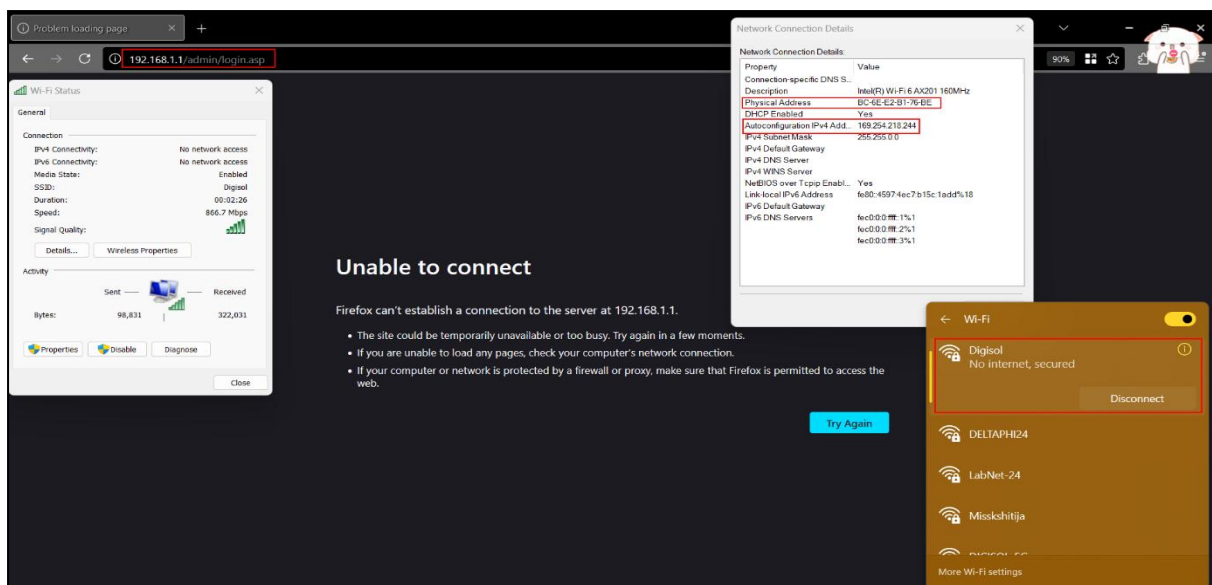


PC1 able to access DUT via WIFI

To verify that the PC2 is not able to access the DUT, on system Navigate to WIFI and enter the credentials



PC2 Connected to the DUT via WIFI



PC2 not able to Connect DUT via WIFI

11.1.4. **Test Observations:** PC1 is able to access DUT while PC 2 is not able to access

11.1.5. **Evidence Provided:** Screenshots of the DUT info page, when DUT was accessed from a MAC filtered device.

12. Test Case Results

Sl. No	TEST CASS NAME	PASS/FAIL	Remarks
1	TC_WHITELIST_MAC		



2.13.4 Configuration and management of ONTs (Using OMCI/TR69 protocols)

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.5
---	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

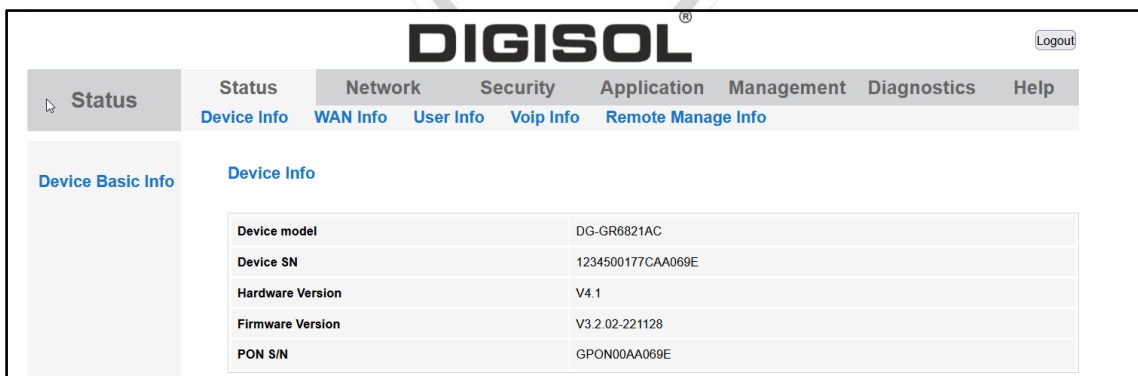
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 13: Specific Requirement

2. <Security Requirement No & Name >2.13.4 Configuration and management of ONTs (Using OMCI/TR69 protocols)

3. <Requirement Description:> Remote configuration management, fault management, performance management & security management of ONT/ONU shall comply mutual authentication & encryption of the management traffic using Secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)".

4. DUT Confirmation Details:



The screenshot displays the DIGISOL web interface. At the top, there is a navigation bar with the DIGISOL logo and a 'Logout' button. Below the navigation bar, there are tabs for 'Status', 'Network', 'Security', 'Application', 'Management', 'Diagnostics', and 'Help'. The 'Status' tab is selected, and it contains sub-tabs: 'Device Info', 'WAN Info', 'User Info', 'Voip Info', and 'Remote Manage Info'. The 'Device Info' sub-tab is active, showing a table with device details.

Device Basic Info	
Device model	DG-GR6821AC
Device SN	1234500177CAA069E
Hardware Version	V4.1
Firmware Version	V3.2.02-221128
PON S/N	GPON00AA069E



5. DUT Configuration

- i. The DUT (IP:192.168.1.1) is connected to the lab's testing machine via LAN1 and to the OLT via fiber cable on PON Port.

DIGISOL® Logout

Status **Status** **Network** **Security** **Application** **Management** **Diagnostics** **Help**

Device Info WAN Info User Info Voip Info Remote Manage Info

WLAN Info

LAN Info

Device Info

IP Address	192.168.1.1
MAC Address	1cef03378de2

LAN Port Status

Interface	State	Speed	Mode
Port_1	up	1000 M	Full duplex
Port_2	down	--	--

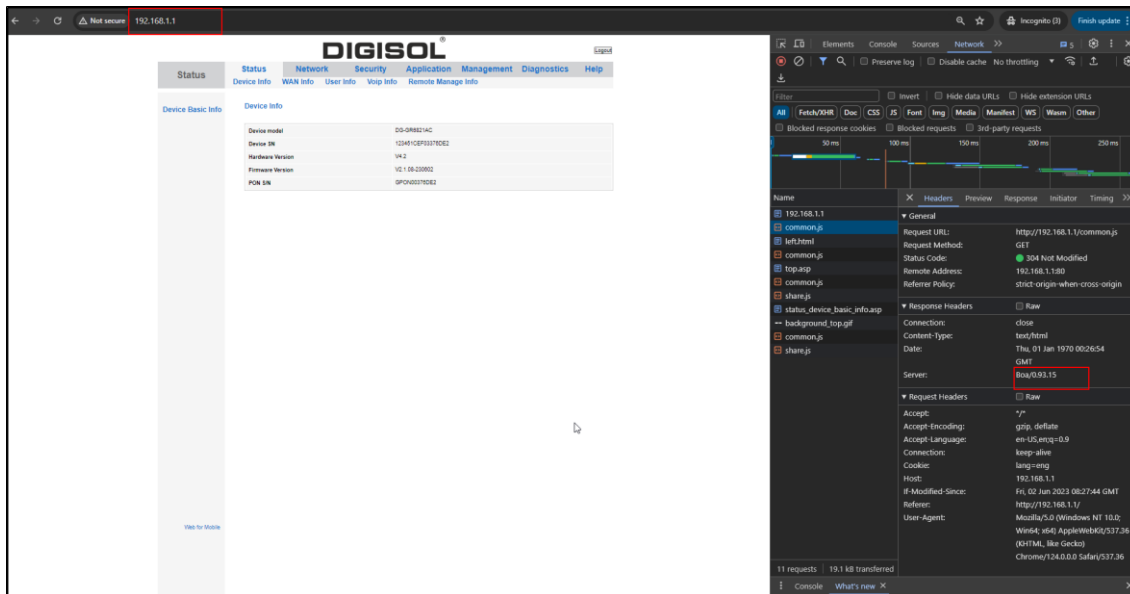
Send and Recv

Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
Port_1	4011	580881	0	0	4474	1841937	0	0
Port_2	0	0	0	0	0	0	0	0

Active DHCP Clients

Device Type	MAC Address	IP Address	Lease Time
-------------	-------------	------------	------------

ii. DUT is pre-configured with **BOA** as a webserver and its version 0.93.15.



6. Preconditions

- i. ONT/ONU is connected to the network and can communicate with the **OLT (for OMCI)** or **ACS (for TR-069)**.
- ii. Management protocols (**OMCI/TR-069**) are enabled.
- iii. The ONT supports **mutual authentication and encryption** using cryptographic controls.
- iv. Access to ONT/ONU CLI or Web Interface for log collection.

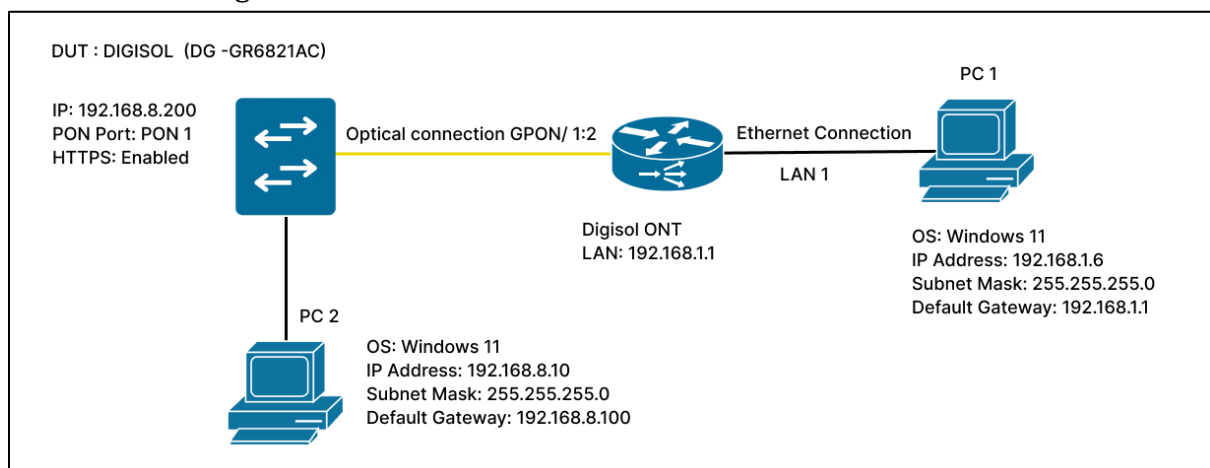
7. Test Objective: To verify Secure Remote Configuration, Fault Management, and Performance Management of ONT/ONU with Mutual Authentication and Encryption.

8. Test Plan

8.1. Number of Test Scenarios

8.1.1 Testing the mutual authentication Remote management protocol testing (TR069/OMCI) and testing the ciphers used for encryption of traffic between OLT and ONT.

8.2. Test Bed Diagram



8.3. Tools Required: Network logger, Browser

8.4. Test Execution Steps

- i. Initiate a remote management session between the **ACS (for TR-069) / OLT (for OMCI)** and the ONT.
- ii. Verify that the ONT and the server exchange certificates for mutual authentication.
- iii. Check logs on ONT for authentication details:

9. Expected Results:

- i. Remote Configuration of ONT should apply changes securely.
- ii. Fault Management of ONT should generate fault alarms.
- iii. For performance monitoring ONT should report correct usage.
- iv. Security Authentication in ONT should enforce mutual authentication.

10. Expected Form of Evidence: Screenshots or log files.

11. Test Execution

11.1 Test Case Number: 01

11.1.1. Test Case Name: TC_CONFIG_MGMT

11.1.2. Test Case Description: Verifying the protocol used for remote management of the DUT and its mutual authentication

11.1.3. Execution Steps: Check Secure remote configuration, fault management and performance management:

i) Remote configuration:

1. Connect PC1 to the ONT and PC2 to the OLT, ensuring the ONT and OLT are connected via an optical cable.
2. OMCI Configuration for ONT refer the [pre-condition](#).
3. On PC2 access the OLT's for remote configuration, Navigate to > config > WIFI SSID configuration > enter name **admin** and share key **12345678** and submit – as shown in figure 4.1.6.1 and 4.1.6.2

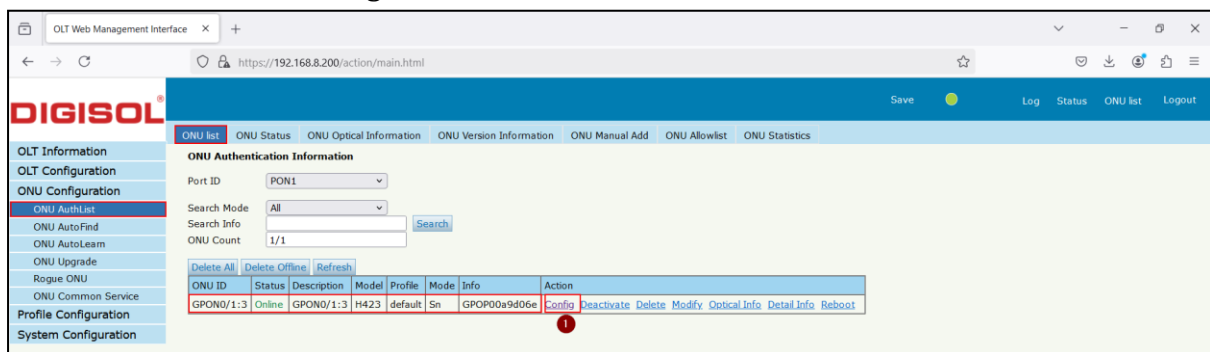


Figure No. 4.1.6.1: Changing ONU configuration

Figure No. 4.1.6.2: Changing ONU WIFI configuration

4. Verify the configuration using the Network Logger tool by checking the normal logs – as shown in figure 4.1.6.3

Figure No. 4.1.6.3: Verify in network logger tool as per the changes.

ii) Fault management:

1. To simulate fault, disconnect the optical cable from the ONT – as shown in figure 4.1.6.4

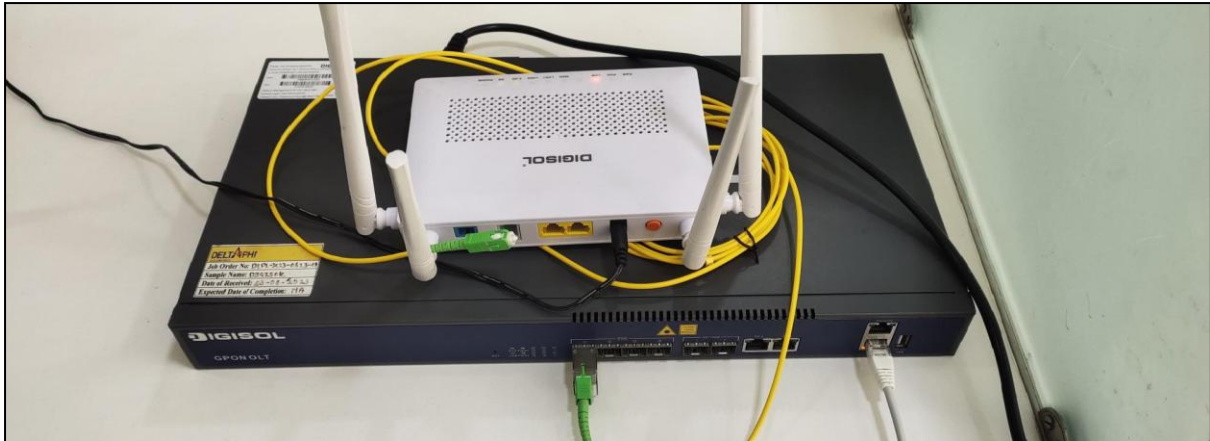


Figure No. 4.1.6.4: Disconnect the cable and simulate fault

2. Verify in normal log in network logger tool – as shown in figure 4.1.6.5

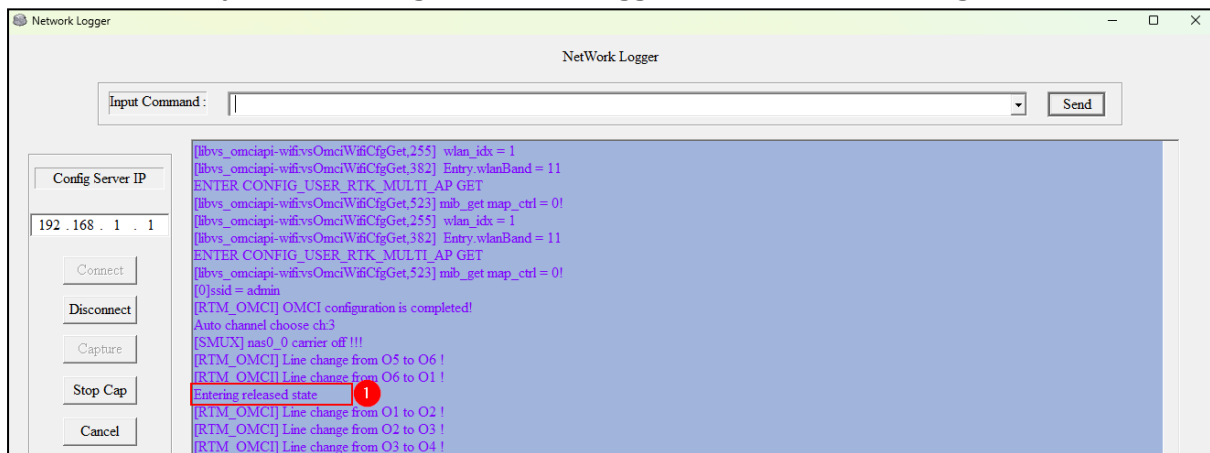


Figure No. 4.1.6.5: Verify in the network logger tool.

iii) Performance Management

1. Configure performance management settings on the OLT from PC2 as a **pre-condition**
2. On PC1, open the Net Logger tool and simulate laser on/off using the specified command – as shown in figure 4.1.6.6.
 - gpon set tx-laser force-on
 - gpon set tx-laser force-off
 - gpon set tx-laser normal

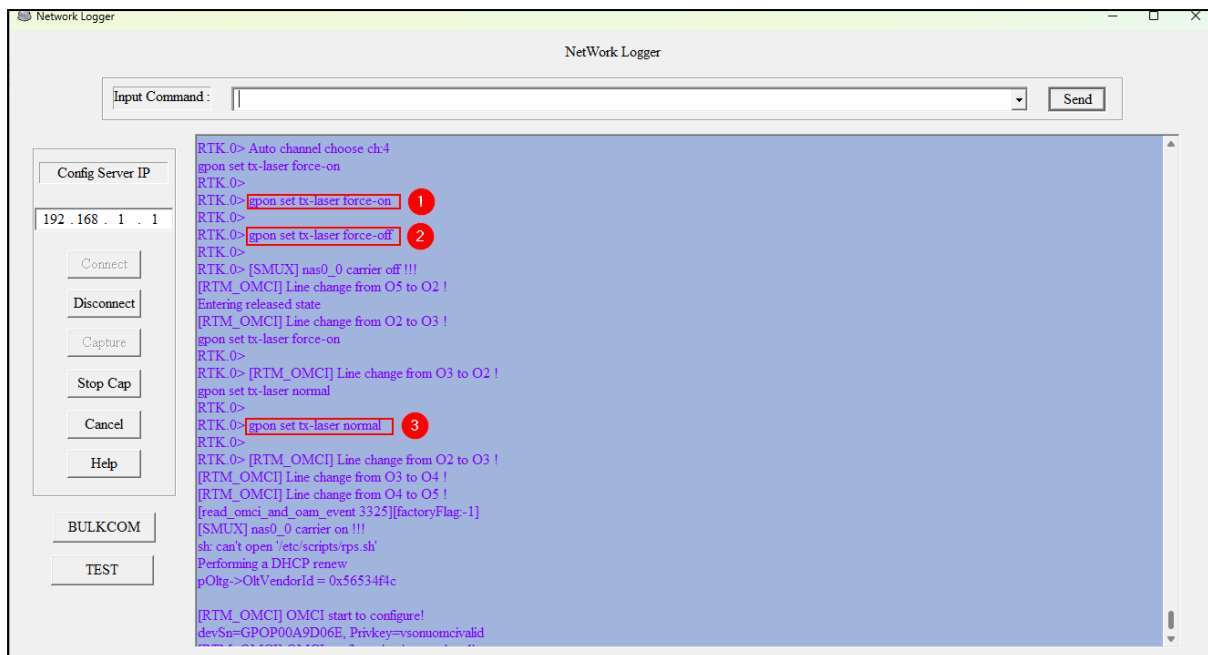


Figure No. 4.1.6.6: Simulate on/off the laser

3. Verify performance management in the OLT log – as shown in figure 4.1.6.7

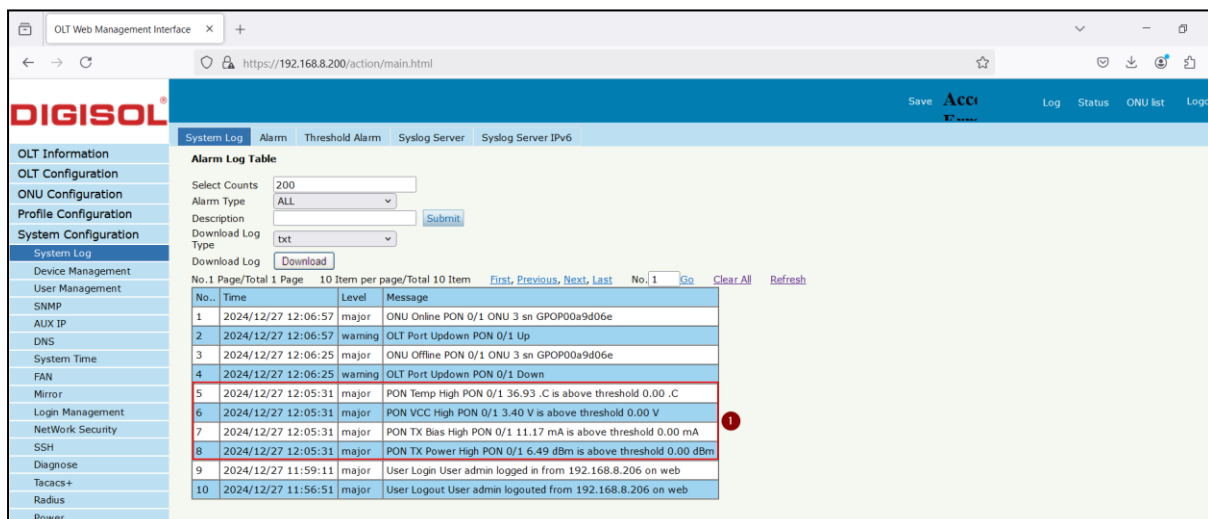
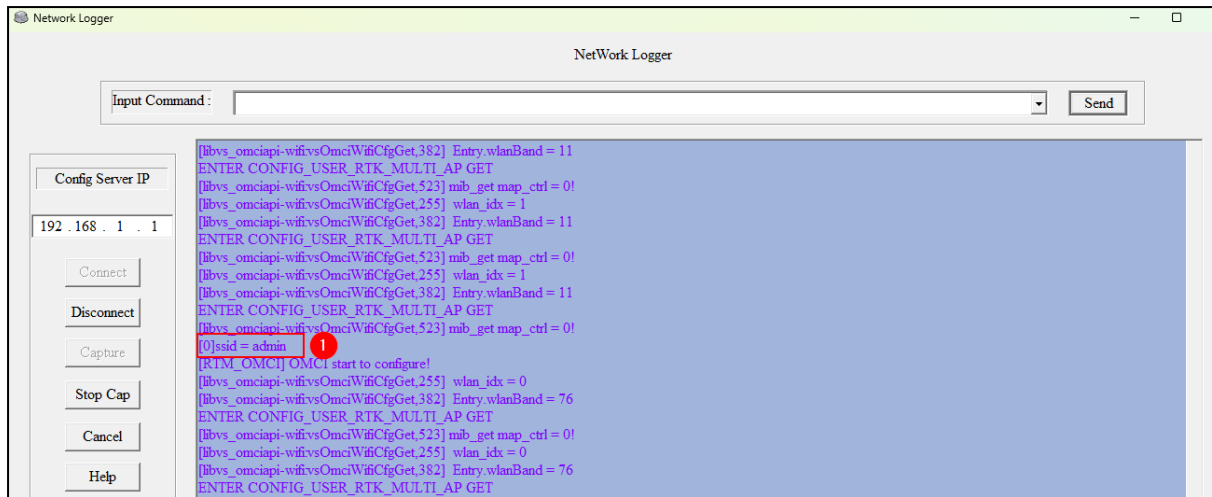


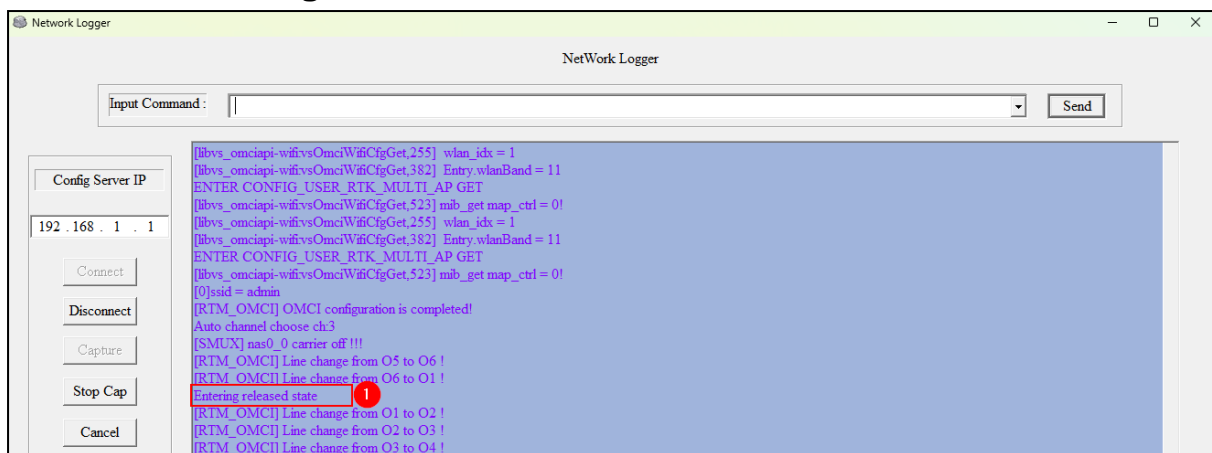
Figure Verify in OLT, ONT performance is recorded.

11.1.4. Evidence Provided:

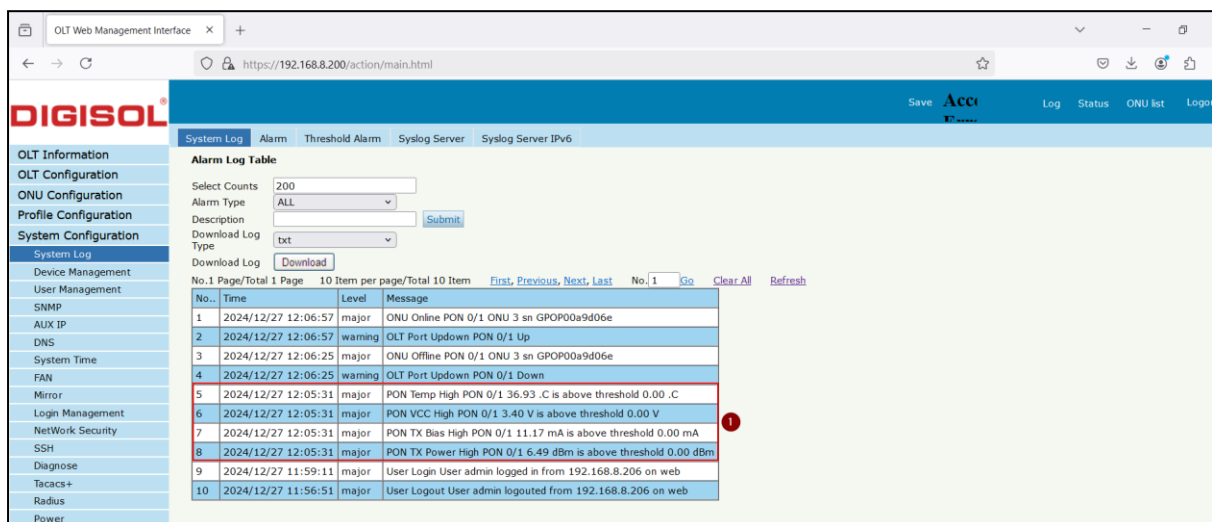
i. Remote configuration:



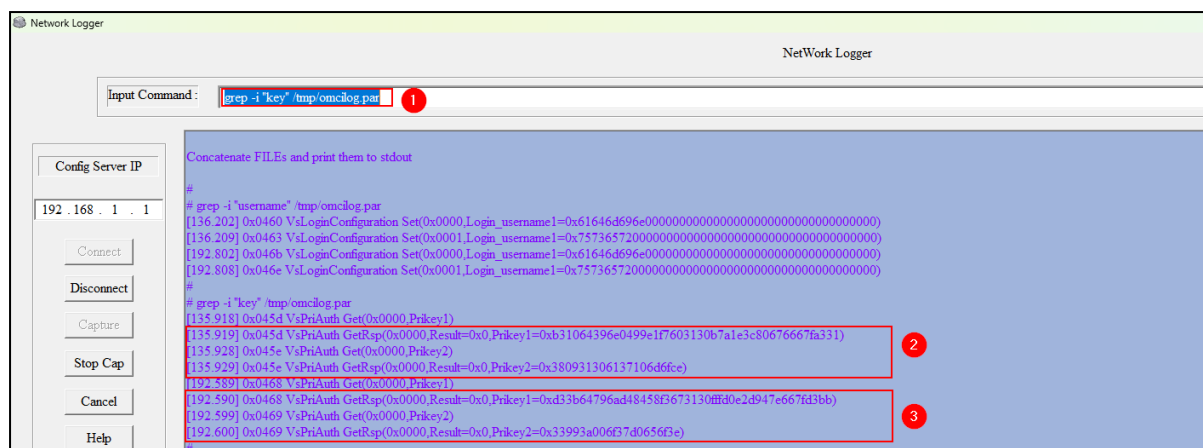
ii. Fault management:



iii. Performance Management:



Note: All configuration and management are logged in ONT's OMCI logs. The **OLT authenticates the ONT** by retrieving **Prikey1** and **Prikey2**, while the ONT authenticates the OLT it's not showing in the log OEM need to provide.



11.1.5. Test Observations:

- i. All configuration and management are logged in ONT's OMCI logs. The OLT authenticates the ONT by retrieving Prikey1 and Prikey2, while the ONT authenticates the OLT it's not showing in the log OEM need to provide.
- ii. There is only one-way authentication, with no mutual authentication. The OEM must specify the encryption method used in the OMCI logs.

11.1.6. Evidence Provided: screenshots or Web GUI

12. Test Case Results

Sl. No	TEST CASS NAME	PASS/FAIL	Remarks
1	TC_CONFIG_MGMT	OEM Dependent	

2.13.5 TSTP for IGMP Filter

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.5
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

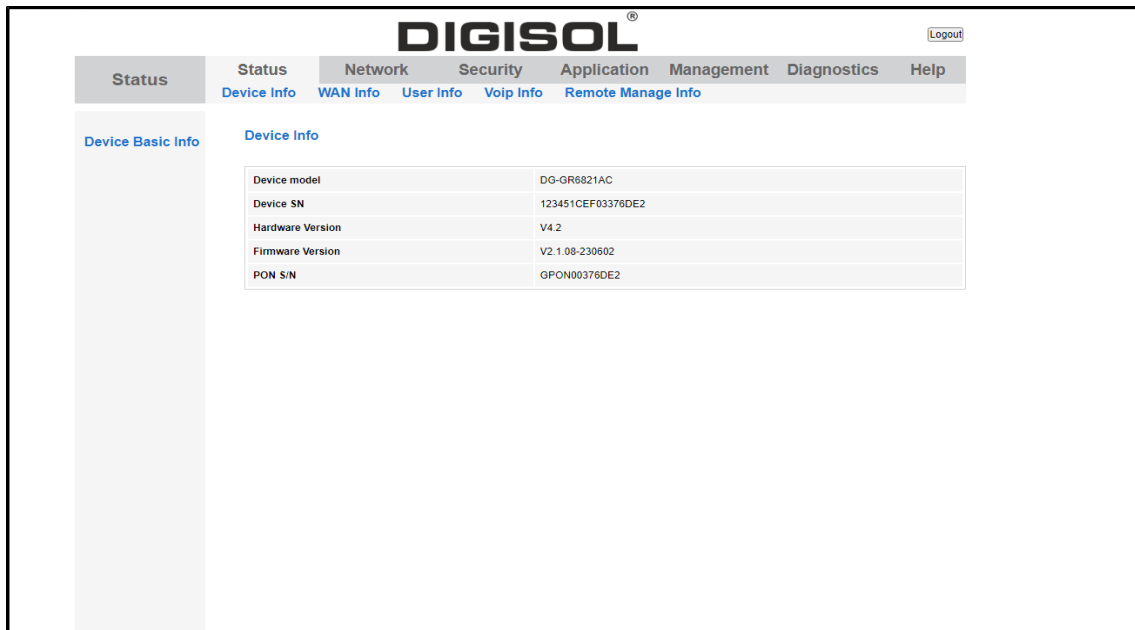
1. <ITSAR Section No & Name> Section 13: Vulnerability Testing Requirements

2. <Security Requirement No & Name > 2.13.5 IGMP Filter

3. <Requirement Description:> The ONT must be able to filter upstream IGMP requests based on white and black lists of multicast groups (defined by both source and destination IP address and placed by the OLT through appropriate OMCI messages) that will allow subscribers to request only multicast streams from the white list or any multicast stream except from the black list.

Reference clause 134 of ETSI TS 102 973 V1.1.1 (2008-09)

4. DUT Confirmation Details:



The screenshot displays the DIGISOL web management interface. At the top, the 'DIGISOL' logo is centered, with a 'Logout' link on the right. Below the logo is a navigation bar with tabs: 'Status', 'Network', 'Security', 'Application', 'Management', 'Diagnostics', and 'Help'. The 'Status' tab is active, and within it, the 'Device Info' sub-tab is selected. On the left side, there is a sidebar with 'Device Basic Info' and 'Device Info' options. The main content area shows a table with device details:

Device model	DG-GR6821AC
Device SN	123451CEF03376DE2
Hardware Version	V4.2
Firmware Version	V2.1.08-230602
PON S/N	GPON00376DE2



5. DUT Configuration

Note: “The provided configuration is an example serves as a reference point for when such functionality becomes available.”

- i. The DUT (192.168.1.1) is connected to the Tester Machine’s via LAN2 interface.

DIGISOL®

Logout

Status Network Security Application Management Diagnostics Help

Device Info WAN Info User Info Voip Info Remote Manage Info

WLAN Info

LAN Info

Device Info

IP Address 192.168.1.1

MAC Address 00177caa069e

LAN Port Status

Interface	State	Speed	Mode
Port_1	down	--	--
Port_2	up	1000 M	Full duplex

Send and Recv

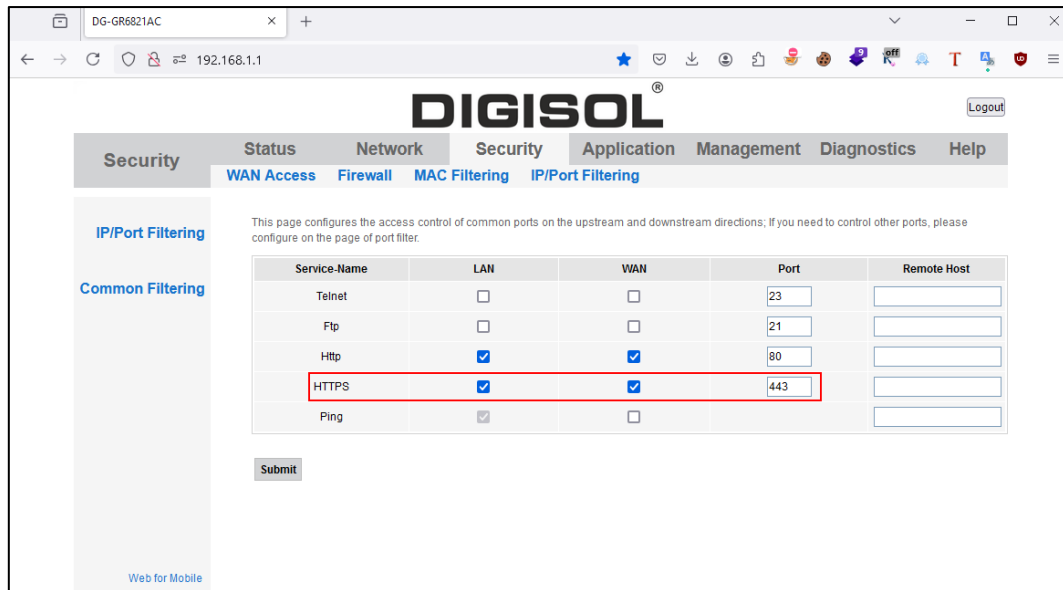
Interface	Receive				Send			
	Packets	Bytes	Errors	Dropped	Packets	Bytes	Errors	Dropped
Port_1	2079	467487	0	0	2204	636909	0	0
Port_2	784	171280	0	0	608	204454	0	0

Active DHCP Clients

Device Type	MAC Address	IP Address	Lease Time
-------------	-------------	------------	------------

Web for Mobile

- ii. HTTPS is enabled.



iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN
aravind@Aravind_V:~$ |

```

6. Preconditions: OEM document is required which will provide the detailed configuration and management of OMCI (ONT management and control interface) message format and handling procedures.

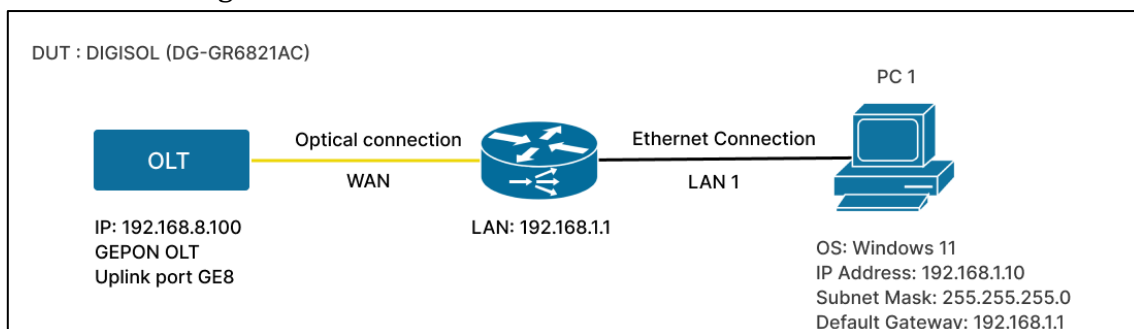
7. Test Objective: To verify filtering of IGMP packets according to configured blacklist/whitelist

8. Test Plan

8.1. Number of Test Scenarios

8.1.1. To verify that DUT filters upstream igmp request based on White and Black list of multicast group placed by OLT through OMCI messages.

8.2. Test Bed Diagram



8.3. Tools Required: Firefox Browser

8.4. Test Execution Steps

- i. The tester configures the backlisting of the multicast groups in the OLT.
- ii. The tester then connects the ONT with the OLT via optical terminal.
- iii. Tester then checks the active devices list in the OLT. Tester sends the IGMP packets to the OLT.
- iv. If the status of the ONT is active than device is whitelisted for multicast group otherwise its in the backlisted group.

9. Expected Results: Tester should ensure filtering of IGMP packets according to configured blacklist/whitelist

10. Expected Form of Evidence: Screenshots

11. Test Execution

11.1 Test Case Number: 01

11.1.1. Test Case Name: FILTER_IGMP_PACKET

11.1.2. Test Case Description: To verify that the DUT correctly filters upstream IGMP requests based on whitelist and blacklist configurations for multicast groups set by the Optical Line Terminal (OLT) via OMCI messages.

11.1.3. Execution Steps:

- i. Login into OLT.
 - ii. Configure the OLT with a whitelist and blacklist of multicast groups.
 - iii. Ensure that the whitelist and blacklist include both source and destination IP addresses.
 - iv. Configure OMCI messages to send the whitelist and blacklist information to the DUT.
 - v. Configure DUT to receive and correctly interpret the OMCI.
 - vi. Generate IGMP requests for both whitelisted and blacklisted multicast groups.
 - vii. Verify that the DUT, Allows IGMP requests for multicast groups in the whitelist and Denies IGMP requests for multicast groups in the blacklist.
- **Note:** The OLT does not support the creation of whitelists and blacklists for IGMP multicast group filtering. Additionally, the ONT's IGMP configuration via OLT only includes IGMP snooping but lacks the ability to filter multicast groups based on predefined lists. Consequently, the OLT cannot instruct the ONT to filter IGMP requests using OMCI messages based on whitelist and blacklist criteria.

11.1.4. Test Observations: Case 1:

- i. The OLT does not support the creation of whitelists and blacklists for IGMP multicast group filtering.
- ii. Additionally, the ONT's IGMP configuration via OLT only includes IGMP snooping but lacks the ability to filter multicast groups based on predefined lists.
- iii. Therefore, the OLT cannot instruct the ONT to filter IGMP requests using OMCI messages based on whitelist and blacklist criteria.

11.1.5. Evidence Provided: Tester should attach output screenshots. (Here DUT is not having this functionality)

12. Test Case Results

Sl. No	TEST CASS NAME	PASS/FAIL	Remarks
1	FILTER_IGMP_PACKET		

2.13.6 TSTP Evaluation for SSID Scanning

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.6
--	--------------------------	------------------

<DUT Details: > **SyroTech**

<DUT Software Version:> **V 3.2.02-231205**

<Digest Hash of OS>

<Digest Hash of Configuration> Hash of DUT configuration is required

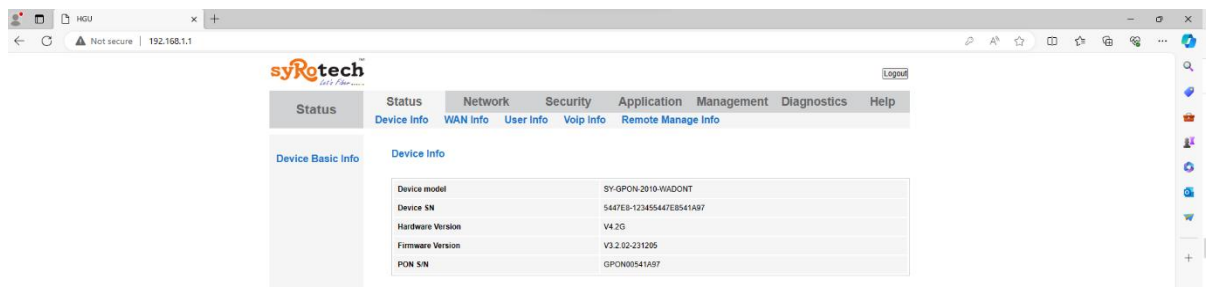
<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

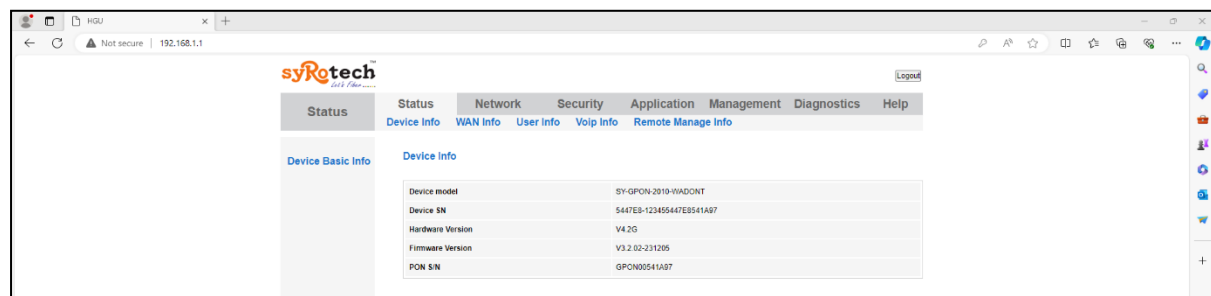
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

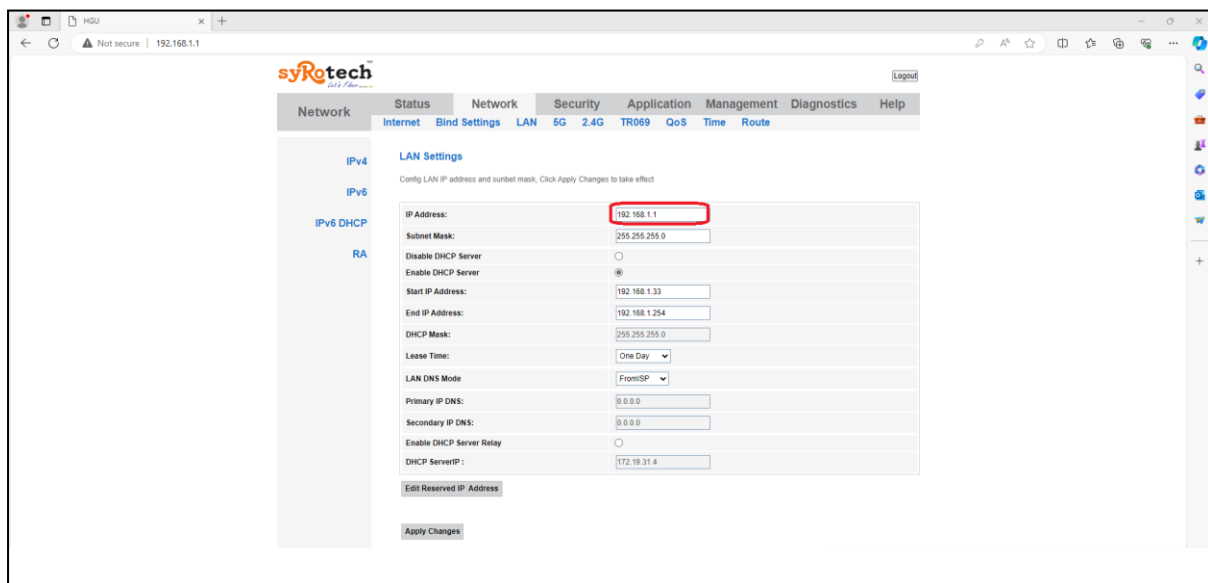
1. <ITSAR Section No & Name> Section 13: Specific Requirement.
2. <Security Requirement No & Name > 2.13.6 SSID Scanning
3. <Requirement Description: > The ONT/ONU shall not disclose sensitive information, PIN details on SSID scan / attack techniques. It needs to provide disguised feedback to users on unsuccessful attempts without revealing a reason for failures. Option to hide / unhide SSID on user selection is an essential feature.

4. DUT Confirmation Details:



Below screenshot is IP address of DUT:





Below Screenshot is IP address of DUT Test Machine:

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\GRL MAS> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 2001:db8::2
    IPv6 Address . . . . . : fe80::f15:48d0:ec20:8580%5
    Link-local IPv6 Address . . . . . : fe80::f15:48d0:ec20:8580%5
    IPv4 Address . . . . . : 192.168.1.22
    Subnet Mask . . . . . : 255.255.255.0
    IPv4 Address . . . . . : 192.168.3.1
    Subnet Mask . . . . . : 255.255.248.0
    Default Gateway . . . . . : 2001:db8::1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::828b:589b:918f:89ec%15
    IPv4 Address . . . . . : 192.168.1.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f620:5e07:cb37:86aa%4
    IPv4 Address . . . . . : 192.168.100.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e92b:1eeb:17bc:293a%25
    IPv4 Address . . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1042:cb42:a604:410e%20
    IPv4 Address . . . . . : 169.254.19.174
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet 6:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::be98:ec2f:d4cc:6198%2
    IPv4 Address . . . . . : 192.168.169.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 
  
```

Additionally, to ensure the connectivity between the DUT and the test machine, a ping test is conducted. This test verifies the ability to test machine to communicate with the DUT over the Ethernet connection by sending ICMP echo requests and receiving ICMP echo replies. A successful ping indicates that the network connection is established and

functioning properly, enabling further testing and data transfer between the DUT and the test machine.

```
PS C:\Users\GRL MAS> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

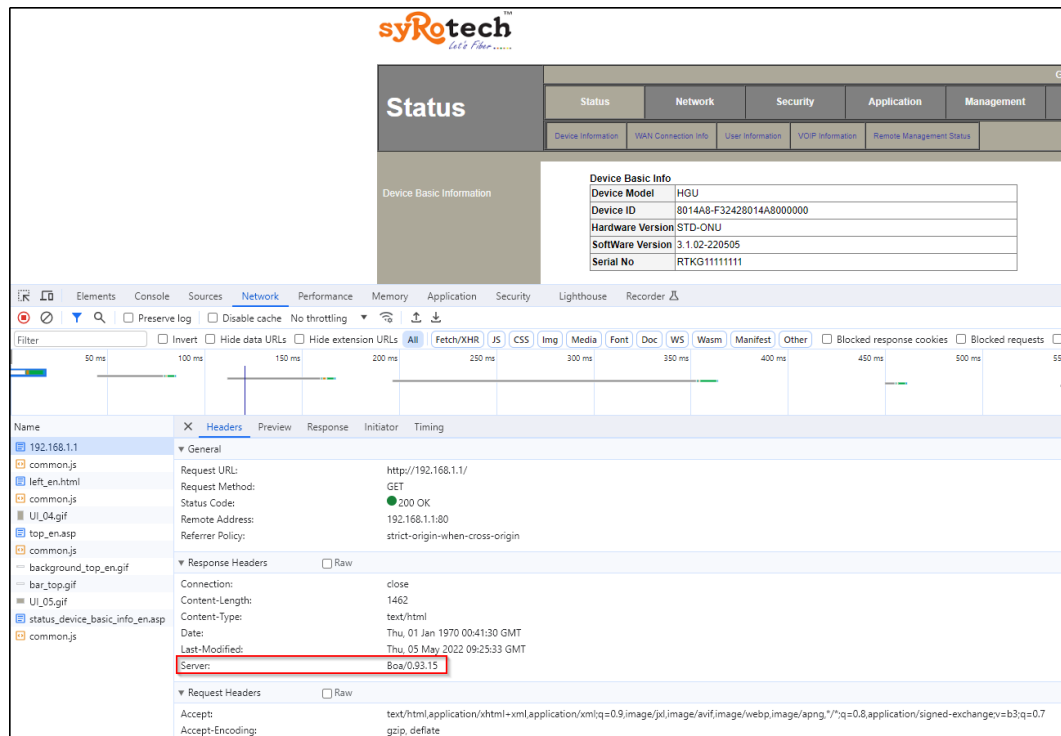
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\GRL MAS>
```

5. DUT Configuration:

- i. DUT is configured with SSID Name (Syrotech) and SSID Key (Delta@00).
- ii. DUT (192.168.1.1) is connected to the Testing machine (192.168.1.2) via WI-FI.

The screenshot shows the Syrotech web interface. The top navigation bar includes 'Gateway Name: HGU' and a 'Logout' button. Below this is a 'Network' section with tabs for 'Status', 'Network', 'Security', 'Application', 'Management', 'Diagnose', and 'Help'. The 'Security' tab is active, showing 'WLAN Security Settings'. The settings include: 'SSID Type' set to 'Syrotech', 'Encryption' set to 'WPA2 Mixed', 'Authentication Mode' set to 'Personal (Pre-Shared Key)', 'WPA Cipher Suite' set to 'TKIP', 'WPA2 Cipher Suite' set to 'AES', 'Group Key Update Timer' set to '86400', 'Pre-Shared Key Format' set to 'Passphrase', and 'Pre-Shared Key' set to '*****'. The 'Apply Changes' button is at the bottom.

- iii. DUT is pre-configured with **boa** as a webserver and its version **0.93.15**.



6. Preconditions

13.1.24. The tester should have the Privileges to log in to the DUT.

i. The tester should have all the system resources access.

13.1.25. The OEM should provide document on how to enable the option to hide SSID from the DUT

7. **Test Objective:** To ensure that The ONT shall not disclose sensitive information, PIN details on SSID scan / attack techniques. It needs to provide disguised feedback to users on unsuccessful attempts without revealing of reason for failures. Option to hide / unhide SSID on user selection is an essential feature.

8. Test Plan:

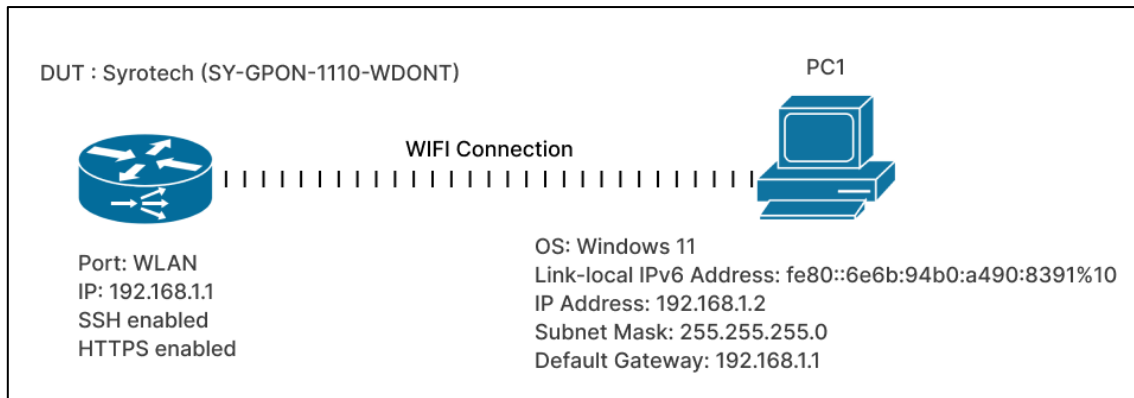
8.1 Number of Test Scenarios

8.1.1 Verify that the DUT does not disclose any sensitive information, PIN details on SSID scan/ attack techniques.

8.1.2 Verify that the DUT does not provide the reason for failure while incorrect login attempts on SSID.

8.1.3 Verify that the option to hide/unhide SSID is available in the DUT.

8.2 Test Setup Diagram:



8.3 Tools Used: airteddon,

8.4 Test Execution Steps

- i. CASE I: Verify that the DUT does not disclose any sensitive information, PIN details on SSID scan/ attack techniques.
 1. To check if DUT has any protection mechanism for Key (Password) Disclosure, navigate through terminal, launch the tool Airteddon by entering following command: `./airteddon.sh`
 2. To capture BSSID of the DUT, select the following option as follows and copy the bssid. Interface to work with option select: 2 (WLAN0mon interface) in option for menu select: 2 (Enable Monitor Mode) in option for menu select: 6 (PMKID/Handshake tool menu) in option for menu select: 6 (Capture Handshake)
 3. To check if any sensitive information has been disclosed (Password (PSK)), navigate through terminal, enter following command: `wifite -bssid <DUT SSID>` (copied from the previous tool)
- ii. CASE II: Verify that the DUT does not provide the reason for failure while incorrect login attempts on SSID.
 1. Enter incorrect SSID credentials and verify that the DUT does not provide the reason of failure.
- iii. CASE III: Verify that the option to hide/unhide SSID is available in the DUT.
 1. Launch the tool wifite in terminal and enter the following command to scan the network and ensure that the SSID is **"not hidden"**.
 2. Refer to precondition and configure the DUT to hide SSID.
 3. Launch the tool wifite in terminal and enter the following command to scan the network and ensure that the SSID is **"hidden"**. `wifite --clients-only`

9. Expected Results for Pass:

- a. The tester checks and verifies the following on the DuT:
 - i. The Dut shall not disclose sensitive information, PIN details on SSID scan / attack techniques.

- ii. The DuT needs to provide disguised feedback to users on unsuccessful attempts without revealing of reason for failures.
- iii. Option to hide / unhide SSID on user selection as an essential feature should be present on DUT.

10. **Expected Format of Evidence:** screen shots of test executions.

11. Test Execution:

11.1 Test Case Number: 01

11.1.1. **Test Case Name:** Verify that the DUT does not disclose any sensitive information, PIN details on SSID scan/ attack techniques.

11.1.2. **Test Case Description:** Ensure that the DUT does not reveal any sensitive information or PIN details during SSID scan/attack techniques.

11.1.3. Execution Steps:

- i. Launch the tool airgeddon by entering the following command in terminal `sudo airgeddon`
- ii. To Capture the BSSID of the DUT enter the following option as follows and copy the bssid – as shown in figure Interface to work with option select:2 (wlan0)

```

kali@kali: ~
***** Interface selection *****
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82545EM
2. wlan0 // 2.4Ghz // Chipset: Qualcomm Atheros Communications AR9271 802.11n
*Hint* Do you have any problem with your wireless card? Do you want to know what card could be nice to be used
in airgeddon? Check wiki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets
> 2

```

Figure Select the wlan0 interface
in option for menu select: 2 (Enable Monitor Mode)

```

kali@kali: ~
***** airgeddon v11.31 main menu *****
Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz
Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits / Sponsorship mentions
12. Options and language menu
*Hint* Since airgeddon 9.20 version, tmux is supported and it can be used instead of xterm as windows handler.
Script can be launched in a headless environment without a graphical X window system. It is recommended only fo
r advanced users. Like any other option, it can be configured on the options menu, on the /usr/share/airgeddon/
.airgeddonrc options file or launched using AIRGEDDON_WINDOWS_HANDLING "flag" in the command line. More informa
tion about options customization at Wiki: https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Options
> 2

```

Figure– Select interface monitoring mode.
in option for menu select: 6 (PMKID/Handshake tool menu)

```

kali@kali: ~
***** airogeddon v11.31 main menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
0. Exit script
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. DoS attacks menu
5. Handshake/PMKID tools menu
6. Offline WPA/WPA2 decrypt menu
7. Evil Twin attacks menu
8. WPS attacks menu
9. WEP attacks menu
10. Enterprise attacks menu
11. About & Credits / Sponsorship mentions
12. Options and language menu

*Hint* It is known that the software used in the 5Ghz band still presents some problems sometimes. For example
airodump, that when scanning networks can show a value "-1" on channel depending on the card chipset and the dr
iver. It is also known that Ralink chipsets sometimes are getting errors on high channels "

> 5

```

Figure- Select handshake menu.
in option for menu select: 6 (Capture Handshake)

```

kali@kali: ~
***** Handshake/PMKID tools menu *****
Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
   (monitor mode needed for capturing)
5. Capture PMKID
6. Capture Handshake
7. Clean/optimize Handshake file

*Hint* In WPA/WPA2-PSK networks you can crack either PMKIDs or Handshakes to obtain the network passphrase

> 6

```

Figure- Capture the handshake.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
CH 4][Elapsed: 18 s][2024-01-03 04:42								
F8:0D:A9:F1:A6:C9	-80	2	0 0	11	130	WPA2 CCMP	PSK	Airtel_SUNIL K2
18:0F:76:80:39:16	-70	4	0 0	13	270	WPA2 CCMP	PSK	Labs-24
42:62:8B:F1:11:0E	-86	4	0 0	11	540	WPA2 CCMP	PSK	SARA MOBILE
5C:62:8B:F1:11:0E	-83	2	0 0	11	540	WPA2 CCMP	PSK	SARA PRIVATE
AC:84:C6:E2:65:54	-90	2	0 0	5	195	WPA2 CCMP	PSK	NG MEADOWS
58:C1:7A:91:76:92	-78	5	0 0	5	130	WPA2 CCMP	PSK	Express WiFi by F
58:C1:7A:91:76:90	-79	5	0 0	5	130	WPA2 CCMP	MGT	<length: 0>
58:C1:7A:91:76:91	-78	6	0 0	5	130	WPA2 CCMP	MGT	AnOkIt-ss3ccA-Eth
B4:3D:08:05:91:31	-81	9	0 0	2	270	WPA2 CCMP	PSK	EQUIP_ENGINEER -2
80:14:A8:00:00:00	-43	28	0 0	5	270	WPA2 CCMP	PSK	Syrotech
8C:FD:18:89:04:44	-86	4	4 0	7	130	WPA2 CCMP	PSK	SUNIL K
B4:A7:C6:01:97:31	-86	12	0 0	6	130	WPA2 CCMP	PSK	Airtel_HGS 102
1C:EF:03:37:6D:E7	-57	36	0 0	8	130	WPA2 CCMP	PSK	DIGISOL
78:9A:18:66:BD:71	-68	39	0 0	7	54	WPA2 CCMP	PSK	MikroTik-66BD71
BA:A1:F3:79:C0:09	-83	10	0 0	1	360	WPA2 CCMP	PSK	ASUS 8Z
E0:3F:49:A8:FA:F8	-40	21	0 0	1	195	WPA2 CCMP	PSK	ASUS_2.4G
60:BD:2C:44:15:C9	-83	10	0 0	1	130	WPA2 CCMP	PSK	Airtel_Zerotouch

Figure- Capture BSSID of the Network.

- iii. In terminal launch the tool wifite and enter the following command to scan the network for sensitive information – as shown in figure
“wifite --bssid 80:14:A8:00:00:00 (copied from the previous tool)”

```
(root@kali)~# wifite --bssid 80:14:A8:00:00:00

wifite2 2.6.6
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[+] option: targeting BSSID 80:14:A8:00:00:00
[!] Conflicting processes: NetworkManager (PID 661), wpa_supplicant (PID 1911)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

[+] Using wlan0 already in monitor mode

[+] Scanning. Found 0 target(s), 0 client(s). Ctrl+C when ready
[+] found target 80:14:A8:00:00:00 (Syrotech)

[+] (1/1) Starting attacks against 80:14:A8:00:00:00 (Syrotech)
[+] Syrotech (58db) WPS Pixie-Dust: [--3s] Failed: Timeout after 300 seconds
[+] Syrotech (58db) WPS NULL PIN: [--3s] Failed: Timeout after 300 seconds
[+] Syrotech (56db) WPS PIN Attack: [19m14s PINs:1] Failed: Reaver process stopped (exit code: 1)
[+] Syrotech (48db) PMKID CAPTURE: Failed to capture PMKID

[+] Syrotech (60db) WPA Handshake capture: Discovered new client: C8:09:A8:D9:07:CE
[+] Syrotech (28db) WPA Handshake capture: Listening. (clients:1, deauth:11s, timeout:0s)
[!] WPA handshake capture FAILED: Timed out after 300 seconds
[+] Finished attacking 1 target(s). exiting
```

Figure– Sensitive Information revealed

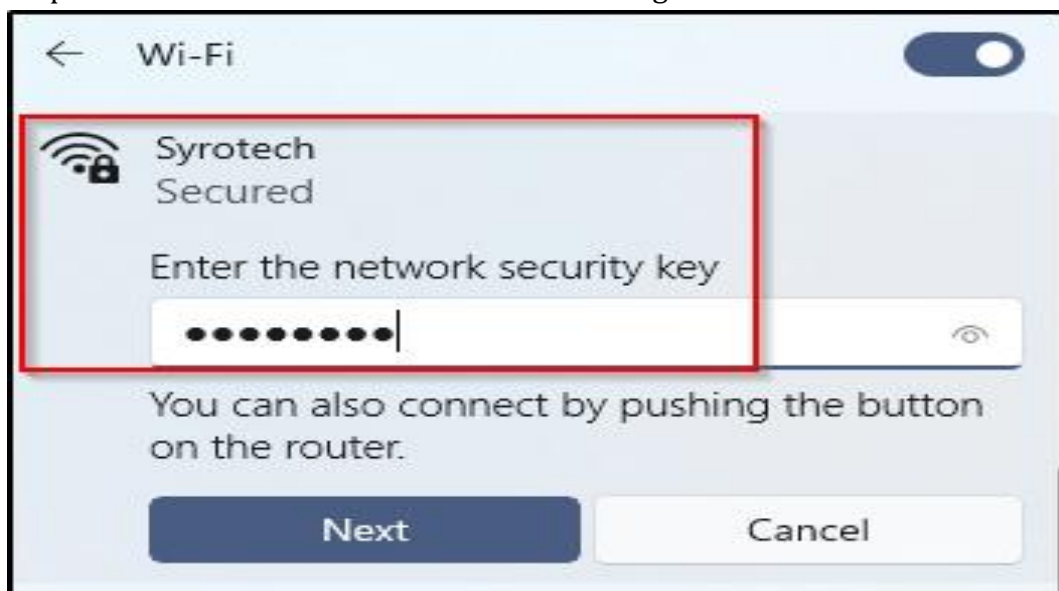
11.2 Test Case Number: 02

11.2.1. **Test Case Name:** Verify that the DUT does not provide the reason for failure while incorrect login attempts on SSID.

11.2.2. **Test Case Description:** Ensure that the DUT does not disclose the cause of failure during unauthorized login attempts on the SSID.

11.2.3. Execution Steps:

- i. Enter incorrect SSID credentials (ex. password) and ensure that the DUT does not provide the reason of failure – as shown in figure



- ii. DUT reveals the reason behind failure to connect WI-FI.



11.3 Test Case Number: 03

- 11.3.1. Test Case Name: Verify that the option to hide/unhide option is available in the DUT.
- 11.3.2. Test Case Description: To ensure there is option to hide / unhide SSID on user selection as is an essential feature on the DUT Execution
- 11.3.3. Execution Steps:
 - i. Launch the tool wifite in terminal and enter the following command to scan the network and ensure that the SSID is "not hidden". – as shown in figure

```
[*] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[*] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools
[*] Conflicting processes: NetworkManager (PID 659), wpa_supplicant (PID 637394)
[*] If you have problems: kill -9 PID or re-run wifite with --kill

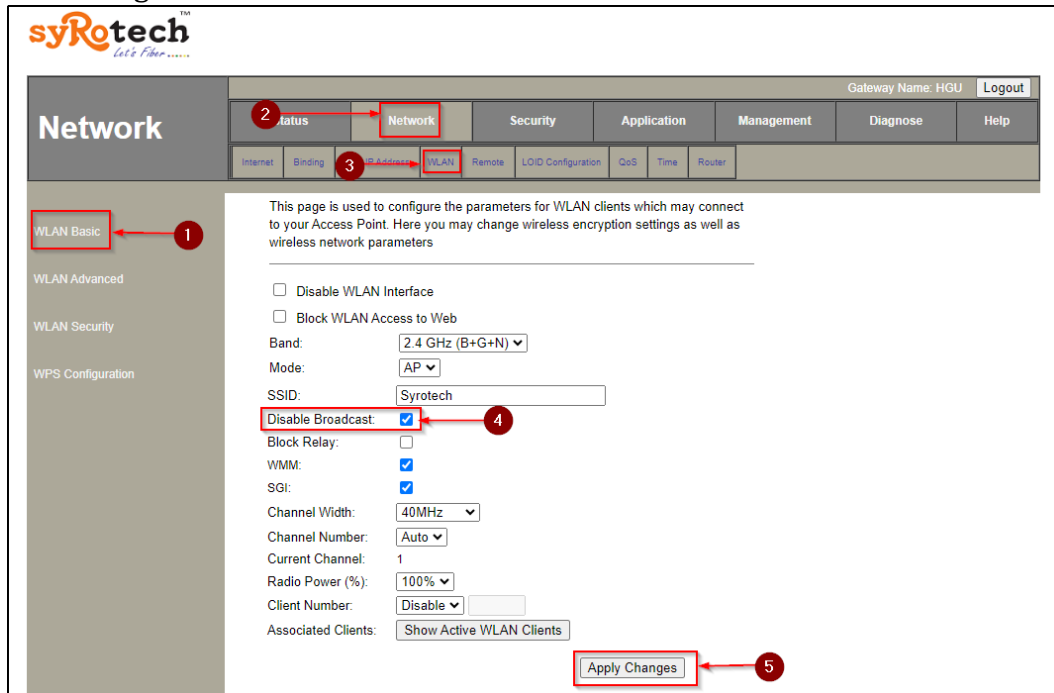
[+] Using wlan0mon already in monitor mode
```

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENT
1	(AC:84:C6:E2:65:54)	5	WPA	99db	no	
2	DIGISOL	8	WPA-P	62db	no	
3	LabNet-24	1	WPA-P	38db	no	2
4	DELTAPHI24	11	WPA-P	38db	no	10
5	Deltaphi Guest	11	WPA-P	38db	no	1
6	Syrotech	4	WPA-P	38db	no	
7	MikroTik-66BD71	1	WPA-P	24db	yes	
8	EEIPL A	1	WPA-P	21db	yes	
9	DIGISOL	9	WPA-P	17db	no	
10	Airtel_Zerotouch	2	WPA-P	17db	no	
11	SARA MOBILE	11	WPA-P	13db	no	
12	SARA PRIVATE	11	WPA-P	12db	no	
13	SARA CONF	11	WPA-P	12db	no	
14	SUNIL K	3	WPA-P	9db	yes	
15	SARA PRIVATE	11	WPA-P	9db	no	
16	Airtel_SUNIL K2	11	WPA-P	9db	yes	
17	SARA MOBILE	11	WPA-P	9db	no	
18	SARA CONF	11	WPA-P	8db	no	

```
[+] Select target(s) (1-18) separated by commas, dashes or all: █
```

Figure– Result of wifite tool scan.

- ii. To log into the web interface of the DUT, open a web browser and enter the default gateway address (http://192.168.1.1) in the address bar. Then, enter the username **admin** and password **Delta@00** in the login dialog box.
- iii. To hide SSID of the DUT Navigate to Network > WLAN > On WLAN Basic Tick mark the **disabled Broadcast** option and click on apply change to save the changes in the DUT.



- iv. Launch the tool wifite in terminal and enter the following command to scan the network and ensure that the SSID is “hidden” – as shown in figure “wifite --clients-only”

```
(root@kali)-[/home/kali]
# wifite --clients-only

wifite2 2.6.6
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[+] option: ignoring targets that do not have associated clients
[!] Conflicting processes: NetworkManager (PID 661), wpa_supplicant (PID 1911)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

[+] Using wlan0 already in monitor mode
```

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENT
1	Deltaphi_Guest	10	WPA-P	38db	no	1
2	DELTA PHI24	10	WPA-P	38db	no	11
3	RelifeMS-2	10	WPA-P	28db	yes	4
4	NG MEADOWS	5	WPA-P	15db	yes	2

```
[+] Scanning. Found 4 target(s), 18 client(s). Ctrl+C when ready
```

Figure Result of wifite tool scan.

11.3.4. Test Observations:

- i. TC 01: We observed that the DUT does not disclose any sensitive information, PIN details on SSID scan/ attack techniques.

- ii. TC 02: We observed by passing on the wrong credentials DUT reveals the reason behind failure to connect WI-FI.
- iii. TC 03: We observed that on the CPE there is a feature to hide and unhide the SSID.

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL (Please see Note Below)
1	Verify that the DUT does not disclose any sensitive information, PIN details on SSID scan/ attack techniques	Pass
2	Feature to hide /unhide the SSID.	Pass
3	The unsuccessful attempt to SSID disclose any information or not.	Fail

2.13.7 TSTP for Password Change for User Facility

Optical Network Terminal (ONT)- PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.7
--	--------------------------	------------------

<DUT Details: >

<DUT Software Version:>

<Digest Hash of OS> Hash of DUT OS is required

<Digest Hash of Configuration> Hash of DUT configuration is required

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT)-PON family Broadband Equipment- V1.0.1

<ITSAR Version No:> ITSAR403012311 and Version: 1.0.1

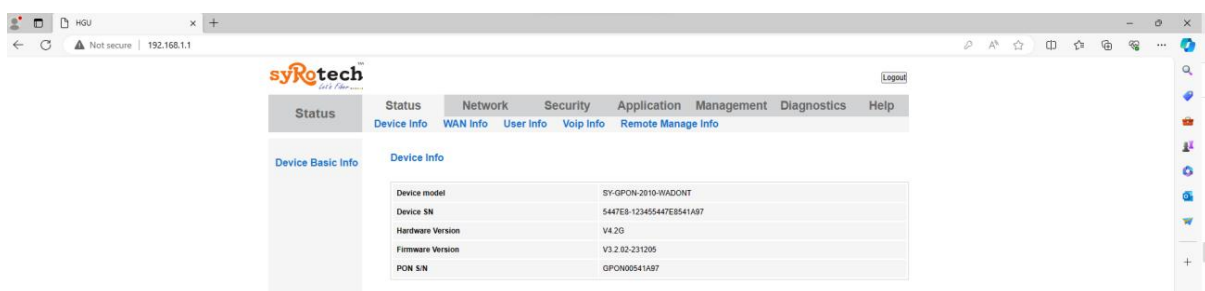
<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. <ITSAR Section No & Name> Section 13: Specific Requirement

2. <Security Requirement No & Name > 2.13.7 Password Change for User Facility

3. <Requirement Description:> 1st Installation /Factory Reset ONT/ONU shall change of authentication attribute (eg: - password) on 1st installation configuration or on factory reset conditions. If a password is used as an authentication attribute, then the ONT shall provide a function that facilitates the user to change his password at any time. However, the ONT shall not allow the previously used passwords up to a certain number (Password History).

4. DUT Confirmation Details:



5. **DUT Configuration:** - No additional configuration required to meet the clause requirement.

6. Preconditions

- OEM shall provide documentation which describes that DUT enforce password change on 1st installation.
- OEM shall provide documentation which describes that DUT provide a function that facilitates the user to change his password at any time.

- iii) OEM shall provide confirmation that DUT shall not allow the previously used passwords up to a certain number (Password History).

7. Test Objective: To verify the change of authentication attribute on 1st installation/factory reset.

8. Test Plan

8.1. Number of Test Scenarios

8.1.1 The Tester verify that the DUT allow user to change his password at any time.

- i. The Tester verify that DUT enforce password change after initial login.
- ii. The Tester verify that DUT enforce password change based on password management policy.
- iii. The Tester configures the limit of previously used passwords (Password History) on DUT as per criteria mentioned in ITSAR requirement.
- iv. The Tester verify that limit of previously used password is working or not. (Positive and Negative scenarios).

8.2. Test Bed Diagram



8.3. Tools Required: CLI/GUI Interface of DUT

8.4. Test Execution Steps:

- i. Factory Reset the DUT
- ii. Post Reset Verify if the DUT enforces password change
- iii. Access te DUT with updated credentials.
- iv. Attempt to change the Password again
- v. Set previously used password which exists in configured password history.

9. Expected Results: DUT should be able to change the authentication attribute on 1st installation/factory reset.

10. Expected Form of Evidence: Output screenshots.

11. Test Execution

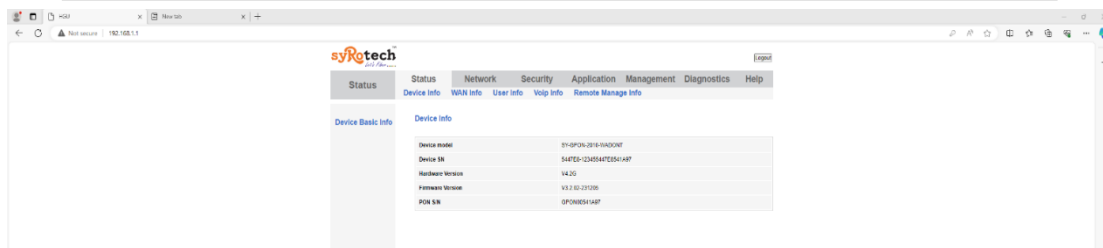
11.1 Test Case Number: 01

11.1.1 Test Case Name: change_password_any_time.

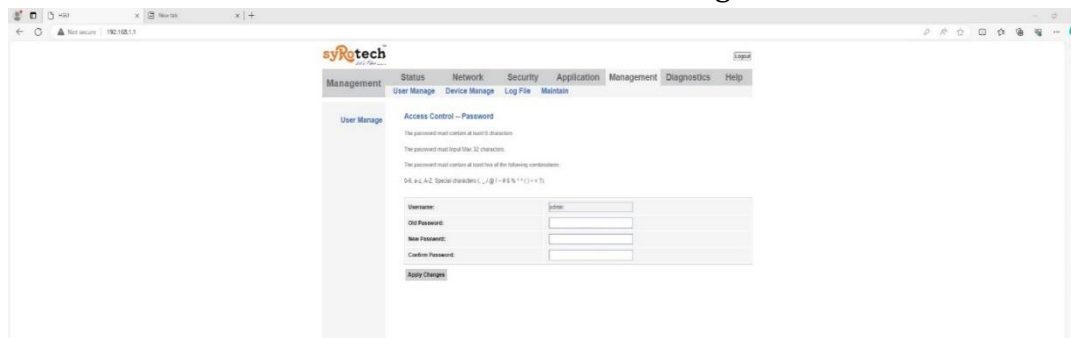
11.1.2 Test Case Description: The Tester verify that the DUT allow user to change his password at any time.

11.1.3 Execution Steps:

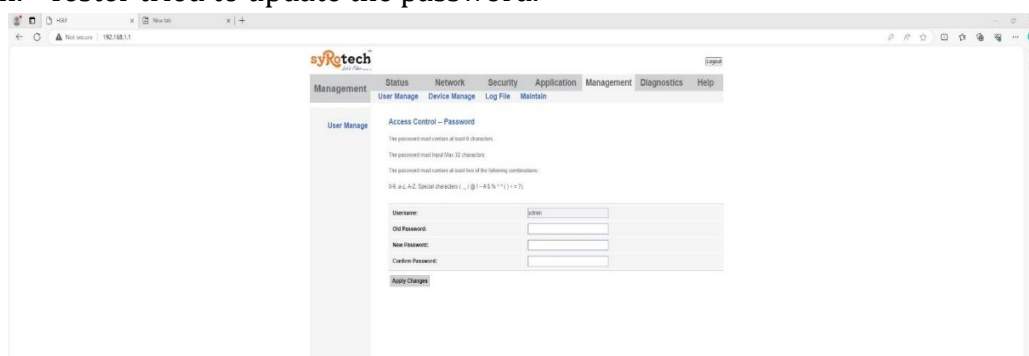
- i. The tester login the DUT's Web GUI (192.168.1.1) in web browser of the test machine (192.168.1.101) account "admin" with using the respective authentication attribute (Syro@43210\$) through Web Interface.



- ii. The tester clicks on Administration > User Management.



- iii. Tester tried to update the password.





ii. The Tester observed DUT have enforced password change after initial login.

11.2.4 Test Observation: The Tester observed DUT have enforced password change after initial login.

11.2.5 Evidence Provided: Screenshots are attached above

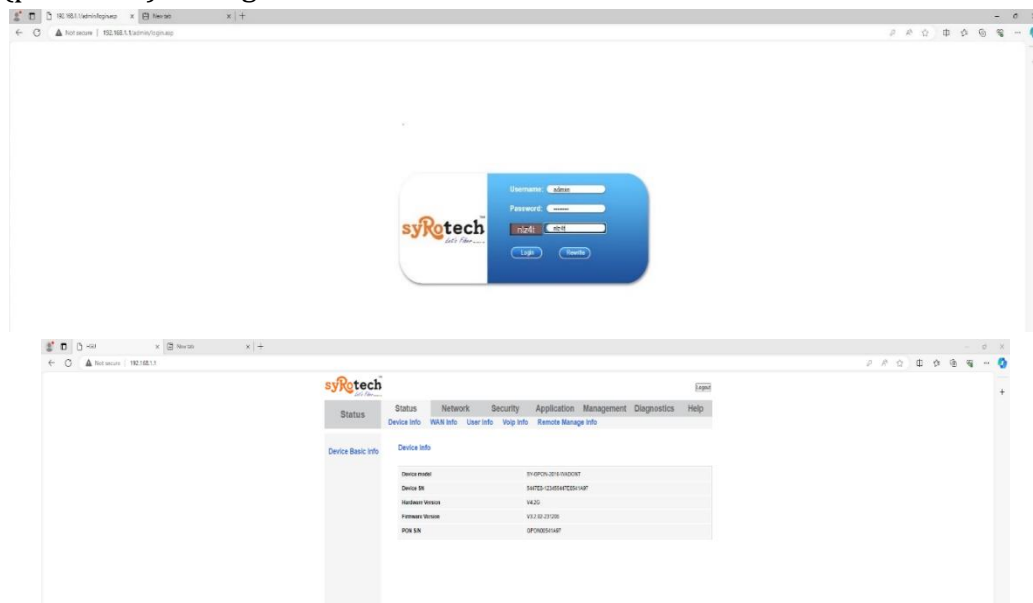
11.3 Test Case Number: 03

11.3.1 Test Case Name: password_change_management_policy.

11.3.2 Test Case Description: The Tester verify that DUT enforce password change based on password management policy.

11.3.3 Execution Steps:

- The tester login the DUT's Web GUI (192.168.1.1) in web browser of the test machine (192.168.1.101) account "admin" with using the respective authentication attribute (password) through Web Interface.

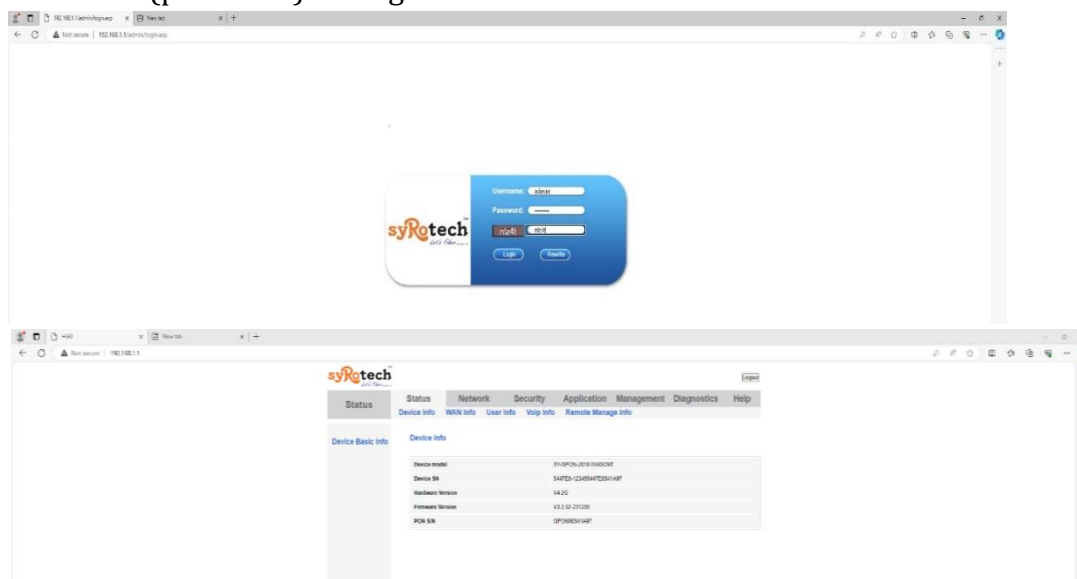


-
- The screenshot shows the Ayretech User Management interface. The navigation menu includes 'Management', 'Status', 'Network', 'Security', 'Application', 'Management', 'Diagnostics', and 'Help'. The 'User Manage' section is active, displaying the 'Access Control - Password' settings. The password requirements are listed as follows:
- The password must contain at least 8 characters.
 - The password must contain Min 32 characters.
 - The password must contain at least two of the following combinations:
 - 0-9 a-z A-Z Special characters (, / @ ! % * ' ") ~ -
- The form includes fields for 'Username', 'Old Password', 'New Password', and 'Confirm Password', each with a corresponding password strength indicator. The 'Add/Change' button is located at the bottom of the form.

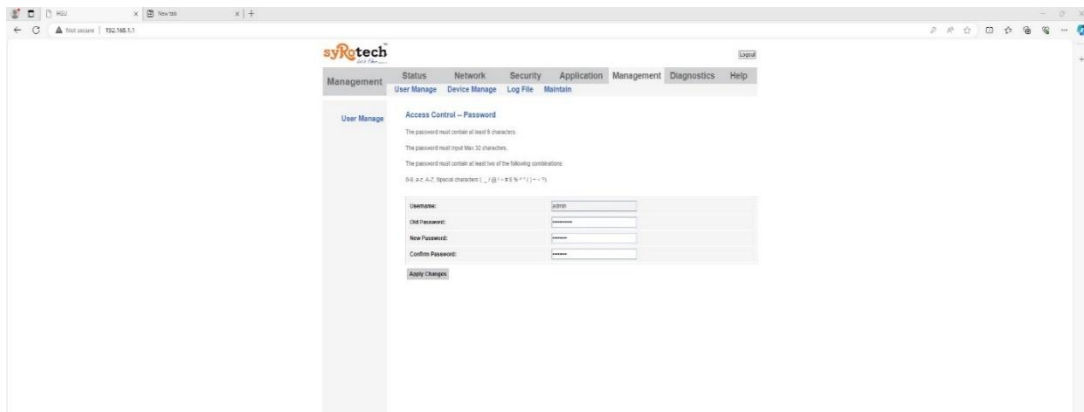
- #### 1.4 Test Case Number: 04

- 11.4.2. Test Case Description:** The Tester configures the limit of previously used passwords (Password History) on DUT as per criteria mentioned in ITSAR requirement.

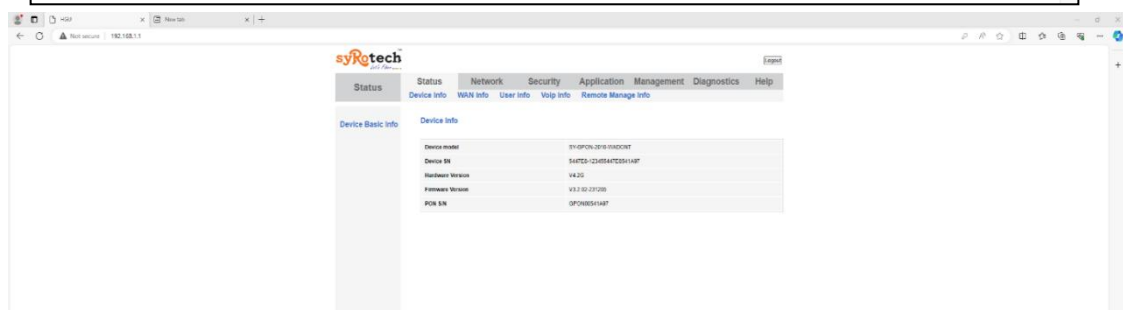
- i. The tester login the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) account "admin" with using the respective authentication attribute(password) through Web Interface.



- 525



- iii. The Tester observed during password change that DUT doesn't have feature to configure the limit of previously used passwords (Password History).
- iv. Tester set/updated the password "Syro@43210\$" and tried to login the DUT again.
- v. Tester didn't see any password history while changing the password.



- vi. Tester successfully logged in the DUT.

11.4.4. Test Observation: The Tester observed during password change that DUT doesn't have feature to configure the limit of previously used passwords (Password History).

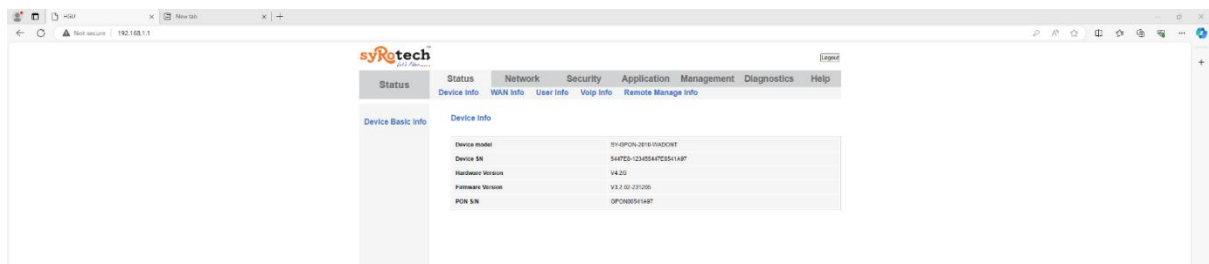
11.5 Test Case Number: 05

11.5.1 Test Case Name: password history

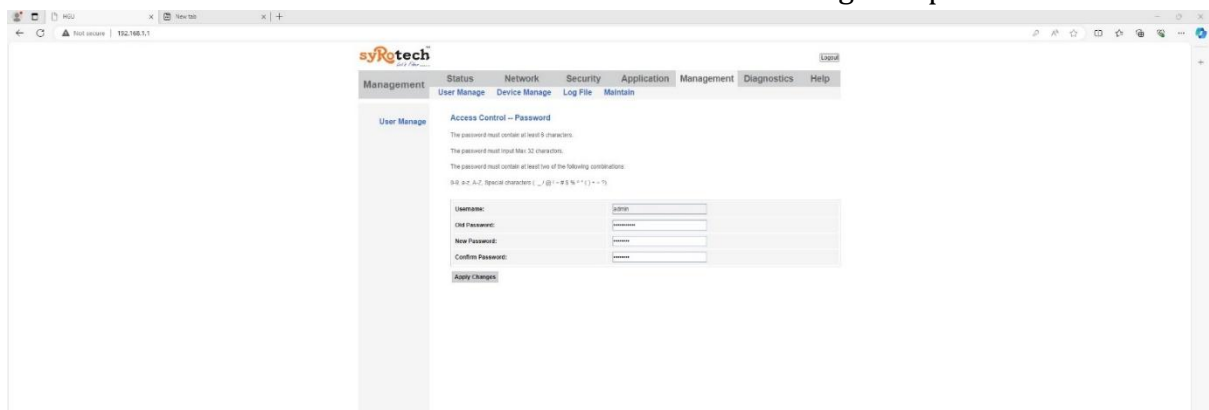
11.5.2 Test Case Description: The Tester verify that limit of previously used password is working or not. (Positive and Negative scenarios).

11.5.3 Execution Steps:

- i. The tester login the DUT's Web GUI (<http://192.168.1.1>) in web browser of the test machine (192.168.1.22) account "admin" with using the respective authentication attribute(password) through Web Interface.

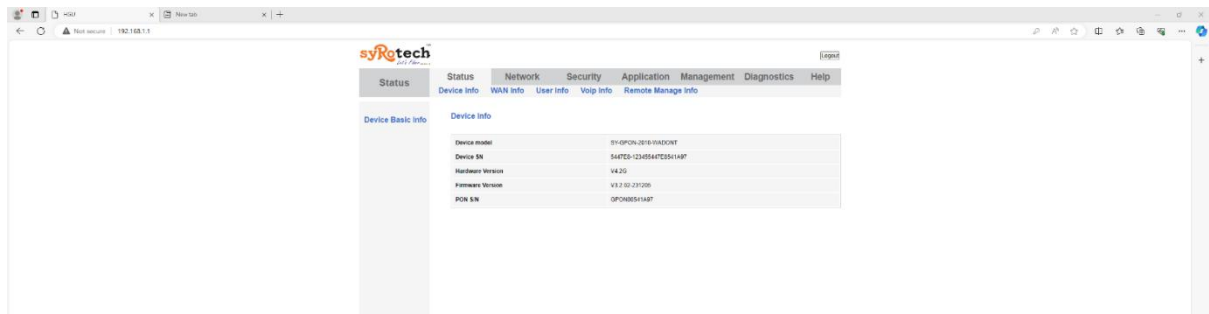


- ii. The Tester observed that DUT can allow user to change the password



- iii. The Tester observed during password change that DUT doesn't have feature to configure the limit of previously used passwords (Password History).
- iv. Tester set/updated the password "Syro@43210\$" and tried to login the DUT again.





- v. The Tester observed during password change that DUT doesn't have feature to configure the limit of previously used passwords (Password History).

11.5.4 Test Observation: The Tester observed during password change that DUT doesn't have feature to configure the limit of previously used passwords (Password History).

12. Test Case Results

Sl. No	TEST CASS NAME	PASS/FAIL	Remarks
1			

2.13.8 TSTP for Evaluation of Key exchange mechanism

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.8
---	--------------------------	------------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF
DOCA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

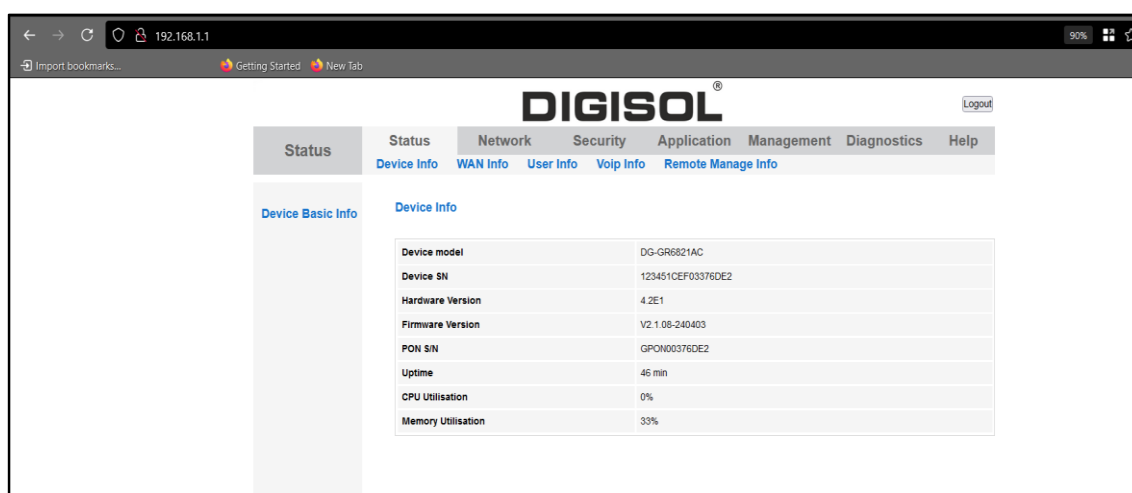
1. **<ITSAR Section No & Name>** Section 13 Specific Requirement
2. **<Security Requirement No & Name >** 2.13.8 Key exchange mechanism
3. **<Requirement Description: >** The data encryption between the OLT and ONT shall use Secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR).

The keys generated during this process must be unpredictable.

4. DUT Confirmation Details:

- i. Use the command line/GUI interface to get details of the machine on which test is conducted.
- ii. Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT

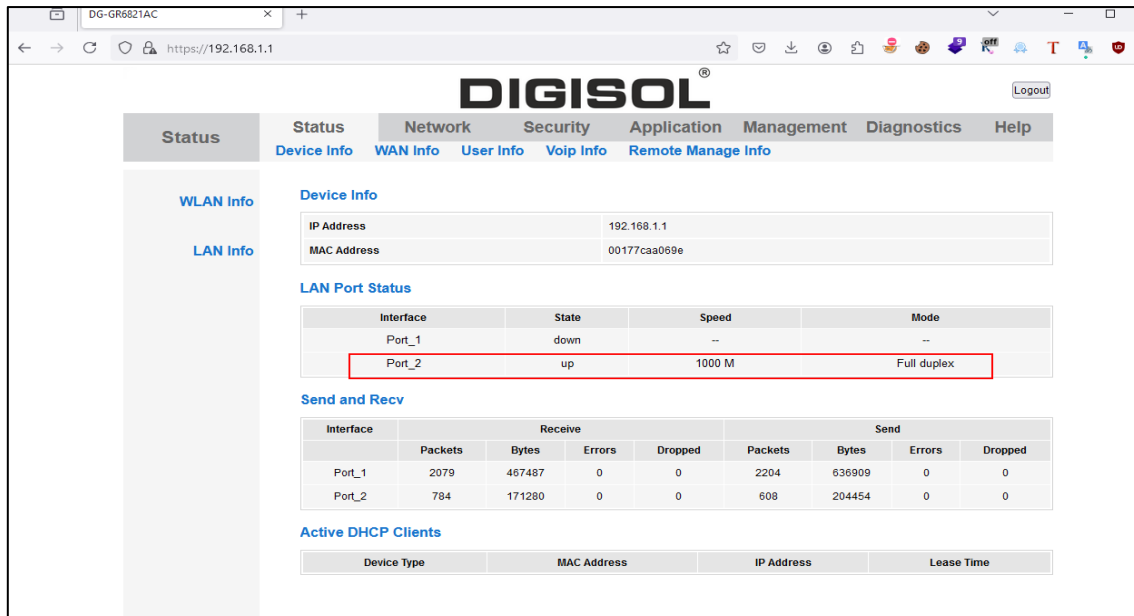




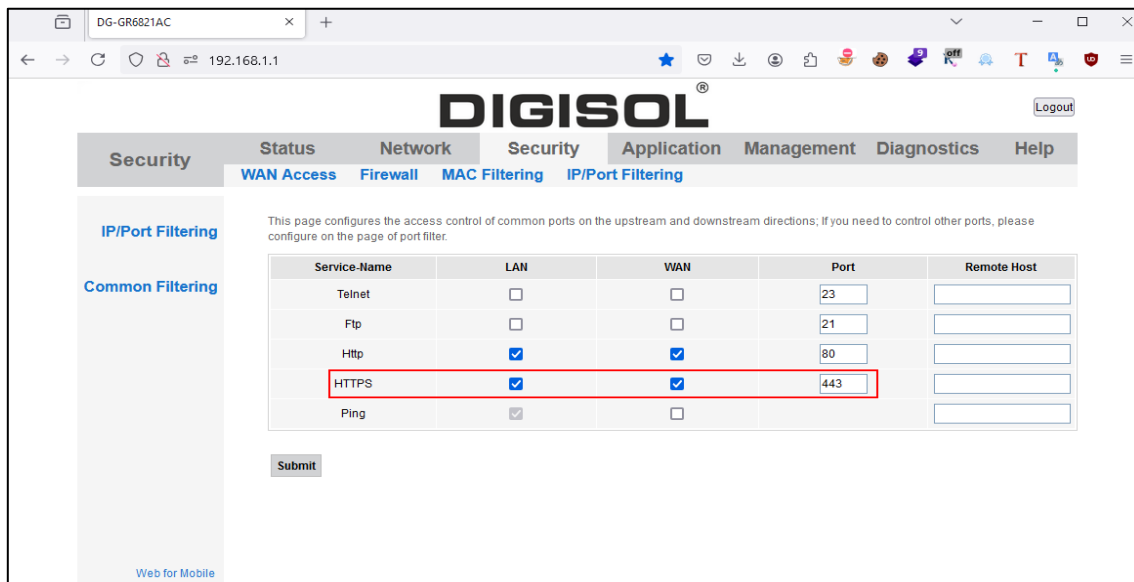
Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

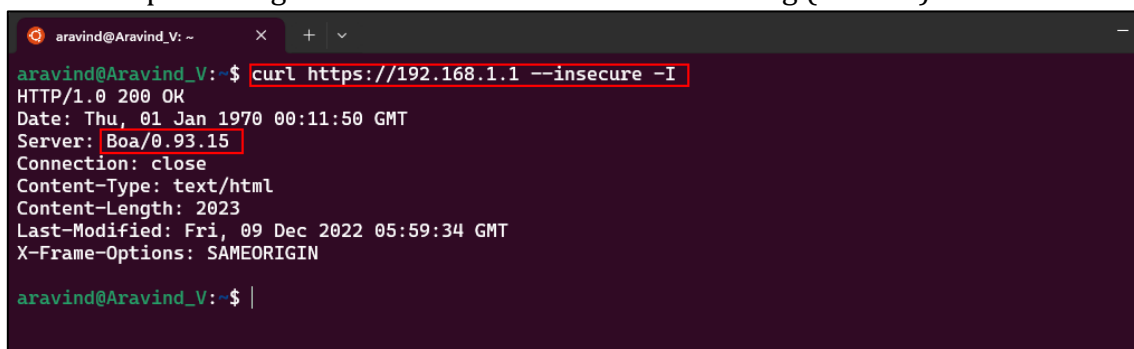
- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.



ii. HTTPS is enabled.



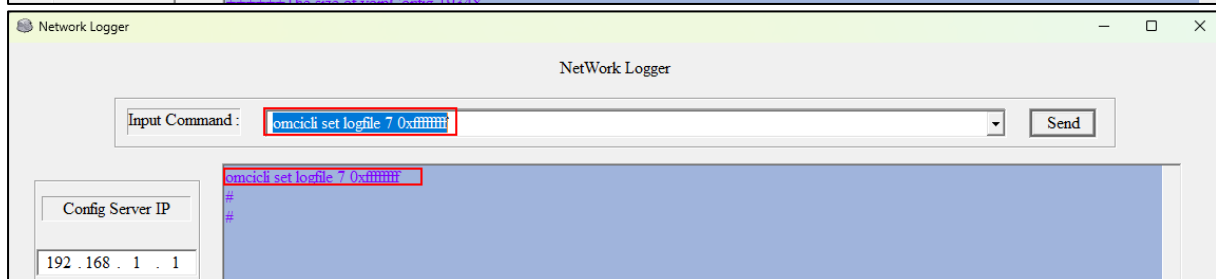
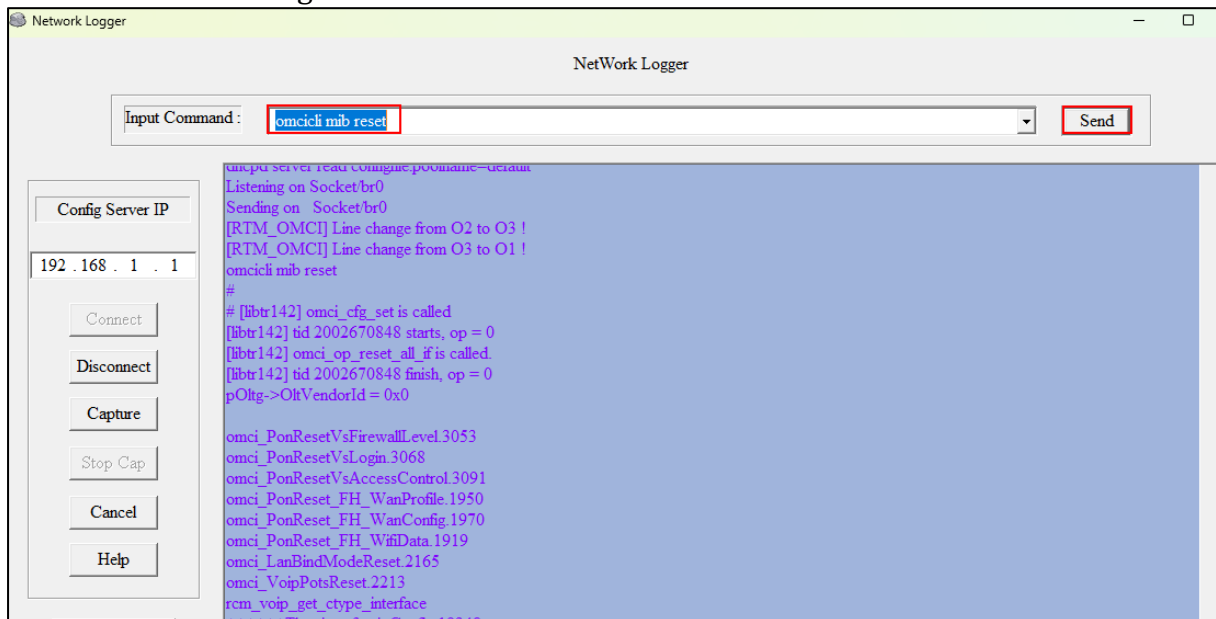
iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.



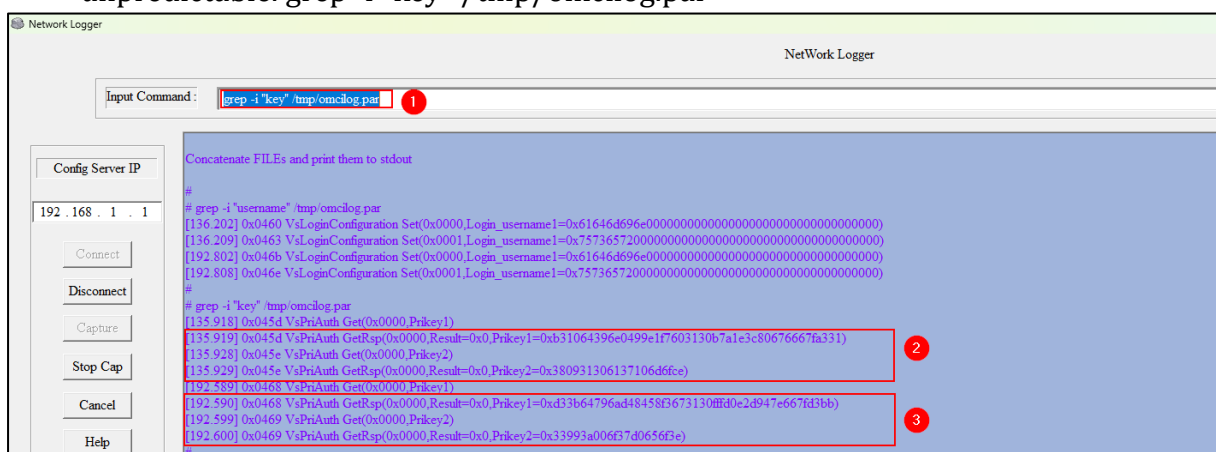
iv. Connect ONT to PC, open the **network logger** application and verify is connected – enter the following command

- admin
- admin123
- enterlinuxshell

- `omcicli mib reset`
- `omcicli set logfile 7 0xffffffff`



- vi. Then physically connect the ONU to the OLT over PON2 port and grep the OMCI log key.
- vii. Then verify the OMCI logs, keys generated during this process must be unpredictable. `grep -i "key" /tmp/omcilog.par`



6. **Precondition:** OEM document regarding key generation (OMCI log) in the DUT.

7. Test Objective: To verify that data encryption between the OLT and DUT(ONT) shall use Secure cryptographic controls prescribed in Table1 of the latest document of

“Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) and the keys generated during this process must be unpredictable.

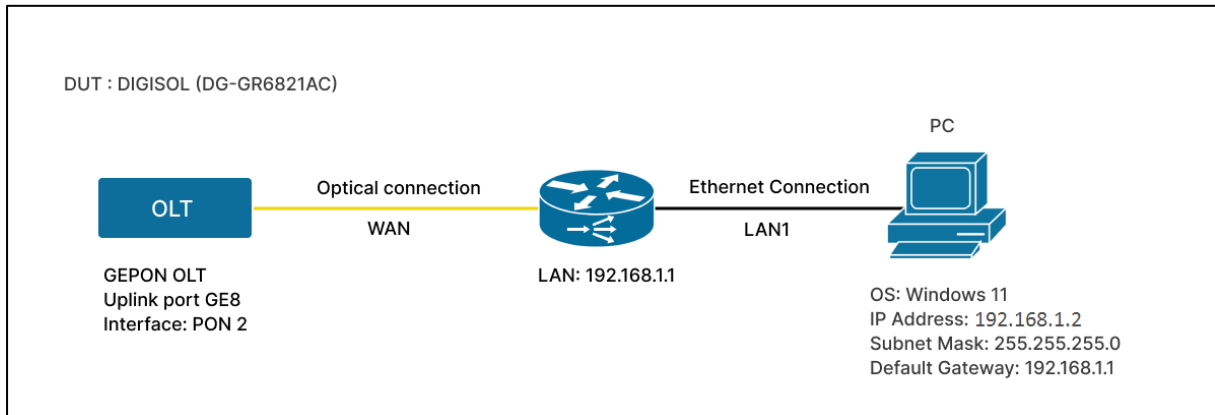
8. Test Plan:

8.1 Number of Test Case Scenarios: 2

8.1.1 To verify that the data encryption between the OLT and DUT(ONT) shall use secure cryptographic controls.

8.1.2 To verify the keys generated during this process must be unpredictable.

8.2 Test Setup Diagram



8.3 Tools Used: - Web browser (For access GUI of DUT), Network logger

8.4 Test Execution Steps

- a. To verify that the data encryption between the OLT and ONT shall use secure cryptographic controls.
 - i. Then verify the OMCI logs, data encryption between the OLT and ONT shall use secure cryptographic controls.
`grep -i "key" /tmp/omcilog.par`
- b. To verify keys generated during this process must be unpredictable.
 - i. To capture the traffic (data encryption) between ONT and OLT, enable and start the OMCI logs.
 - ii. To log into the web interface of the OLT, open a web browser and enter the default gateway address (192.168.8.100) in the address bar. Then, enter the username **admin** and password **Xpon@Olt9417#** in the login dialog box.
 - iii. Physically connect the ONU to the OLT over PON port.
 - iv. To check the connection status, navigate to ONU configuration > ONU list > set Port ID as PON2 > Refresh. By default, the authentication is disabled, and connection is established without any key exchanges for authentication.
 - v. To enforce authentication between OLT and ONU for registration, log into the web interface of the ONT, open a web browser and enter the default gateway address (**192.168.1.1**) in the address bar. Then, enter the username **admin** and password **admin123** in the login dialog box.
 - vi. Navigate to Network > LOID register.
 - vii. To create a new LOID, provide the LOID name as **Deltaphi** and password as **admin123**.
 - viii. To add a LOID in the OLT, navigate to ONU configuration > Authentication > LOID List.

ix. **Port ID: PON2**

x. **LOID: Deltaphi**

xi. **Password: admin123**

xii. Navigate to ONU configuration > Authentication > Authentication mode.

xiii. Set Auth Mode: for **PON2** as **LOID** and submit – as shown in figure

xiv. To verify if the registration of the ONU is done with the ONT (post enforcing authentication) and check the connection status in the OLT, navigate to ONU configuration > ONU list > set Port ID as PON2 > Refresh.

xv. Analyse the OMCI logs, keys generated during this process must be unpredictable – run the following command.

xvi. To verify random key generation, connect and disconnect three times ONT to OLT and check in OMCI log.

9. **Expected Results for Pass:** Communication between ONT and OLT should be encrypted as per crypto control ITSAR Generated key should not be predictable

10. **Expected Format of Evidence:** - Screenshots of GUI, log

11. Test Execution:

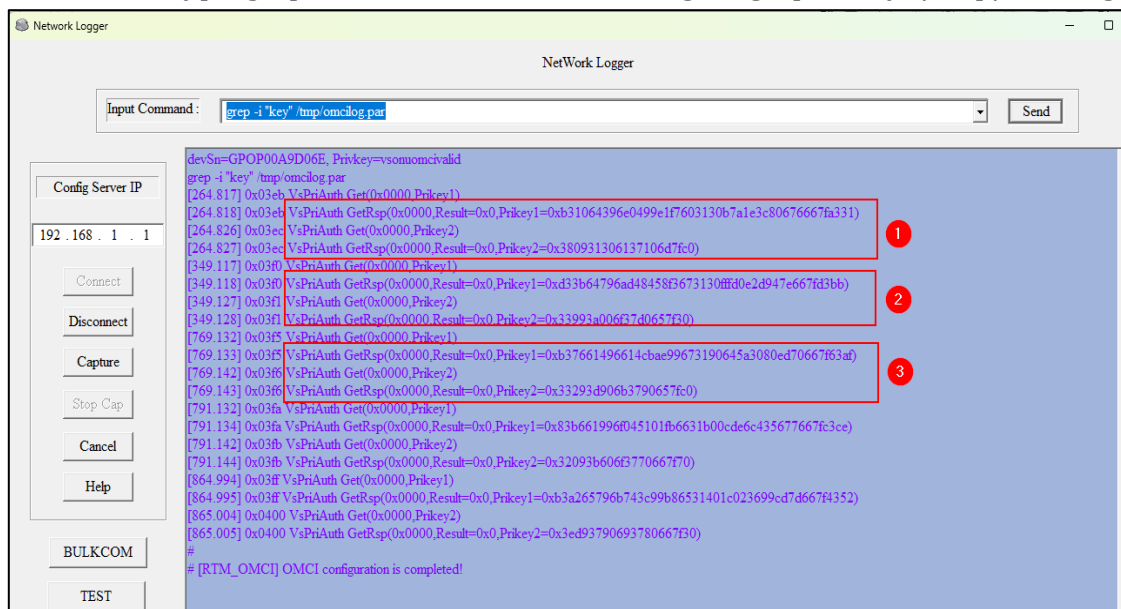
11.1 Test Case Number: 01

11.1.1 Test Case Name: 8.1.1

11.1.2 Test Case Description: The tester verifies that the data encryption between the OLT and ONT shall use secure cryptographic controls.

11.1.3 Execution Steps:

i. Then verify the OMCI logs, data encryption between the OLT and ONT shall use secure cryptographic controls – as shown in figure `grep -i "key" /tmp/omcilog.par`



11.1.4 Test **Observation:** Communication between DUT(ONT) and OLT keys are encrypted

11.2 Test Case Number: 02

11.2.1 Test Case Name: 8.1.2

11.2.2 Test Case Description: Verify that the code signing certificate associated with the upgrade package is valid and not expired.

11.2.3 Execution Steps:

- To capture the traffic (data encryption) between ONT and OLT, enable and start the OMCI logs in the OLT.
- To log into the web interface of the OLT, open a web browser and enter the default gateway address (192.168.8.100) in the address bar. Then, enter the username admin and password Xpon@Olt9417# in the login dialog box.
- Physically connect the ONU to the OLT over PON port.
- To check the connection status, navigate to ONU configuration > ONU list > set Port ID as PON2 > Refresh. By default, the authentication mode is disabled, and connection is established without any key exchanges for authentication – as shown in figure

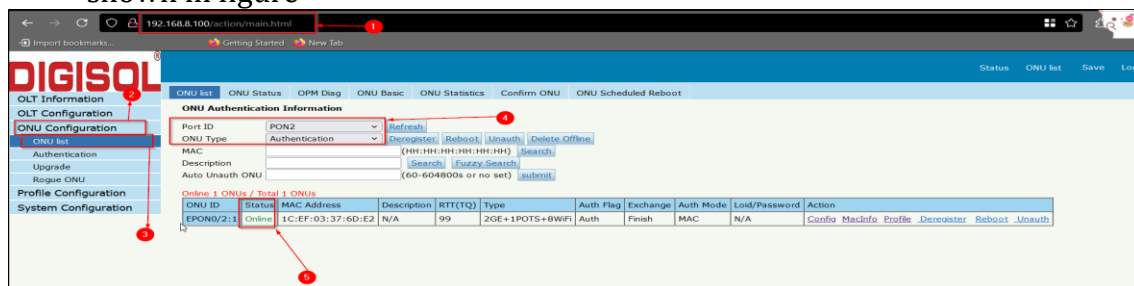


Figure No. Check ONT-ONU connection status.

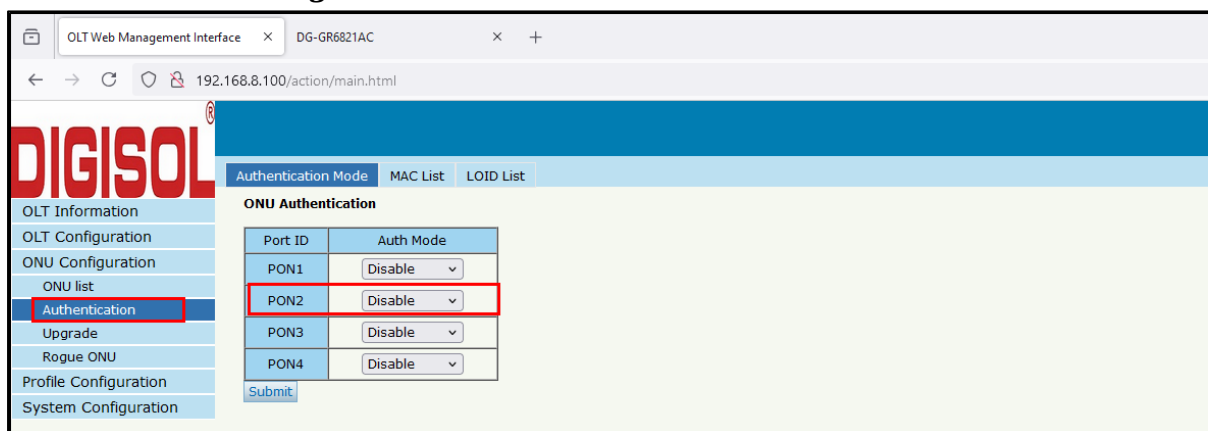


Figure No. Check ONT-ONU default authentication state for PON.

- To enforce authentication between OLT and ONU for registration, log into the web interface of the ONT, open a web browser and enter the default gateway address (192.168.1.1) in the address bar. Then, enter the username admin and password admin123 in the login dialog box.
- Navigate to Network > LOID register.
- To create a new LOID, provide the LOID name as **Deltaphi** and password as **admin123**. – as shown in figure

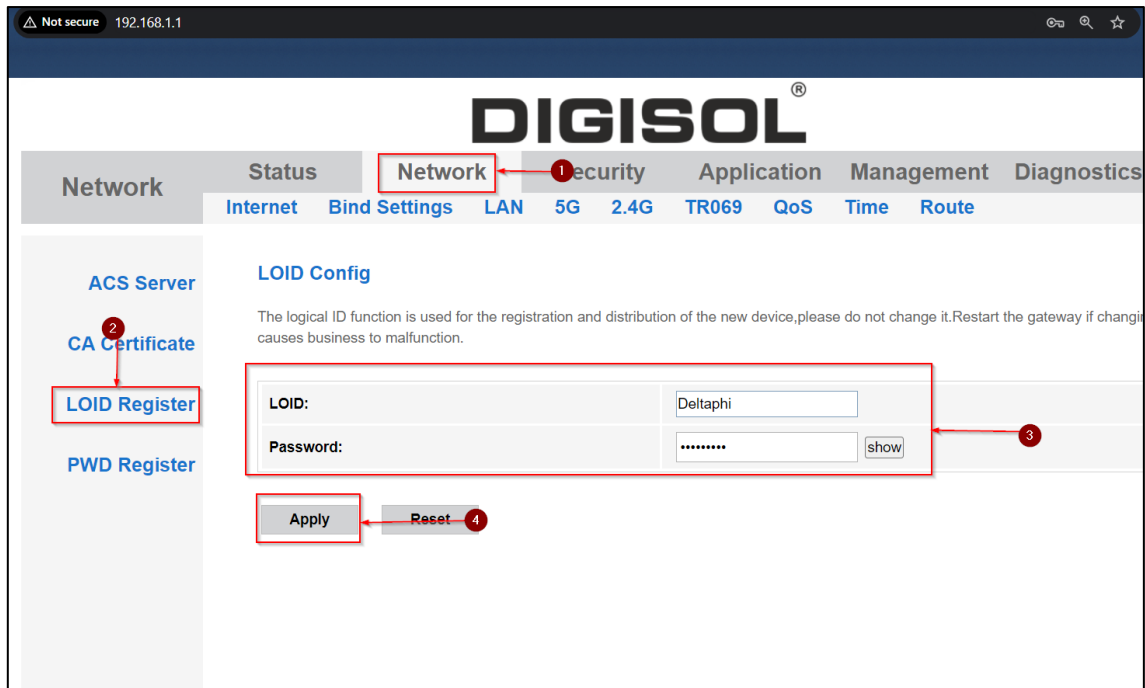


Figure No. Configuring LOID and password for ONT

1. To add a LOID in the OLT, navigate to ONU configuration > Authentication > LOID List. – as shown in figure

- **Port ID: PON2**
- **LOID: Deltaphi**
- **Password: admin@123**

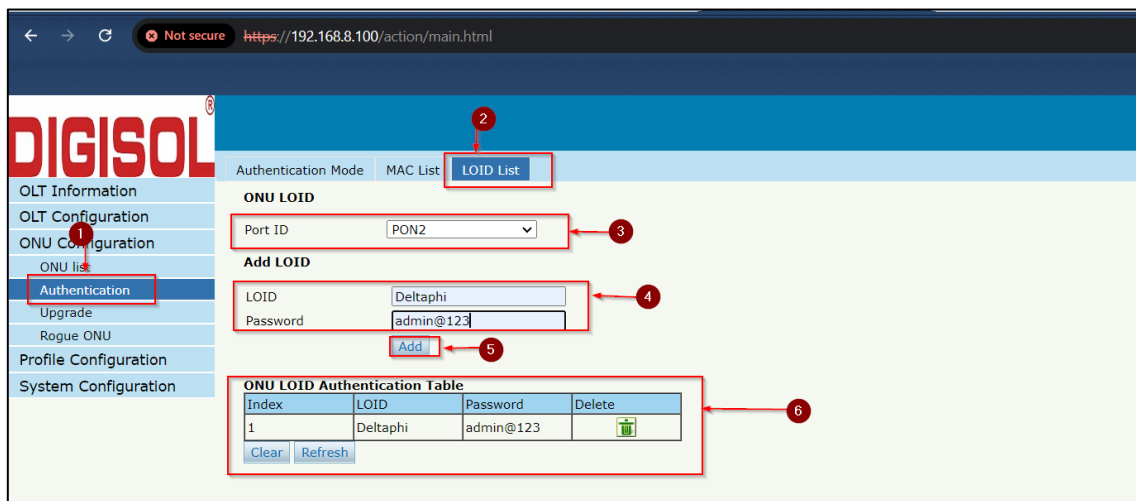


Figure No.: Setting LOID details for OLT

2. Navigate to ONU configuration > Authentication > Authentication mode.

- **Set Auth Mode: for PON2 as LOID** and submit – as shown in figure

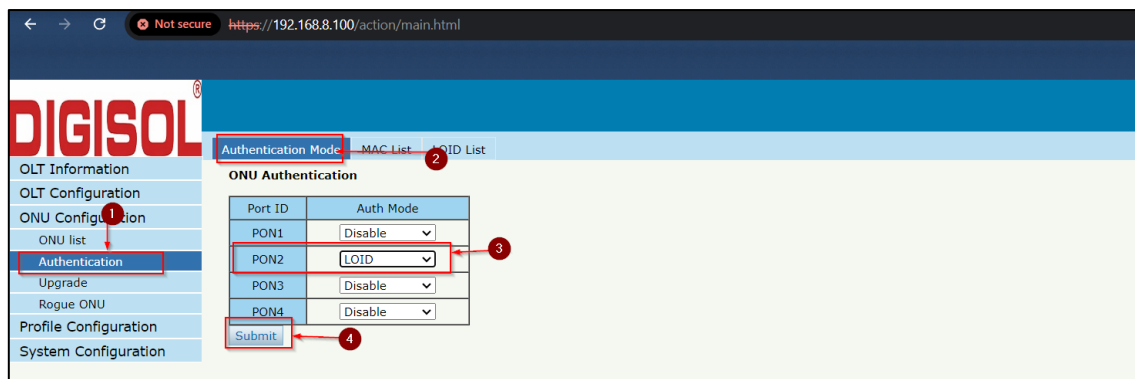


Figure No.: Set Authentication mode to LOID.

3. To verify if the registration of the ONU is done with the ONT (post enforcing authentication) and check the connection status in the OLT, navigate to ONU configuration > ONU list > set Port ID as PON2 > Refresh, remove the Optical cable and connect again 2 time – as shown in figure

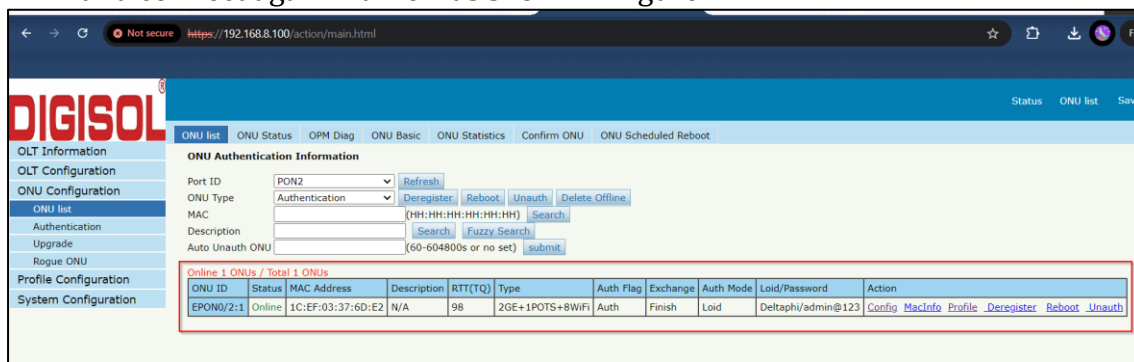


Figure No. Check ONT-ONU connection status.

4. Analyse the OMCI logs, keys generated during this process must be unpredictable – run the following command.

```
grep -i "key" /tmp/omcilog.par
```
5. To verify random key generation, connect and disconnect three times ONT to OLT and check in OMCI log.

11.2.4 Test Observation: Comparing the three keys generated by the DUT(ONT), they are unpredictable

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		
2	8.1.2		

2.13.9 TSTP for Evaluation of of Rogue detection

Optical Network Terminal (ONT)-PON family Broadband Equipment ITSAR	ITSAR No: ITSAR403012311	Clause no:2.13.9
---	--------------------------	------------------

<DUT Details: > DIGISOL DG-GR6821AC

<DUT Software Version:> V2.1.08-240403

<Digest Hash of OS> DC5E1F822E3B838B7546D77DE8116648AAF

D0CA4F823AEAE417EA1F8D6114B8E

<Digest Hash of Configuration> xxxx

<Applicable ITSAR: > NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) - PON family Broadband Equipment

<ITSAR Version No:> 1.0.0

<OEM Supplied Document list: > All the documents provided by OEM to be listed here

1. **<ITSAR Section No & Name>** Section 13 Specific Requirement

2. **<Security Requirement No & Name >** 2.13.9 Rogue detection

3. **<Requirement Description: >** The ONU should have the capability to monitor its own behaviour and autonomously turn off the laser if a fault condition is detected. This capability would serve as a secondary measure in the event that the primary method to turn off the laser via the OLT is not possible. 1) The ONU should turn its laser off if it detects rogue behaviour in order to prevent possible harm to the PON. 2) The ONU should attempt to send a message to the OLT to indicate why the ONU is going out of service.

The ONU transmitter default state (e.g., at installation) should be in the "off" position.

This is a precaution to prevent, for example, cases where there is a failure to prevent the transmitter from being shut off, resulting in potential rogue behaviour. Reference:

ITU-T Rec, Series G Supplement 49 (02/2011) Rouge Optical Network unit (ONU)

Reference: ITU-T Rec, Series G Supplement 49 (02/2011) Rouge Optical Network unit (ONU)

4. DUT Confirmation Details:

Use the command line/GUI interface to get details of the machine on which test is conducted.

- i. Use GUI to get Application No/Version No & hardware Info

The below screenshot shows the firmware version of the DUT

←→🔍192.168.1.1

🔖Getting Started🔖New Tab

90%🌟🌟🌟

DIGISOL®

Logout

Status

StatusNetworkSecurityApplicationManagementDiagnosticsHelp

Device InfoWAN InfoUser InfoVoip InfoRemote Manage Info

Device Basic Info

Device Info

Device model	DG-GR6821AC
Device SN	123451CEF03376DE2
Hardware Version	4.2E1
Firmware Version	V2.1.08-240403
PON S/N	GPOM00376DE2
Uptime	46 min
CPU Utilisation	0%
Memory Utilisation	33%



Interfaces	No.of Ports	Interface Type	Interface Name
PON	1 Port(s)	Physical	PON
LAN	2Port(s)	Physical	LAN1, LAN2

5. DUT Configuration:

- i. The DUT is connected to LAN 2 – with the Lab's Testing Machine.

The screenshot shows the DIGISOL web interface at the URL <https://192.168.1.1>. The interface has a top navigation bar with tabs: Status, Network, Security, Application, Management, Diagnostics, and Help. Under the Status tab, there are sub-tabs: Device Info, WAN Info, User Info, Voip Info, and Remote Manage Info. The left sidebar has links for WLAN Info and LAN Info. The main content area shows the Device Info section with the following details:

IP Address	192.168.1.1
MAC Address	00177caa069e

Below this is the LAN Port Status section with a table:

Interface	State	Speed	Mode
Port_1	down	--	--
Port_2	up	1000 M	Full duplex

The Port_2 row is highlighted with a red border. Below this is the Send and Recv section with a table showing network statistics for Port_1 and Port_2. The Active DHCP Clients section is also visible at the bottom.

- ii. HTTPS is enabled.

The screenshot shows the DIGISOL web interface at the URL <https://192.168.1.1>. The interface has a top navigation bar with tabs: Status, Network, Security, Application, Management, Diagnostics, and Help. Under the Security tab, there are sub-tabs: WAN Access, Firewall, MAC Filtering, and IP/Port Filtering. The left sidebar has links for IP/Port Filtering and Common Filtering. The main content area shows the IP/Port Filtering section with a table for configuring access control:

Service-Name	LAN	WAN	Port	Remote Host
Telnet	☐	☐	23	
Ftp	☐	☐	21	
Http	☒	☒	80	
HTTPS	☒	☒	443	
Ping	☒	☐		

The HTTPS row is highlighted with a red border. Below the table is a Submit button. The bottom of the page has a link for Web for Mobile.

- iii. DUT is pre-configured with BOA as a webserver having (0.93.15) version.

```

aravind@Aravind_V: ~$ curl https://192.168.1.1 --insecure -I
HTTP/1.0 200 OK
Date: Thu, 01 Jan 1970 00:11:50 GMT
Server: Boa/0.93.15
Connection: close
Content-Type: text/html
Content-Length: 2023
Last-Modified: Fri, 09 Dec 2022 05:59:34 GMT
X-Frame-Options: SAMEORIGIN

aravind@Aravind_V: ~$

```

6. **Precondition:** The OEM should provide documentation explaining the behavior of the ONU in rogue conditions.
7. **Test Objective:** To verify that DUT have mechanism that detect rogue state(unstable) by itself.

8. Test Plan:

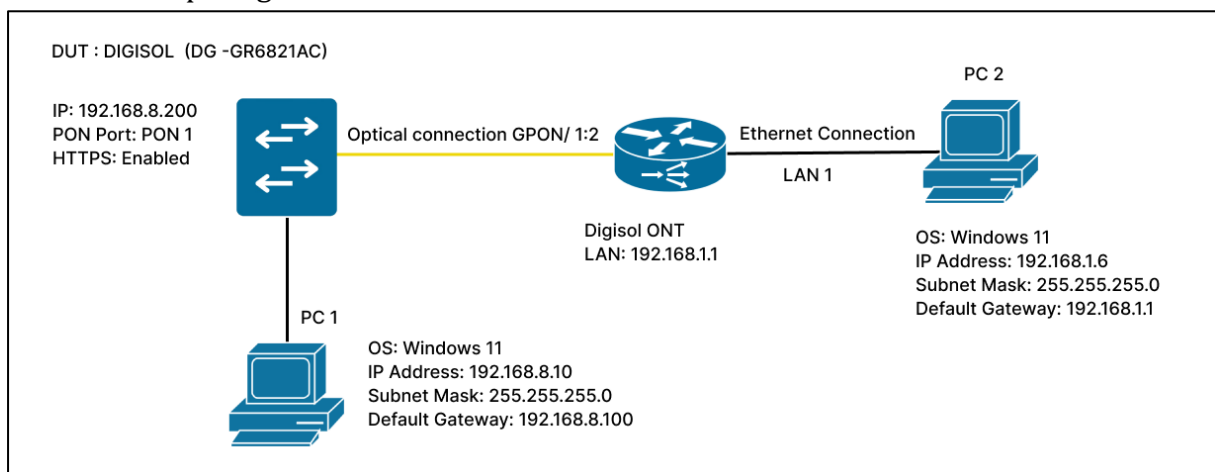
8.1 Number of Test Case Scenarios: 4

8.1.1 ONT PON port should be turn off by itself, if unstable condition (autonomously ONT) detected.

8.1.2 ONT should send alert to the OLT regarding service reachability

8.1.3 ONT transmitter should be turned off by default (factory reset)

8.2 Test Setup Diagram



8.3 Tools Used:- Web browser(For access GUI of DUT), logs

8.4 Test Execution Steps

a. Verify that ONT PON port should be turn off by itself, if unstable condition (autonomously ONT) detected.

- 1) Login to the DUT(ONT)
- 2) Forcefully turn on the laser on the connected ONT port
- 3) Check the ONT automatically turn off the laser light or not

b. ONT should send alert to the OLT regarding service reachability

- 1) Login to the DUT(ONT)
- 2) Forcefully turn on the laser on the connected ONT port

3) Check the ONT sending alert to the OLT regarding ONT unreachability

c. ONT transmitter should be turned off by default (factory reset)

- 1) Perform factory reset on the DUT(ONT)
- 2) Check the status of PON port (ON or OFF)

9. Expected Results for Pass:

- i. ONT PON port should be turn off by itself, if unstable condition detected
- ii. ONT should send alert to the OLT regarding service reachability
- iii. ONT transmitter should be turned off by default (factory reset)

10. Expected Format of Evidence: Screenshots of GUI, log

11. Test Execution:

11.1 Test Case Number: 01

11.1.1 Test Case Name: 8.1.1

11.1.2 Test Case Description: ONT PON port should be turn off by itself, if unstable condition detected

11.1.3 Execution Steps:

- i. To log into the web interface of the ONT, open a web browser
- ii. Try to forcefully turn on the PON port on the DUT
- iii. Check the DUT behavior after, either DUT turn off the PON port or not in the DUT

11.1.4 Test Observation: The testcase is "Not Tested."

11.2 Test Case Number: 02

11.2.1 Test Case Name: 8.1.2

11.2.2 Test Case Description: ONT should send alert to the OLT regarding service reachability

11.2.3 Execution Steps:

- i. To log into the web interface of the ONT, open a web browser
- ii. Forcefully turn on the laser on the connected ONT port
- iii. Check the ONT sending alert to the OLT regarding ONT unreachability

11.3 Test Case Number: 03

11.3.1. Test Case Name: 8.1.3

11.3.2. Test Case Description: ONT transmitter should be turned off by default (factory reset)

11.3.3. Execution Steps:

- i. To log into the web interface of the ONT, open a web browser
- ii. Perform factory reset on the DUT(ONT)
- iii. Check the status of PON port (ON or OFF)

12. Test Case Result:

S. No	TEST CASE NAME	PASS/FAIL	Remarks
1	8.1.1		Not tested
2	8.1.2		Not tested
3	8.1.3		Not tested