Indian Telecom Security Assurance Requirements (ITSAR)

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

Wi-Fi CPEs

ITSAR Number: ITSAR402122401
ITSAR Name: NCCS/ITSAR/Customer Premises Equipment/Data CPEs/Wi-Fi CPEs

Date of Release: 03.01.2024 Version: 1.0.1
Date of Enforcement: 01.07.2024

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

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.	Wi-Fi CPEs	ITSAR402121811	1.0.0	12.11.2018	First release
2.	Wi-Fi CPEs	ITSAR402122401	1.0.1	03.01.2024	Editorial Changes

Table of Contents

Introduction

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies security requirements for Wi-Fi Customer Premises Equipment (CPE). The Wi-Fi CPEs are the equipment that are used or deployed at customer premises in telecom networks for providing internet connectivity to end users.

The types of devices for which ITSAR is applicable are Wi-Fi Routers, Wi-Fi Modems, Broadband Modems with Wi-Fi facility, Cable Modems with Wi-Fi facility, FTTH ONTs with Wi-Fi facility, and Wi-Fi Data cards which provide Wi-Fi facility with backend 2G / 3G / 4G connectivity.

The security requirements are drawn from national, international standards and best security practices for telecom networks. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 is the reference document on which the ITSAR is modelled. The security requirements are grouped into 12 sections based on the sub-areas, the Wi-Fi CPE devices seeking certification has to meet the security requirements mentioned in this document.

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.

Chapter 1: Common Security Requirement

`

Section 1.1: Access and Authorization

1.1.1: Management Protocols Entity Mutual Authentication

The CPE shall communicate with authenticated management entities only. The protocols used for the CPE management shall support mutual authentication mechanisms, preferably with pre- shared key arrangements or by equivalent entity mutual authentication mechanisms. This shall be verified for all protocols used for CPE management. (This feature shall be supported on all WAN management interfaces).

1.1.2: Management Traffic Protection

All management traffic shall be protected by integrity and encryption. Unprotected sessions shall not be accepted. The remote access methods can support traffic encryption using protocols such as HTTPS, SSHv2 or can be based on lower tunnelling protocols (IPsec VPN, TLS VPN, etc.).

1.1.3: Role-Based access control

CPE shall support Role-Based Access Control (RBAC) which provides at least two 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.

1.1.4: User Authentication - Local/Remote

Local/Remote access to the CPE 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 user's name 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.

1.1.5: Remote Management Standards

The remote management mechanisms for CPE to be fully compliant with the remote management standards that the OEM chose to implement, example: TR-069 or any other relevant standards, such mechanisms to include entity mutual authentication, encryption of the management traffic.

1.1.6: Remote Management Standards for Connected Devices, Additional Features

The remote management mechanisms for devices connected to CPE, or for configuration of additional features of CPE like DDNS, UPnP etc., are to be compliant with the respective

latest standards published at the time of commencement of security testing. These additional features are to be configured as disabled in the factory default settings, with provision for user to enable individual features on menu-selection. Such mechanisms to include entity mutual authentication, encryption of the management traffic.

1.1.7: Unambiguous identification of the user & group

The CPE shall identify each login user unambiguously. CPE 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 CPE.

Section 1.2: Authentication and Attribute Management

1.2.1: Authentication Policy

The usage of a system functions such as network services (like SSH, SFTP, Web services), management access, local usage of operating systems and applications shall be allowed only after successful authentication on the basis of the user identity and at least one authentication attribute (e.g., password, certificate).

This requirement shall also be applied to accounts that are only used for communication between systems.

1.2.2: Authentication Support - External

If CPE supports external authentication (for the Cyber- Cafe use-case scenario), the user authentication credentials should be protected and securely communicated if the authentication credentials are managed by external authentication servers.

1.2.3: Protection against brute force and dictionary attacks

CPE 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.

CPE 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 CPE and on authentication attempts on Wi-Fi access through SSID with PSK.

1.2.4: Enforce Strong Password

CPE shall only accept passwords that comply with the following complexity criteria:

1. Password containing a minimum length of 8 characters are only permitted by default. Shorter lengths shall be rejected by the NE.
2. Minimum password length - the default minimum value of 8 characters.
3. 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., @; $.)

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

1.2.5: Inactive Session Timeout

CPE 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.

1.2.6: Password Change facility, 1st Installation /Factory Reset

CPE shall enforce 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 CPE shall provide a function that facilitates the user to change his password at any time. However, the CPE shall not allow the previously used passwords up to a certain number (Password History).

1.2.7: Protected Authentication feedback

When a user enters the password at the local console, local or remote management GUI, the CPE should give obscure feedback by displaying characters like “*”.

1.2.8: Removal of predefined or default authentication attributes

CPE may come with predefined (by the vendor, developer or producer) authentication attributes such as password or cryptographic keys. CPE 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.

1.2.9: Storage of Passwords in encrypted form

User passwords should be stored using password hashes or encrypted, based on a strong hashing mechanism designed for use with passwords (example: HMAC, PBKDF2, Argon2), OEM may choose his own hashing mechanism for implementation. Passwords may not be stored in clear text. This requirement does not apply to pre-shared keys that must be used in raw form, such as IKE pre-shared keys.

Section 1.3: Software Security

1.3.1: Secure Update

The update process should verify the authenticity of the source repository and the integrity of the software patch preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity before updating the software in the CPE. The update mechanism should prevent illegal software patching.

1.3.2: Secure Upgrade

CPE should support authenticity and integrity check while performing software upgrade Preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity.

1.3.3: Source Code security assurance

Source code of the CPE (in high level programming language) shall be free from known security vulnerabilities, the high security critical weaknesses listed in the CWE database and all the exploitable security vulnerabilities listed in the latest SANS Top 25 and OWASP Top 10. OEM may provide Software Test Document (STD) in this regard.

1.3.4: Known Malware Check

The Operating System and the applications installed in the CPE shall be free from any known malware. The CPE shall support mechanism to carry out anti-malware checks. OEM to submit Software Test document (STD) to establish that the CPE is free from Known Malware.

1.3.5: No unused software

Unused software components or parts of software which are not needed for operation or functionality of the CPE shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g., default web pages, example databases, test data). OEM to provide Software Test Document (STD) in this regard.

1.3.6: Unnecessary Service Removal

The OEM to provide list of essential services and the related ports required for functioning

of CPE, list of optimal services supported by CPE and their related ports. The CPE 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 CPE 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 (Identd)
- PAD
- MOP

1.3.7: Secure Time Synchronization

The CPE shall support time synchronization feature for its core functionality or for the additional supported functionality. For CPEs that have time synchronization feature, it shall support the secure time synchronization feature preferably by using Network Time Protocol NTP.

The CPE clock shall be synchronized with NTP server in a secure manner. The CPE 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.

1.3.8: Self-Testing

The CPE shall support the detection mechanism for identification of failure of underlying security mechanisms (such as software image integrity, runtime integrity, cryptographic modules etc.) used. The CPE to perform such self-tests periodically/at the time of booting, visual indication on failure is a desirable feature.

1.3.9: Feature / Service Activation Policy

The CPE shall have factory default settings such that only the essential features / services and ports required for main operational needs of CPE are only enabled. Optional features, added services, futuristic service / applications are disabled by default. Such disabled services could only be enabled after successful authentication and selection by ADMIN user.

1.3.10: Restricted reachability of services

The CPE 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 CPE to only LAN ports and not to permit access on Wi-Fi, WAN side.

Section 1.4: System Secure Execution Environment

1.4.1: No unused functions

Unused functions of the CPEs' software and hardware shall be deactivated.

During installation of software and hardware often functions will be activated that are not required for operation or function of the system. If unused functions of software cannot be deleted or de-installed individually, such functions shall be deactivated in the configuration of the CPE in permanent manner.

Also, hardware functions which are not required for operation or function of the system (e.g., unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after CPE reboot.

OEM to provide report in this regard, List of the used functions of the CPE's software and hardware as given by the OEM shall match the list of used software and hardware functions that are necessary for the operation of the CPE.

1.4.2: No unsupported components

The CPE 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.

1.4.3: No Known Vulnerabilities in System on Chip (SOC) solution

This test is applicable for such CPEs which have System on Chip solutions, where majority of CPE functions are realized in a VLSI chip. OEM to provide self-test / third-party / Chip-vendor test report indicating that the SOC is free from malware, known-vulnerabilities.

Section 1.5: User Audit

1.5.1: Audit Event Generation

CPE 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.

Section 1.6: Data Protection

1.6.1: Cryptographic Based Secure Communication

The communication security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). The data is protected against well know attacks related to Sniffing, Disclosure, reconnaissance etc.,

The secure communication mechanisms between the CPE and connected entities shall use industry standard protocols such as IPSEC, VPN, SSH, TLS/SSL, etc., and NIST specified cryptographic algorithms with specific key sizes such as SHA, Diffie-Hellman, AES etc.

1.6.2: Cryptographic Based Secure Communication on Wi-Fi Access

The communication security dimension on Wi-Fi access ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). The security mechanism to protect against well-known attacks like capture-decrypting, PIN detection, Key recovery, Key reinstallation attacks.

It shall support WPA2-PSK with AES as default standard. Other encryption options stronger than WPA2 may be made available under configuration menu for user choice selection.

1.6.3: Cryptographic Algorithm selection for Wi-Fi Access

It shall support WPA2-PSK with AES-128 as default standard. Other internationally accepted encryption standards stronger like AES-192 etc., may also be made available with user choice selection. Weaker encryption options like WEP, WPS, TKIP etc., are not to be available for selection / configuration.

1.6.4: Crypto-Key Protection Mechanism

The CPE to have protection mechanisms against access to keys in the CPE against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroing blocks of key etc.

1.6.5: Protecting data and information - Confidential System Internal Data

When CPE is not in debug (maintenance) mode, there shall be no system function that reveals confidential system internal data in the clear to users and administrators. Such system functions could be, for example, local or remote OAM CLI or GUI, error messages, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e., PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e., stack traces in error messages).

1.6.6: Protecting data and information in storage

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

1.6.7: Protection against Copy of Data

CPE shall have protection against creating a copy of data in use / data in transit. Protective measures should exit against use of available system functions / software residing in CPE to create copy of data for illegal transmission. The software functions, components in the CPE for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

1.6.8: Protection against Data Exfiltration - Overt Channel

CPE shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound overt channels such as FTP, HTTP, HTTPS IM, P2P, Email etc. are to be forbidden if they are initiated by / originate from the CPE. Outbound-use of such services are to be disabled in the CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

1.6.9: Protection against Data Exfiltration - Covert Channel

CPE 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 initiated by / originate from the CPE. Outbound-use of such services are

to be disabled in the CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Section 1.7: Network Services

1.7.1: Traffic Filtering - Network Level

The CPE shall provide a mechanism to filter incoming IP packets on any IP interface. It is preferable to configure Access Control List (ACL) as default deny-all on WAN port, with feature to enable the types of traffic permitted on user selection.

Section 1.8: Attack Prevention Mechanism

1.8.1: Excessive Overload Protection

The CPE 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.

1.8.2: Filtering IP Options

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g., source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered. OEMs may refer to standards such as RFC 6192, RFC 7126.

Section 1.9 Vulnerability Testing Requirements

1.9.1: Fuzzing - Network and Application Level

The protocols supported by the CPE shall be robust when receiving unexpected or malformed inputs. This requirement shall be applicable for both network level as well as application-level protocols supported by the equipment.

1.9.2: Port Scanning

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 CPE.

1.9.3: SSID Scanning

The CPE 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.

1.9.4: Vulnerability Scanning

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, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces. OEM to provide self-test report establishing that no publicly known vulnerability exists.

Section 1.10: Operating System

1.10.1: Handling of ICMP

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the CPE. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk. Refer standards such as RFC 6192, RFC 7279, RFC 4890.

1.10.2: Privilege Escalation

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.

1.10.3: System account identification

Each system account in Operating system of the CPE shall have a unique identification, the OEM to provide information on implementation mechanism for this requirement.

1.10.4: OS-Hardening Kernel Security

OEM may submit the process for OS Hardening undertaken to justify that the OS is sufficiently hardened and Kernel based applications / functions not needed for the operation of the CPE are deactivated. OEM to provide information on steps taken in this regard.

1.10.5: Protection from buffer overflows

The system 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.

1.10.6: External file system mount restrictions

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

Section 1.11: Web Interface

1.11.1: HTTPS Support

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. CPE to be protected against sniffing and side jacking attacks.

1.11.2: logging

Access to the webserver (both successful as well as failed attempts) shall be logged. 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

1.11.3: HTTP User sessions

1. The session ID shall uniquely identify the user and distinguish the session from all other active sessions.
2. The session ID shall be unpredictable.
3. The session ID shall not contain sensitive information in clear text (e.g., account number, social security, etc.).
4. In addition to the Session Idle Time out.
5. Session IDs shall be regenerated for each new session (e.g. each time a user logs in).
6. The session ID shall not be reused or renewed in subsequent sessions.
7. The CPE shall not use persistent cookies to manage sessions but only session cookies.
8. Where session cookies are used the attribute 'Http Only' shall be set to true.
9. Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.
10. Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.
11. The CPE shall not accept session identifiers from GET/POST variables.
12. The CPE shall be configured to only accept server generate session ID's.

1.11.4: HTTP input validation

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

1.11.5: No unused HTTP methods

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.

1.11.6: No unused add-ons

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.

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

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).

1.11.8: No CGI or other Scripting for uploads

If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

1.11.9: No execution of system Commands with SSI

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

1.11.10: No Default Content

Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed.

1.11.11: No Directory Listing

Directory listings (indexing) / Directory browsing shall be deactivated.

1.11.12: Information in HTTP Headers

The HTTP header shall not include information on the version of the web server and the modules/add-ons used.

1.11.13: Information in Error Page

User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the web server shall be replaced by error pages defined by the vendor.

Section 1.12: Other Security Requirement

1.12.1: Remote Diagnostic Procedure - Verification

If the CPE is providing Remote access for troubleshooting purposes/alarm maintenance, then it should be allowed only for authorized users and all activities performed by the remote user is to be logged with parameters like User id, time stamp, interface type, event level (e.g., CRITICAL, MAJOR, MINOR), result type (e.g., SUCCESS, FAILURE).

1.12.2: No Password Recovery

Network devices have a function that resets the current system password. In the event of system password reset, the entire configuration of the CPE shall be irretrievably deleted. No provision should exist for password recovery.

1.12.3: Software Integrity Check - Installation

CPE should validate the software package integrity before the installation / upgrade. Tampered software shall not be executed or installed if integrity check fails.

1.12.4: Software Integrity Check - Boot

The CPE shall verify the integrity of a software component at the time of boot / re-boot typically by comparing the result of a measurement (typically a cryptographic hash / CRC) of the component to the expected reference value.

1.12.5: Unused Physical Interfaces Disabling

The CPE 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.

1.12.6: No Default Profile

Predefined or default user accounts shall be deleted or disabled. Default accounts such as guest, master are generally preconfigured with known or nil authentication attribute and therefore such standard users shall be deleted or disabled.

Annexure-I

Acronyms

AAA Server	Authentication, Authorization, And Accounting Server
ACL	Access Control List
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
ICMP	Internet Control Message Protocol
IPSec VPN	Internet Protocol Security Virtual Private Network
MD5	Message Digest Algorithm
NE	Network Element
NIST	National Institute Of Standards And Technology
NMS	Network Management System
NTP	Network Time Protocol
OS	Operating System
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
TLS VPN	Transport Layer Security Virtual Private Network
VLAN	Virtual Local Area Network