Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

Optical Line terminal (OLT) – PON family Broadband Equipment

ITSAR Number: ITSAR307072311
ITSAR Name: NCCS/ITSAR/Access Equipment/PON Access Equipments/Optical Line Terminal (OLT) - PON family Broadband Equipment

Date of Release: 24.11.2023 Version: 1.0.1
Date of Enforcement: 01.01.2026

जारीकर्ता
राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)
दूरसंचार विभाग, संचार मंत्रालय
भारत सरकार
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

Issued by
National Centre for Communication Security (NCCS)
Department of Telecommunications
Ministry of Communications
Government of India
City Telephone Exchange, SR Nagar, Bangalore-560027, India

About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. Security Assurance Standards (SAS) division of NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.

Document History

Sr. No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Optical Line terminal (OLT) - PON family	ITSAR307072209	1.0.0	26.09.2022	First release
2.	Optical Line terminal (OLT) - PON family	ITSAR307072311	1.0.1	24.11.2023	Editorial Changes

Table of Contents

Overview

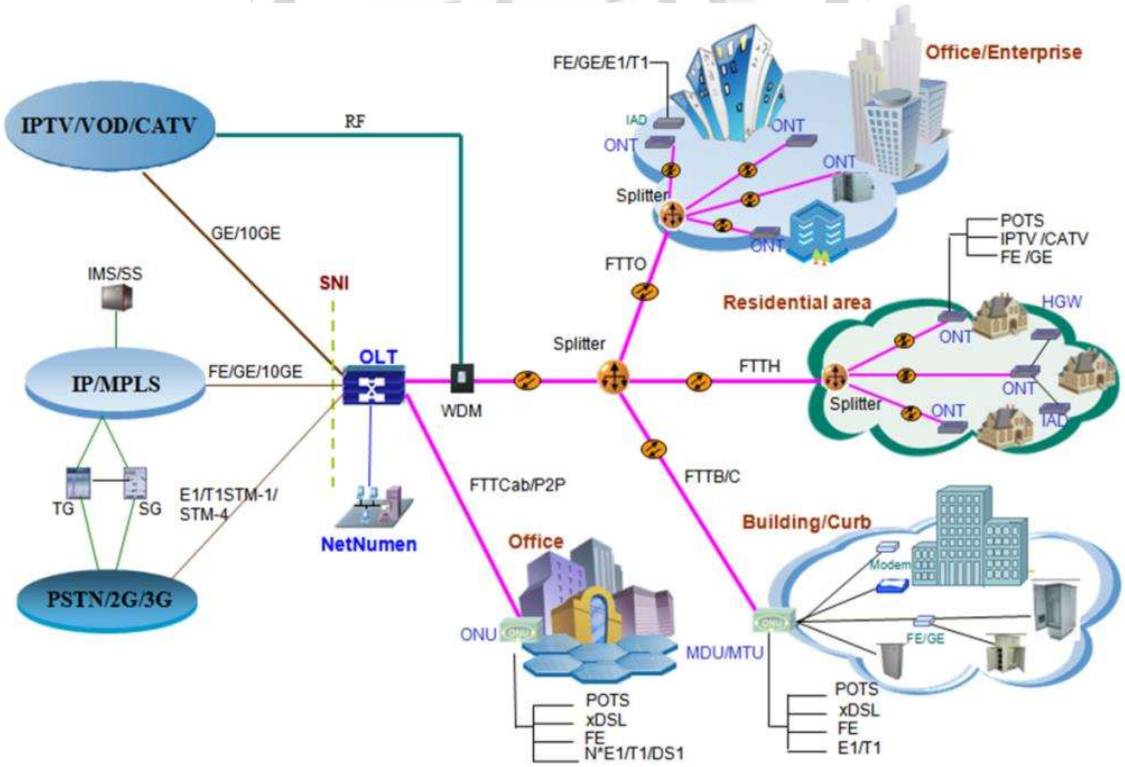
The OLT/Optical Line Terminal, also known as optical line termination, is the endpoint hardware device in a passive optical network (PON).

An OLT has two primary functions:

a) Converting the standard signals used by a FiOS service provider to the frequency and framing used by the PON system.
b) Coordinating the multiplexing between the conversion devices on the optical network terminals (ONTs) located on the customers' premises.

The OLT contains a central processing unit (CPU), passive optical network cards, a gateway router (GWR) and voice gateway (VGW) uplink cards. It can transmit a data signal to users at 1490 nanometers (nm). That signal can serve up to 128 ONTs at a range of up to 12.5 miles by using optical splitters.

As one of the indispensable components of PON, optical line terminal thus plays an essential role in the performance of the whole network connection.



Scope

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) to the stand-alone OLT (Optical Line Terminal), a passive optical network Core element with a dedicated hardware and dedicated software, which includes system software as well as application software.

Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
3. Should or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above.

Section 1: Access and Authorization

1.1 Management Protocols Mutual Authentication

Requirement:

The protocols used for the OLT 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 OLT management and maintenance.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.4.4.1

1.2 Management Traffic Protection

Requirement:

OLT 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]

1.3 Role-Based access control

Requirement:

OLT shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which determines how users interact with domains and resources. The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform i.e. the specific operation command or command group.

OLT supports Role Based Access Control (RBAC) with minimum of 3 user roles, in particular, for OAM privilege management, for OLT Management and Maintenance, including authorization of the operation for configuration data and software via the OLT console interface.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.2]

1.4 User Authentication – Local and Remote

Requirement:

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user.
Authentication attributes include

- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker. Minimum two of the above authentication attributes shall be mandatorily combined for protecting the all accounts from misuse.

Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from OLT local hardware interface.

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 V.1.0.0. Section 4.2.3.4.2.1]

1.5 Remote login restrictions for privileged users

Requirement:

Login to OLT as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to OLT remotely.

This remote root user access restriction is also applicable to application softwares / tools such as TeamViewer, desktop sharing etc which provide remote access to the OLT.

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

1.6 Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.
Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g. configuration and logging files).

Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.3.4.6.1]

1.7 Unambiguous identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the OLT.

OLT shall support assignment of individual accounts per user, where a user could be a person, or, for machine accounts, an application, or a system.
OLT shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

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

Section 2: Authentication Attribute Management

2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes in case of user accounts (e.g. password, certificate, token) and single authentication attribute in case of machine account, 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.

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

2.2 Authentication Support – External

Requirement:

If the OLT supports external authentication mechanism such as AAA server (for authentication, authorization and accounting services) then the communication between OLT 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.

2.3 Protection against brute force and dictionary attacks

Requirement:

A protection against brute force and dictionary attacks that hinder AUTHENTICATION ATTRIBUTE guessing shall be implemented.
Brute force and dictionary attacks aim to use automated guessing to ascertain AUTHENTICATION ATTRIBUTE for user and machine accounts.
Various measures or a combination of the following measures can be taken to prevent this:

(i) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").

(ii) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.

(iii) Using an AUTHENTICATION ATTRIBUTE blacklist to prevent vulnerable passwords.

(iv) Using CAPTCHA to prevent automated attempts (often used for Web applications).

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by OLT. An exception to this requirement is machine accounts.

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

2.4 Enforce Strong Password

Requirement:

(a) The configuration setting shall be such that an OLT shall only accept passwords that comply with the following complexity criteria:

(i)Absolute minimum length of 8 characters (shorter lengths shall be rejected by the OLT). It shall not be possible setting this absolute minimum length to a lower value by configuration.

(ii) Password shall mandatorily comprise all the following four categories of characters:

- 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. @;!$.)

The minimum length of characters in the passwords and the set of allowable special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.

OLT shall have in-built mechanism to support this requirement, further 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 complexity rules 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 complexity rules shall be performed on the OLT.

When a user is changing a password or entering a new password, OLT/central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3]

2.5 Inactive Session Timeout

Requirement:

An OAM user inactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.

OLT shall monitor inactive sessions of administrative login users 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, normally set between 2 to 5 minutes.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.Section 4.2.3.5.2]

2.6 Password Changes

Requirement:

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. OLT shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed upto 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 OLT shall store at least the three previously set passwords. The maximum number of passwords that the OLT 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.

OLT 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 OLT

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

2.7 Protected Authentication feedback

Requirement:

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 "*".

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4]

2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, vendor or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the vendor provides instructions on how to manually change it.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.3]

Section 3: Software Security

3.1 Secure Update

Requirement:

OLT'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.
OLT 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.

3.2 Secure Upgrade

Requirement:

(i) OLT 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) OLT shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the OLT shall have a list of public keys or certificates of authorised 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) OLT'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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5]

3.3 Source code security assurance

Requirement:

a) Vendor should follow best security practices including secure coding for software development. Source code shall be offered to designated TSTL 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 OLT software, which includes vendor developed code, third party software and open-source code libraries used/embedded in the OLT.
   (ii) The OLT software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of OLT to designated TSTL for testing. For other security weaknesses, OEM shall give mitigation plan.
   (iii) The binaries for OLT and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

3.4 Known Malware and backdoor Check

Requirement:

Vendor shall submit an undertaking stating that OLT is free from all known malware and backdoors as on the date of offer to the TSTL for testing and shall submit Malware test document (MTD).

3.5 No unused software

Requirement:

Software components or parts of software which are not needed for operation or functionality of the OLT shall not be present.

Orphaned software components /packages shall not be present in OLT.

OEM shall provide the list of software that are necessary for its operation.

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

3.6 Unnecessary Services Removal

Requirement:

OLT shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. OLT Shall not support following services.. Any other protocols, services that are vulnerable are also to be permanently disabled.

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 and v2
- SSHv1
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- 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 V.1.0.0. Section 4.3.2.1]

3.7 Restricting System Boot Source

Requirement:

OLT 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]

3.8 Secure Time Synchronization

Requirement:

OLT shall provide reliable time and date information provided by itself or through NTP/PTP server.

OLT shall provide reliable time and date information provided through NTP/PTP server. OLT shall establish secure communication channel with the NTP/PTP server.
OLT shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only with NTP/PTP server.
OLT shall generate audit logs for all changes to time settings.

3.9 Restricted reachability of services

Requirement:

The OLT shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose.
On interfaces where services are active, the reachability should be limited to legitimate communication peers.

Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.2]

Section 4: System Secure Execution Environment

4.1 No unused functions

Requirement:

Unused functions i.e. the software and hardware functions which are not needed for operation or functionality of the OLT shall not be present in the OLT'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 OLT.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]

4.2 No unsupported components

Requirement:

Vendor to ensure that the OLT shall not contain software and hardware components that are no longer supported by vendor or its third parties including the open source communities, such as components that have reached end-of-life or end-of-support.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.2.5]

Section 5: User Audit

5.1 Audit trail storage and protection

Requirement:

The security event log shall be access controlled using file access rights such that only privilege users including the administrator have access to read the log files. The rights to delete or modify the log files are to be restricted, a trail of delete or modify activities may be logged in separate log file.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]

5.2 Audit Event Generation

Requirement:

The OLT shall log all important security events with unique System Reference details as given in the Table below.
OLT shall record within each audit record at least information pertaining to date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event Types (Mandatory or optional)	**Description**	**Event data to be logged**
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the DUT	• Username,
		• Source (IP address) if remote access
		Outcome of event (Success or failure)
		• Timestamp
Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	• Username,
		• Timestamp,
		• Length of session,
		Outcome of event (Success or failure)
		• Source (IP address) if remote access
Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, enable, and disable.	• Administrator username,
		• Administered account,
		• Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)

		• Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	• Value exceeded,
		• Value reached
		(Here suitable threshold values shall be defined depending on the individual system.)
		Outcome of event (Success or failure)
		• Timestamp
Configuration change (Mandatory)	Changes to configuration of the network device	• Change made
		* Timestamp
		Outcome of event (Success or failure)
		• Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the network device that forces a reboot or shutdown OR where the network device has crashed.	• Action performed (reboot, shutdown, etc.)
		• Username (for intentional actions)
		Outcome of event (Success or failure)
		• Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the network device (e.g. shutdown)	• Interface name and type
		• Status (shutdown, missing link, etc.)
		Outcome of event (Success or failure)
		• Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	• Administrator username,
		• Administered account,
		• Activity performed (group added or removed)
		Outcome of event (Success or failure)
		• Timestamp.
Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	• Administrator username,
		• Administered account,
		• Activity performed (configure, delete, enable and disable)
		Outcome of event (Success or failure)
		• Timestamp

Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
User login (Mandatory)	All use of identification and authentication mechanism	user identity
		origin of attempt (e.g. IP address)
		Timestamp
		outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update (Optional)	attempt to initiate manual update, initiation of update, completion of update	user identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change (Mandatory)	Change in time settings	old value of time
		new value of time
		Timestamp
		origin of attempt to change time (e.g. IP address)
		Subject identity
		outcome of event (Success or failure)
		user identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, Termination of a remote session by the session locking mechanism, Termination of an interactive session	user identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity
		Activity performed
		Type of event
Trusted Communication paths (with IT entities such as Authentication Server,	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)

Audit Server, NTP Server, etc. and for authorised remote administrators) (Optional)		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Audit data changes (Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure, as applicable)
		Subject identity
		user identity
		origin of attempt to change time (e.g. IP address)
		Details of data deleted or modified
Port Scan Attempts	Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters	Date & Time Stamp
		Source IP Address
		Destination Port Address

[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]

5.3 Secure Log Export

Requirement:

(I) (a) The OLT shall support forwarding 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 or to a system external for the OLT.

(II) OLT shall be able to store generated audit data itself, may be with limitations.

(III) OLT 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), OLT shall have mechanism to store audit data locally. OLT

shall have sufficient memory to store minimum 1000 messages/events 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 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 4.2.3.6.2]

Section 6: Data Protection

6.1 Cryptographic Based Secure Communication with connecting entities

Requirement:

OLT 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.

6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the OLT (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.

Till further instructions, this clause will be considered complied by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the OLT (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."

OEM shall submit cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny.

6.3 Cryptographic Algorithms implementation Security Assurance

Requirement:

An undertaking is to be submitted by the vendor mentioning that "Cryptographic algorithms embedded in the crypto module of OLT 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.

6.4 Protecting data and information – Confidential System Internal Data

Requirement:

When OLT is in normal operational mode (i.e., not in maintenance mode) 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 authorised privileged user.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.2.]

6.5 Protecting data and information in storage

Requirement:

For Sensitive data in storage (persistent or temporary), read access rights shall be restricted. Files of OLT system that are needed for the functionality shall be protected against manipulation.

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, encrypt it by implementation-specific means, strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

(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: Files having sensitive data shall be protected against manipulation strictly using checksum or cryptographic methods as defined in NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

Sensitive data: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3 ;

6.6 Protection against Copy of Data

Requirement:

Without authentication, OLT 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 OLT to create copy of data for illegal transmission. The software functions, components in the OLT for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

6.7 Protection against Data Exfiltration - Overt Channel

Requirement:

OLT 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 OLT.

6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

OLT 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 OLT.

Section 7: Network Services

7.1 Traffic Separation

Requirement:

OLT 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].

7.2 Traffic Filtering – Network level

Requirement:

OLT 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 V.1.0.0. section 4.2.6.2.1]

7.3. Traffic Protection –Anti-Spoofing

Requirement:

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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.3.1.1]

Section 8: Attack Prevention Mechanisms

8.1 Network Level and application-level DDoS

Requirement:

OLT shall have protection mechanism against known network level and application level DDoS attacks.
OLT 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.
Potential protective measures (as applicable to OLT) include, but not limited to, the following:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of a user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/port address in a specific time range

Any two protective measures shall be implemented in OLT to deal with the overload situations.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.3.1]

8.2 Excessive Overload Protection

Requirement:

OLT shall act in a predictable way if an overload situation cannot be prevented. OLT shall be built in this way that it can react on an overload situation in a controlled way.
However, it is possible that a situation happens where the security measures are no longer sufficient. In such case, it shall be ensured that OLT cannot reach an undefined and thus potentially insecure state. In an extreme case, a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.2.3.3.3]

Section 9: Vulnerability Testing Requirements

9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of OLT are reasonably robust when receiving unexpected input.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.4]

9.2 Port Scanning

Requirement:

It shall be ensured that on all network interfaces of OLT, only documented ports on the transport layer respond to requests from outside the system.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.4.2]

9.3 Vulnerability Scanning

Requirement:

It shall be ensured that no known critical/ high/medium (as per CVE-IDs of NIST- NVD) vulnerabilities (as on date of offer of OLT to designated TSTL for testing) shall exist in the OLT. For low/uncategorised (as per CVE-IDs of NIST- NVD) category vulnerabilities remediation plan is to be provided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

Section 10: Operating System

10.1 Growing Content Handling

Requirements:

Growing or dynamic content on OLT shall not influence system functions. A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop OLT from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.1.1.1]

10.2 Handling of ICMP

Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for OLT operation shall be disabled on the OLT.
OLT shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table :

Type (IPv4)	Type (IPv6)	Description	Send	Respond to

0	129	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	128	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet Too Big	Permitted	N/A
N/A	135	Neighbour Solicitation	Permitted	Permitted
N/A	136	Neighbour Advertisement	Permitted	N/A

OLT shall not respond to, or process (i.e. do changes to configuration), under any circumstances certain ICMP message types as marked in below table.

Type (IPv4)	**Type (IPv6)**	**Description**	**Send**	**Respond to**	**Process (i.e. do changes to configuration)**
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.2.]

10.3 Authenticated Privilege Escalation only

Requirement:

OLT shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.1.2.1]

10.4 System account identification

Requirement:

Each system account in OLT shall have a unique identification with appropriate non-repudiation controls.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.2.2]

10.5 OS Hardening

Requirement:

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in OLT.

Kernel based network functions not needed for the operation of the OLT shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.2]

10.6 No automatic launch of removable media

Requirement:

OLT 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]

10.7 Protection from buffer overflows

Requirement:

OLT shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by the vendor.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.3.1.5]

10.8 External file system mount restrictions

Requirement:

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in OLT 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]

10.9 File-system Authorization privileges

Requirement:

OLT 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.

Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.7]

Section 11: Web Servers

11.1 HTTPS

Requirement:

The communication between web client and web server shall be protected strictly using the 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 4.2.5.1]

11.2 Webserver logging

Requirement:

Access to the OLT webserver (for both successful as well as failed attempts) shall be logged by OLT.
The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.2.5.2.1]

11.3 HTTPS input validation

Requirement:

The OLT shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.
OLT 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]

11.4 No system privileges

Requirement:

No OLT web server processes shall run with system privileges.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for OLT operation shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3]

11.6 No unused add-ons

Requirement:

All optional add-ons and components of the web server shall be deactivated if they are not required for OLT operation.
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]

11.7 No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:

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.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.3.4.5]

11.8 No CGI or other scripting for uploads

Requirement:

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]

11.9 No execution of system commands with SSI

Requirement:

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.7]

11.10 Access rights for web server configuration

Requirement:

Access rights for OLT web server configuration files shall only be granted to the owner of the web server process or 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]

11.11 No default content

Requirement:

Default content that is provided with the standard installation of the OLT web server shall be removed.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9]

11.12 No directory listings

Requirement:

Directory listings (indexing) / "Directory browsing" shall be deactivated.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.10]

11.13 Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the NE web server 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]

11.14 Web server information in error pages

Requirement:

User-defined error pages and error messages shall not include version information and other internal information about the OLT web server and the modules/add-ons used.
Default error pages of the OLT web server shall be replaced by error pages defined by the vendor.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.12]

11.15 Minimized file type mappings

Requirement:

File type or script-mappings that are not required for OLT operation shall be deleted.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]

11.16 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the OLT web server's document directory.
In particular, the OLT web server shall not be able to access files which are not meant to be delivered.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]

11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:

If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]

Section 12: Other Security requirements

12.1 No System / Root Password Recovery

Requirement:

No provision shall exist for OLT System / Root password recovery.

In the event of system password reset (e.g., through press of Hard-reset button), the entire configuration of the OLT shall be irretrievably deleted.

12.2 Secure System Software Revocation

Requirement:

Once the OLT 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 non-repudiation controls.

OLT shall support a well-established control mechanism for rolling back to previous software image.

12.3 Software Integrity Check – Boot

Requirement:

The OLT 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.

12.4 Unused Physical and Logical Interfaces Disabling

Requirement:

OLT shall support the mechanism to verify both the physical and logical interfaces exist in the product.
Physical and logical accessible interfaces which are not under use shall be disabled so that they remain inactive even in the event of a reboot.

12.5 No Default Profile

Requirement:

No pre-defined user accounts other than Highest privilege (Admin / Root) user account would be available.

12.6 Security Algorithm Modification

Requirement:

It shall not be possible to modify security algorithms supported by OLT without admin / root credentials. Bidding-down beyond prescribed security / cryptographic algorithms by means of negotiation by communicating entities is not permitted.

Section 13 Specific Requirement

The section contains Indian Telecom Security Assurance Requirements (ITSAR) specific to the stand-alone OLT (Optical Line Terminal), a PON (Passive Optical Network) family network Core element with a dedicated hardware and dedicated software, which includes system software as well as application software

13.1 Mutual Authentication with ONT

Requirement:

The OLT must support mutual authentication with ONT by any combination of serial No, registration ID, logical ONU/ONT ID.

OLT should support this mutual authentication

a) 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.

b) 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]

13.2 MAC address filtering

Requirement:

Before letting any device join the network, the OLT should checks the device's MAC address against a list of approved addresses. If the client's address matches one on list, access is granted as usual; otherwise, it's blocked from joining.

13.3 Configuration and management support (Using OMCI/TR69 protocols)

Requirement:

Remote configuration management, fault management, performance management & security management of OLT shall comply mutual authentication & encryption using Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) of the management traffic.

13.4 Identification of Rogue Optical network behaviour

Requirement:

There are cases of rogue optical behaviour as seen by the OLT. For example, in one case, the optical power of the rogue ONU is so low that in its designated time slot, the OLT would

receive a low optic receive level. Similarly in the other case, the rogue is constantly on at full power, resulting in normal average power readings for the rogue ONU's time slot, but higher average power readings in other ONU time slots. OLT should be able to identify such Rogue Optical network behaviour.

Reference: ITU-T Rec, Series G Supplement 49 (02/2011) Rouge Optical Network unit (ONU)

13.5 Key exchange mechanism

Requirement:

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.

13.6 Inter VLAN routing support

Requirement:

Inter VLAN routing functionality by default is not permitted, only permitted configuration by administrator.

13.7 Alarms

Requirement:

The OLT should be able to get the following alarms

a. Loss of Signal(LoS): The OLT did not receive any expected transmission in the upstream(complete PON failure) for 4 consecutive frames. When the OLT receives at least one upstream transmission
b. Loss of Frame (LoF): When 5 consecutive invalid Psync from OLT are received. When 2 consecutive frames have correct PSync.
c. Loss of signal for ONUi (LOSI): No valid optical signal from ONU when it was expected during 4consecutive no continuous allocations to that ONU. When the OLT receives a valid optical signal from ONUi.
d. Loss of frame of ONUi(LOFI): When n (default 4) consecutive invalid delimiters from ONUi are received. When frame delineation for ONUi is achieved in the operation state.

Annexure-I

Acronyms

AES	Advanced Encryption Standard
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDOS	Distributed Denial of Service
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPSec VPN	Internet Protocol Security Virtual Private Network
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PTP	Precision Time protocol
SFTP	Secure File Transfer Protocol
AUTN	Authentication token
DoS	Denial of Service
OLT	Optical Line Terminal
ONT	Optical Network Terminal
ONU	Optical Network Unit
PON	Passive Optical Network
GPON	Gigabit Passive Optical Network
NCCS	National Centre for Communication Security
NTP	Network Time Protocol
OS	Operating System
PTP	Precision Time Protocol

Annexure-II

List of Undertakings to be Furnished by the OEM for OLT (PON Family BB Equipment) Security Testing

1. Source Code Security Assurance (against test case 3.3)
2. Known Malware and backdoor Check (against test case 3.4)
3. Cryptographic Module Security Assurance (against test case 6.2)
4. Cryptographic Algorithms implementation Security Assurance (against test case 6.3)