

**APT REPORT**

**ON**

**TYPE APPROVAL AND
TEST OF INFORMATION TECHNOLOGY EQUIPMENT**

No. **APT/ASTAP/REPT-22**

Edition: March 2016

Source Document: ASTAP-27/OUT-18

**Adopted by**

**The 27th APT Standardization Program Forum (ASTAP-27)**

**7 – 11 March 2016, Pattaya, Thailand**

1. **Introduction**

This report is part of the outcome of a study project on the classification, required and suitable tests, evaluation and type approval methods and procedures in the field of Information Technology (IT). Though many standards, procedures, laboratories, and regulatory institutions exist for testing or certifying the suitability of communication equipment, there is no common agreement or general understanding about the need for, and standards and procedures of IT equipment test, evaluation and type approval. This study intends to fill in this gap and help national regulatory bodies and test laboratories to evaluate IT equipment based on uniform and documented standards.

In this document, we first categorize IT equipment based on their applications, and then present existing standards used in the community for their test and evaluation. We also propose some classifications and acceptance criteria which may be considered as a standard draft that could become a regional or international standard if the technical, scientific and regulatory communities find them interesting and applicable. We present as typical case studies, the evaluation procedures, proposed acceptance criteria, and classification of network and security equipment. It is clear that this survey and analysis is underway and a continuing task that shall comprise other devices that shall be completed in next reports.

1. **IT Equipment Categorization based on Application & Technical specifications**

Information technology (IT) equipment is referred to devices, usually equipped with microprocessors or microcontrollers, destined to store, retrieve, transmit and manipulate data for commercial, industrial or scientific applications. These devices often have one or more inputs, one or more outputs, and a specific functionality controlled by an operating system, a software system or a firmware. Some of these devices (such as general purpose computers) run various applications, and some have a fixed and pre-defined task (such as printers). Some devices have upgrade capability or an option for software functionality changes, such as programmable routers or new software defined network (SDN) equipment, and some can be reconfigured to perform a different task, such as FPGA boards. At present, most of the devices can be tuned, controlled, monitored and programmed through a console port, a terminal or a network connection via software. This is a very desirable and often necessary feature. For instance, manageable network switches report their status while transmitting network traffic, and thus network management software can monitor and report the network status based on this information.

As a remarkable technology and growing market trend, we observe many “embedded systems” comprising low cost processors, memories, and communication interfaces and protocols (such as Bluetooth, Zigbee, WiFi, 3G-4G etc.) destined to do specific jobs (like monitoring or control) in home, factory, hospitals… while being able to communicate with each other, a central office or a server. Hence, we see more and more “smart devices” (smart phone, smart TV, smart home, Internet of Things: IoT…) being able not only to sense their environment and control it but also to communicate with other equipment through radio channels or wired networks. So, it is clear that many IT equipments have entered the category of communication equipment as well, and their tests from a radio standard point of view, is or can become mandatory in near future. That is why features such as EMC (Electromagnetic Compatibility), low radiation and emission, safety, performance, security, fault tolerance, low power consumption are also important features for developers and customers. These features are mostly those which are tested and evaluated in IT test laboratories and will be referred and discussed more in this report.

Figure 1 shows IT equipment categorization in general. As stated before, this categorization is based on application & technical specifications. In this categorization, IT equipment are identified as either a local processing device which is operating as a local device to process, store or retrieve local data or a network processing device which is operating on a communication basis to send or receive data. The later generally operates in the non-physical layer of the network (layers two and upwards). Considering the scope of this project and the mission of national regulatory bodies, we only discuss network processing and security devices in this report. This includes devices referred to as “Data Computing and Communication Devices” and “Security Devices” in Figure 1. These devices are further categorized in Figure 2-Figure 4.



*Figure 1- Information Technology (IT) Equipment Categorization*



*Figure 2 -* ***Data Computing and Communication Devices Categorization***

 

*Figure 3* ***– IP Telephony Devices Categorization***

****

*Figure 4 -* ***Security Devices Categorization***

According to Figure 2, data computing and communication devices can be classified into the following groups:

* ***Switch and Switching Modules***: A network switch is a computer networking device that connects devices together on a computer network by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports. A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Beside most commonly used Ethernet switches, there exist various types of networks, including Fiber Channel, Asynchronous Transfer Mode, and InfiniBand.

Switches can be divided into five categories: ***home or small office***, ***industrial*** and ***access***/***distribution***/***core*** ***layer*** switches. The latter three groups are switches used in multi-layer campus networks. The hierarchical (three-layer) internetworking model is an industry wide adopted model for designing a reliable, scalable, and cost-efficient internetwork. A typical enterprise hierarchical LAN campus network design includes the following three layers, ***access layer*** that provides workgroup/user access to the network, ***distribution layer*** that provides policy-based connectivity and controls the boundary between the access and core layers, and ***core layer*** that provides fast transport between distribution switches within the enterprise campus.

* ***Router and Routing Modules***: A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node. A router is connected to two or more data lines from different networks (as opposed to a network switch, which connects data lines from one single network). When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. This creates an overlay internetwork.

The most familiar type of routers are ***home and small office*** routers that simply pass data, such as web pages, email, IM, and videos between the home computers and the Internet. An example of a router would be the owner's cable or DSL router, which connect to the Internet through an ISP. More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. The enterprise routers can also be categorized as ***branch***/***edge***/***core*** ***layer*** routers. ***Branch routers*** (access layer) are usually placed at the entrance of the local Campus networks. ***Edge routers*** connect the internet servers together and ***core routers*** are placed in backbone network. There are also ***industrial*** routers used in the industrial environments.

* ***Telecommunications Transmission Equipment***: these equipments include ***telecommunication switches and routers***, ***multiplexers*** and ***media converters***. These equipments operate mainly based on PDH and SDH communication standards. ***Plesiochronous Digital Hierarchy (PDH)*** is a technology used in telecommunications networks to communicate large quantities of data over digital transport equipment such as optic fiber and microwave radio systems. This standard has been replaced recently with SDH (***Synchronous Digital Hierarchy***)**.** SDH is a standardized protocol that defines how to transfer multiple digital bit streams synchronously over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs). At low transmission rates data can also be transferred via an electrical interface. This standard was ratified by the International Telecommunication Union in 1987 and has been used by Europe and its commercial partner countries.
* ***IP Telephony Devices***: these include client-side and server-side equipment.

***Client side equipment*** provides audio and video data transmission over the data network or the Internet. These devices are similar to traditional phones, but with more features incorporated in them, including video communication, messaging, remote management, advanced services such as conferencing and so on. Customer premises equipment use SIP and RTP communication protocols to communicate with server-side equipment and exchange information.

1. ***Soft Phone*.** An [application](http://www.webopedia.com/TERM/A/application.html) that enables a [desktop](http://www.webopedia.com/TERM/D/desktop.html), [laptop](http://www.webopedia.com/TERM/L/laptop.html) or [workstation](http://www.webopedia.com/TERM/W/workstation.html) computer to function as a telephone via [VoIP](http://www.webopedia.com/TERM/V/VoIP.html) technology. It uses the computer network as the media for transmitting telephone service. Equipped with a headset or a hand-held device, and using the numbers on the [keyboard](http://www.webopedia.com/TERM/K/keyboard.html) to dial, the computer with soft phone software can perform the full range of telephone features available through traditional systems, such as [teleconferencing](http://www.webopedia.com/TERM/T/teleconference.html) and call forwarding. Soft phones typically make use of the computer's sound card for audio input and output. Soft phones are typically used in call centers and other businesses that rely heavily on a combination of computers and telephones.
2. ***IP Phone*.** An IP telephone system uses packet-switched [VoIP](http://www.webopedia.com/TERM/V/VoIP.html), or [Internet telephony](http://www.webopedia.com/TERM/I/Internet_telephony.html) to transmit telephone calls over the Internet as opposed to the circuit-switched telephony used by the traditional Public Switched Telephone Network ([PSTN](http://www.webopedia.com/TERM/P/PSTN.html)). Also known as VoIP phone systems, IP telephone systems typically comprise a VoIP [private branch exchange](http://www.webopedia.com/TERM/P/PBX.html) (an IP PBX) and desktop VoIP phones ([IP Phones](http://www.webopedia.com/TERM/O/internet_phone.html)) that connect to a VoIP service provider via a [Local Area Network](http://www.webopedia.com/TERM/L/local_area_network_LAN.html) (LAN). One of the key advantages to IP telephone systems is that whereas long-distance calls on a regular phone system can be cost prohibitive, the same calls on an IP phone system are free -- there are no fees beyond the cost of Internet access.
3. ***Analog Telephone Adapter (ATA)*.** A phone handset to [Ethernet](http://webopedia.com/TERM/E/Ethernet.html) adapter that allows traditional (analog) telephone devices be used with [VoIP](http://webopedia.com/TERM/V/VoIP.html) services and equipment. The adapters are roughly the same size as a home Internet [router](http://webopedia.com/TERM/r/router.html) and contain one or more traditional phone jack ports. The analog phone plugs into the adapter, which then communicates with an Internet router via an Ethernet connection.

***Server side equipment***

Server side products are the equipment used by servers to connect various VOIP customers. These products are the opposite of client side equipment. This type of products are used to create a VOIP network within an organization or by small operators to offer services based on VOIP. There are various devices in this category.

1. ***SIP server equipment.*** SIP server equipments that are mostly implemented by software -although there are examples of hardware SIP severs- are responsible to communicate with and serve to IP customers. They receive requests (such as destination address) from customers and after doing the necessary processing, connect the source and destination. These equipments are the core of VOIP architecture and there is no ability to communicate without them. They support several dozen to several hundred thousand ports. Higher capacities are mainly used by major telecom operators who establish their networks on IMS architecture.

SIP servers are used as the core of a VOIP network in enterprise organizations. They are placed in different categories based on their capacity and the number of customers they support. (*Table 1*) Products used in a small organization can have less quality compared to a large organization or operator product. Thus different criteria is defined and suggested for small and large organizations. Large organization products are evaluated more strictly than similar products in small scale organizations. Enterprise products are categorized as follows: (Table 1)

* SOHO application
* Small-medium scale organizational products
* Medium-large scale organizational products
* Large scale organizational products
1. **IP PBX.** IP PBX products are similar to SIP servers. The difference is that they also use analog and E1 interfaces in addition to the SIP protocol and interface IP, to connect to the PSTN network. The core of this type of products is an SIP Server to establish VoIP communications, also the software and hardware parts are provided to convert a VOIP connection to an analog connection in this type of products. As noted before, IP Phones are somehow expensive; so many organizations prefer to continue to use cheap analog phones. On the other hand, the VOIP server-side equipment provides numerous benefits to organizations so that organizations tend to use them to create their own telephone network. IP PBXs are products that provide benefits of VOIP communications for the organization as well as supporting analog interfaces. It should be noted that if you need a large number of analog interface, FXS Gateway equipment are used which will be mentioned later in this report. Usually IP PBX analog lines offer a limited number of analog lines and if you need more, gate equipment are used. However, the exact number of interfaces cannot be defined exactly and depending on the organization approach, there is considerable diversity in the products.

Apart from support for analog interfaces, two important differences exist between the IP PBX and SIP Server. First, telephone services should be implemented in the IP PBX on a mandatory basis while there is no such need in SIP servers. Second, IP PBX is used just by organizations while SIP Server is used in both organizational and operational applications.

IP PBX can connect to the PSTN network in two ways:

* Using the E1 links and PRI protocol: these links are usually used in organizations with more than a few hundred users. An IP PBX can have at least one link, but its maximum number is variable, depending on the different implementations of different vendors.
* Using the urban FXO lines: Similar to E1 links, this method provides analog connection over urban phone lines. A product can have an FXO line. The maximum limit is diverse and varies depending on the manufacturers approach. FXO Gateway equipment can also be used individually in the VOIP network.

According to the above, it is not possible to determine a specific number for analog interfaces. The numbers of FXO, FXS and E1 interfaces are diverse and depend on product design, so it is not possible to determine clear limits for them. So, the number of supported ports is just considered for product rating. (*Table 2*)

1. **Gateway equipment to the PSTN network- E1 Gateway.** By creating a VoIP network, internal communications among customers of this network is provided without the need to connect with other networks. However, in most VoIP networks, customers should be able to communicate with other telecommunication networks such as PSTN or mobile network. The connection between a VOIP network and the traditional network like PSTN is provided through equipment called VOIP Gateway. They connect to the telephone network in different ways. One of these methods is to use E1 communication links. Equipment that use E1 links are known as E1 gateways.
2. **Gateway equipment to PSTN network- FXO gateway.** Another way to connect organizational networks to conventional networks is urban lines - telephone lines - or more technically FXO lines. Each FXO line is capable of carrying one voice channel. For this reason, in applications where a large number of output channels is required, using FXO lines has no advantage compared to E1 lines. Therefore, this method usually supports equipment with limited FXO port number.
3. **Analog interface gateway – FXS gateway equipment.** FXS refers to lines to which an analog telephone connects. FXS gateway equipments are almost the same as an ATA converter we discussed in client side equipment. The difference is the capacity of the device.

*Table 1- SIP server equipment categorization*

|  |  |
| --- | --- |
| **Capacity** | **Applicable for …** |
| Less than 100 ports | SOHO applications |
| 100 to 1000 ports | Small-medium scale organization |
| 1000 to 10’000 ports | Medium-large scale organization |
| 10’000 to 100’000 ports | Large organization |
| Over 100’000 ports | Products with this capacity can't be evaluated in the VOIP laboratory. They are considered as NGN or IMS architecture and should be evaluated in the IMS type approval laboratory. |

*Table 2. IP PBX equipment categorization*

|  |  |
| --- | --- |
| **Capacity** | **Applicable for …** |
| Below 100 ports (SIP and analog) | SOHO applications |
| 100 to 1000 ports | Small-medium scale organization |
| 1000 to 10’000 ports | Medium-large scale organization |
| Over 10’000 ports | Considered as SIP Server |

* ***Traffic Engineering Devices***: This group of equipment is used for network traffic engineering according to usage type and traffic volume. In fact, these instruments are used for managing and shaping and classification of network traffic, mainly with the aim of making better use of network resources such as bandwidth and increase the quality of service (QoS).
* ***Wireless Devices***: these equipments include suitable equipment for outdoors and indoors. ***Ethernet/wireless bridges***, ***wireless modems***, ***access points***, ***wireless LAN cards*** and ***wireless antenna*** are sample equipment for indoor devices. Outdoor equipment is usually categorized according to their operating frequencies.
* ***Data Storage Devices***: these equipments are used in data centers and enterprise networks for data storage and transmission over the network. Simultaneously, independent of the communication context, these equipments are used for massive data storage and parallel processing and cloud computing over a large number of processors or cluster computers, so they have dual functionality from the viewpoint of this project.
* ***Broadband devices***: ***Digital subscriber line (DSL)*** is a data communications technology that enables faster data transmission over copper telephone lines than a conventional voice-band modem can provide. This technology utilizes different frequencies and modulation types not used for ordinary voice communications, to exchange data packets.

Broadband equipment include ***DSLAMs***[[1]](#footnote-1) (network devices often located in telephone exchanges, that connect multiple customer DSL interfaces to a high-speed digital communications channel using multiplexing techniques and ***DSL modems*** (devices used to connect a computer or router to a telephone line which provides the DSL service for connectivity to the Internet).

One specific type of DSL modems are ***Asymmetric DSL (ADSL) modems***. ADSL differs from the less common ***Symmetric Digital Subscriber Line (SDSL)*** in that bandwidths (and bit rate) are greater toward the customer premises (known as downstream) than the reverse (known as upstream). This is why it is called asymmetric. Providers usually market ADSL as a service for consumers to receive Internet access in a relatively passive mode, being able to use the higher speed direction for downloading from the Internet but not needing to run servers that would require high speed in the other direction

Furthermore, security tools are divided into the following groups: (Figure 4)

* ***Anti-malware Devices***: Malware or Malicious software is any software that is used to harm the functionality of a computer system or to gather sensitive information or to access private computer systems. The purpose of Anti-malware devices is to detect and deal with these malwares. These devices are usually deployed as ***host-based*** or ***network-based***. The scope of their functionality, in the former case is the same host and in the latter case is all hosts on the network.
* ***Network Security Devices*** : these equipment are categorized as follows:
	1. ***Identification and Prevention Equipment***: these equipments include devices to identify network vulnerabilities and its intrusion points and equipment to trap and identify the characteristics of the attackers. The latter group is called a “***honey pot***”. A ***honey pot*** is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honey pot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, monitored, and seems to contain information or a resource of value to attackers.
	2. ***Passive Security Equipment***: these equipments include any ***intrusion detection and prevention devices***. ***Intrusion Detection System*** or ***IDS*** is a program that analyzes network traffic and tries to detect attacker activities and reactions to abnormal input traffic. ***Intrusion Prevention System (IPS)*** is similar to ***IDS***, except that after detection, it prevents abnormal traffic from entering the network.
	3. ***Active Security Equipment***: these equipments include a variety of ***firewalls***, ***antivirus tools*** and ***content filtering tools***. A ***firewall*** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A ***firewall*** typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.

***Anti-virus*** is a computer software used to prevent, detect and remove malicious software (viruses, Trojans, worms and other malwares).

***Content-control filter*** is a software designed to restrict or control the content a reader is authorized to access, especially when utilized to restrict material delivered over the Internet via the Web, e-mail, or other means. ***Content-control software*** determines what content will be available or perhaps more often what content will be blocked. Such restrictions can be applied at various levels, a government can attempt to apply them nationwide (see Internet censorship), or they can, for example, be applied by an ISP to its clients, by an employer to its personnel, by a school to its students, by a library to its visitors, by a parent to a child's computer, or by an individual user to his or her own computer

* 1. ***Next Generation Firewalls***: these equipments are also called ***Unified Threat Management (UTM)***. These equipments include the ***network layer firewalls***, ***application layer firewalls***, ***Proxy servers*** and ***Network*** ***Address******Translation******(NAT)*** servers. Protection at the network layer firewalls are done based on the type of service and the application.

A ***proxy*** ***server*** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

* ***Authentication Equipment***: these equipments are used to control users' access to confidential content and include ***hardware security modules (HSM)***, ***security tokens*** and ***smart cards***.
1. **IT equipment Test and Evaluation Standards**

The common standards applied for test and evaluation of IT equipment (those within the scope of this project), include:

1. RFC 2544: Benchmarking methodology for network interconnect devices [1]
2. RFC 2889: Benchmarking methodology for LAN switching devices [2]
3. RFC 6076: Basic Telephony SIP End-to-End Performance Metrics [3]
4. RFC 7501: Terminology for Benchmarking Session Initiation Protocol (SIP) Devices [4]
5. RFC 7502: Methodology for Benchmarking Session Initiation Protocol (SIP) Devices [5]
6. ETSI TS 132 409: Performance measurements IP Multimedia Subsystem (IMS) [6]
7. ETSI TS 132 454: Key Performance Indicators (KPI) for IMS [7]
8. ETSI TS 102 027: Conformance test specification for SIP [8]
9. RFC 4475: SIP torture test [9]
10. ETSI ES 201 168: Transmission characteristics of digital PBXs for interconnection to private networks, to the public switched network or to IP gateways [10]
11. ISO/IEC 15408: Computer security certification [11]
12. RFC 3511: Benchmarking methodology for firewall performance [12]
13. NSS Lab Standards [13]
14. IEC 60950-1: Information technology equipment – Safety [14]
15. IEC 61000: Electromagnetic compatibility (EMC) [15]
16. EN 55022: Information technology equipment, Radio disturbance characteristics [16]
17. EN 55024: Information technology equipment, Immunity characteristics [17]

*Table 3* shows a list of IT devices and the corresponding standards used for their test and evaluation. In the next sections, we present a brief description of each standard.

*Table 3- IT Equipment Test & Evaluation Standards*

|  |  |  |
| --- | --- | --- |
| Standard | **Test Domain** | **Device Under Test** |
| RFC 2544 | Performance | Switch and Switching Modules |
| RFC 2889 |
| RFC 2544 | Performance | Router and Routing Modules |
| - | Conformance |
| TR 100 | Performance | Broadband Devices |
| ETSI TBR 021 | PSTN Performance | Telecommunication Transmission Devices |
|  | Functional | IP Telephony Devices |
| RFC 6076RFC 7501, RFC 7502ETSI TS 132 409ETSI TS 132 454RFC 4475 | SIP Performance |
| ETSI TS 102 027 | SIP Conformance |
| ETSI ES 201 168 | PBX Device Evaluation |
| - |  | Traffic Engineering Devices |
| - |  | Data Storage Devices |
| RFC 3511 | Performance | Security Devices |
| ISO/IEC/ISIRI 15408 | Security |
| NSS Laboratory Standards | Performance & Security |

*Table 4- Safety and EMC Evaluation of IT Equipment)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Standard** | **Basic Standard** | **Test Title** | **Test Domain** | **Device Under Test** |
| IEC60950-1 |  |  | Safety | **Information Technology Equipment** **(in general)** |
| EN 55024 | IEC 61000-4-2 | ESD | Electromagnetic Compatibility (EMC) |
| IEC 61000-4-3  | EMS Radiated |
| IEC 61000-4-4 | Burst |
| IEC 61000-4-5 | Surge |
| IEC 61000-4-6 | EMS Conducted |
| IEC 61000-4-8 | Magnetic Field |
| IEC 61000-4-11 | Voltage Dip,Short Interruptions,Voltage Variation |
| IEC 61000-3-2 | Harmonic Current |
| IEC 61000-3-3 | Voltage Fluctuation and Flicker |
| EN 55022 |  | Radiated EMI |
| Conducted EMI |

* 1. **RFC 2544: Benchmarking Methodology for Network Interconnect Devices**

The Internet Engineering Task Force RFC 2544 is a benchmarking methodology for network interconnect devices. [1] This request for comment (RFC) was created in 1999 as a methodology to benchmark network devices such as hubs, switches and routers as well as to provide accurate and comparable values for comparison and benchmarking.

RFC 2544 provides engineers and network technicians with a common language and results format. The RFC 2544 describes six subtests:

* ***Throughput***: measures the maximum rate at which none of the offered frames are dropped by the device/system under test (DUT/SUT). This measurement translates into the available bandwidth of the Ethernet virtual connection.
* ***Back-to-back or burst measure***: measures the longest burst of frames at maximum throughput or minimum legal separation between frames that the device or network under test will handle without any loss of frames. This measurement is a good indication of the buffering capacity of a DUT.
* ***Frame loss***: defines the percentage of frames that should have been forwarded by a network device under steady state (constant) loads that were not forwarded due to lack of resources. This measurement can be used for reporting the performance of a network device in an overloaded state, as it can be a useful indication of how a device would perform under pathological network conditions such as broadcast storms.
* ***Latency***: measures the round-trip time taken by a test frame to travel through a network device or across the network and back to the test port. Latency is the time interval that begins when the last bit of the input frame reaches the input port and ends when the first bit of the output frame is seen on the output port. It is the time taken by a bit to go through the network and back. Latency variability can be a problem. With protocols like voice over Internet protocol (VoIP), a variable or long latency can cause degradation in voice quality.
* ***System reset***: measures the speed at which a DUT recovers from a hardware or software reset. This subtest is performed by measuring the interruption of a continuous stream of frames during the reset process.
* ***System recovery***: measures the speed at which a DUT recovers from an overload or oversubscription condition. This subtest is performed by temporarily oversubscribing the device under test and then reducing the throughput at normal or low load while measuring frame delay in these two conditions. The different between delay at overloaded condition and the delay and low load conditions represent the recovery time.
	1. **RFC 2889: Benchmarking methodology for LAN switching devices**

This RFC is intended to provide methodology for the benchmarking of local area network (LAN) switching devices [2]. It extends the methodology, already defined for benchmarking network interconnecting devices in RFC 2544 [2], to switching devices.

This RFC primarily deals with devices which switch frames at the Medium Access Control (MAC) layer. It provides a methodology for benchmarking switching devices, forwarding performance, congestion control, and latency, address handling and filtering. In addition to defining the tests, this standard also describes specific formats for reporting the results of the tests.

* 1. **RFC 6076: Basic Telephony SIP End-to-End Performance Metrics**

This RFC [3] defines a standard set of metrics for measuring and reporting SIP performance from an end-to-end perspective in a telephony environment. The metrics introduce a common foundation for understanding and quantifying performance expectations between service providers, vendors, and the users of services based on SIP.

Measurements of the metrics described in this RFC are affected by variables external to SIP. The following is a non-exhaustive list of examples:

* Network connectivity
* Switch and router performance
* Server processes and hardware performance

The RFC defines a list of pertinent metrics for varying aspects of a telephony environment. They may be used individually or as a set based on the usage of SIP within the context of a given telecommunication service.

The metrics defined in this RFC DO NOT take into consideration the impairment or failure of actual application processing of a request or response. The metrics do not distinguish application processing time from other sources of delay, such as packet transfer delay.

The RFC does not provide any numerical objectives or acceptance threshold values for the SIP performance metrics defined below, as these items are beyond the scope of IETF activities, in general.

The metrics defined in this RFC are applicable in scenarios where the SIP messages launched (into a network under test) are dedicated messages for testing purposes, or where the messages are user-initiated and a portion of the live is traffic present. These two scenarios are sometimes referred to as active and passive measurement, respectively.

* 1. **RFC 7501: Terminology for Benchmarking Session Initiation Protocol (SIP) Devices**

This RFC [4] provides a terminology for benchmarking the Session Initiation Protocol (SIP) performance of devices. Methodology related to benchmarking SIP devices is described in the companion methodology document (RFC7502). Using these two documents, benchmarks can be obtained and compared for different types of devices such as SIP Proxy Servers, Registrars, and Session Border Controllers.

Service Providers and IT organizations deliver Voice Over IP (VoIP) and multimedia network services based on the IETF Session Initiation Protocol (SIP) [19]. SIP is a signaling protocol originally intended to be used to dynamically establish, disconnect, and modify streams of media between end users. As it has evolved, it has been adopted for use in a growing number of services and applications. Many of these result in the creation of a media session, but some do not. Examples of this latter group include text messaging and subscription services. The set of benchmarking terms provided in this RFC is intended for use with any SIP-enabled device performing SIP functions in the interior of the network, whether or not these result in the creation of media sessions.

A number of networking devices have been developed to support SIP- based VoIP services. These include SIP servers, Session Border Controllers (SBCs), and Back-to-back User Agents (B2BUAs). These devices contain a mix of voice and IP functions whose performance may be reported using metrics defined by the equipment manufacturer or vendor. The Service Provider or IT organization seeking to compare the performance of such devices will not be able to do so using these vendor-specific metrics, whose conditions of test and algorithms for collection are often unspecified.

SIP functional elements and the devices that include them can be configured in many different ways and can be organized into various topologies. These configuration and topological choices impact the value of any chosen signaling benchmark. Unless these conditions of test are defined, a true comparison of performance metrics across multiple vendor implementations will not be possible.

Some SIP-enabled devices terminate or relay media as well as signaling. The processing of media by the device impacts the signaling performance. As a result, the conditions of test must include information as to whether or not the Device under Test processes media. If the device processes media during the test, a description of the media must be provided. This document and its companion methodology document (RFC7502) provide a set of black-box benchmarks for describing and comparing the performance of devices that incorporate the SIP User Agent Client and Server functions and that operate in the network’s core.

The definition of SIP performance benchmarks necessarily includes definitions of Test Setup Parameters and a test methodology. These enable the Tester to perform benchmarking tests on different devices and to achieve comparable results. This RFC provides a common set of definitions for Test Components, Test Setup Parameters, and Benchmarks. All the benchmarks defined are black-box measurements of the SIP signaling plane. The Test Setup Parameters and Benchmarks defined in this RFC are intended for use with the companion methodology document.

* 1. **RFC 7502: Methodology for Benchmarking Session Initiation Protocol (SIP) Devices**

This RFC [5] describes the methodology for benchmarking Session Initiation Protocol (SIP) performance as described in the Terminology document (RFC7501). The methodology and terminology are to be used for benchmarking signaling plane performance with varying signaling and media load. Media streams, when used, are used only to study how they impact the signaling behavior. This RFC concentrates on benchmarking SIP session setup and SIP registrations only.

The Device Under Test (DUT) is a network intermediary that is RFC 3261 [19] capable and that plays the role of a registrar, redirect server, stateful proxy, a Session Border Controller (SBC) or a B2BUA. This RFC does not require the intermediary to assume the role of a stateless proxy. Benchmarks can be obtained and compared for different types of devices such as a SIP proxy server, Session Border Controllers (SBC), SIP registrars and a SIP proxy server paired with a media relay.

The test cases provide metrics for benchmarking the maximum ’SIP Registration Rate’ and maximum ’SIP Session Establishment Rate’ that the DUT can sustain over an extended period of time without failures (extended period of time is defined in the algorithm in Section 4.10). Some cases are included to cover encrypted SIP. The test topologies that can be used are described in the Test Setup section. Topologies in which the DUT handles media as well as those in which the DUT does not handle media are both considered.

Benchmark metrics could possibly be impacted by Associated Media. The selected values for Session Duration and Media Streams per Session enable benchmark metrics to be benchmarked without Associated Media. Session Setup Rate could possibly be impacted by the selected value for Maximum Sessions Attempted. The benchmark for Session Establishment Rate is measured with a fixed value for maximum Session Attempts.

Finally, the overall value of these tests is to serve as a comparison function between multiple SIP implementations. One way to use these tests is to derive benchmarks with SIP devices from Vendor-A, derive a new set of benchmarks with similar SIP devices from Vendor-B and perform a comparison on the results of Vendor-A and Vendor-B. This RFC does not make any claims on the interpretation of such results.

* 1. **ETSI- TS 132 409: Performance measurements IP Multimedia Subsystem (IMS)**

This standard [6] describes the measurements of IP multimedia subsystem (IMS). These measurements have specific names with a prefix containing the measurement family name (e.g. UR.AttInitReg, SC.AttOrigSession). This family name identifies all measurements which relate to a given functionality and it may be used for measurement administration.

The list of families currently used in the present document is as follows:

* CC (measurements related to Call Control).
* CONF (measurements related to conference service).
* DBU (measurements related to Database Usage).
* DTR (measurements related to Data Read).
* DTU (measurements related to Data Update).
* EQPT (measurements related to Equipment).
* LIQ (measurements related to Location Information Query).
* MA (measurements related Multimedia Authentication).
* NOTIF (measurements related to Notification).
* PoC (measurements related to PoC service).
* PRES (measurements related to Present service).
* QoS (measurements related to Quality of Service).
* RII (measurements related to Routing Information Interrogation).
* RU (measurements related to Roaming Users).
* SC (measurements related to Session Control).
* SUB (Measurements related to Subscription to notifications).
* UP (measurements related to User Profile).
* UR (measurements related to UE registration).
* XDM (measurements related to XDM enabler).

Four mechanisms have been introduced in this standard for measurement:

* **Cumulative Counter (CC)**: The measurement is incremented with each related event.
* **Dynamic Variable (Gauge)**: Is used when the measurement decreases or increases during the measurement period.
* **Discrete Event Registration (DER)**: A specific data related to a specific event is logged.
* **Status Inspection (SI)**: Internal counters used for resource management.

The complete list of the measurements can be found in [6].

* 1. **ETSI TS 132 454: Key Performance Indicators (KPI) for IMS**

This standard [7] specifies Key Performance Indicators (KPIs) for the IP Multimedia Subsystem (IMS). By measuring these indicators in a test laboratory, it becomes possible to study, analyze and compare different systems. Although the indicators are specified for IMS architecture, they are also usable in VOIP because of the central role of SIP in IMS architectures.

The KPIs specified in this standard are classified into the following groups:

* Accessibility KPIs
* Retainability KPIs
* Utilization KPI
	1. **RFC 4475: SIP Torture Test**

This standard contains test messages based on the current version (2.0) of the Session Initiation Protocol as defined in RFC3261 [19]. Some messages exercise SIP’s use of the Session Description Protocol (SDP), as described in RFC3264 [20]. These messages were developed and refined at the SIP Interoperability test events.

The test messages are organized into several sections. Some messages stress only a SIP parser, and others stress both the parser and the application above it. Some messages are valid, and some are not. Each example clearly calls out what makes any invalid messages incorrect.

This standard does not attempt to catalog every way to make an invalid message, nor does it attempt to be comprehensive in exploring unusual, but valid, messages. Instead, it tries to focus on areas that have caused interoperability problems or that have particularly unfavorable characteristics if they are handled improperly. This document is a seed for a test plan, not a test plan in itself.

The messages are presented in the text using a set of markup conventions to avoid ambiguity and meet Internet-Draft layout requirements. To resolve any remaining ambiguity, a bit-accurate version of each message is encapsulated in an appendix.

* 1. **ETSI TS 102 027: Conformance Test Specification for SIP**

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a telecommunication specification. Such an statement is called an Implementation Conformance Statement (ICS).

ETSI TS 102 027 provides the Protocol Implementation Conformance Statement (PICS) proforma for the Session Initiation Protocol (SIP) implementation in compliance with the relevant requirements specified in RFC 3261 [19], and in accordance with the relevant guidance given in ISO/IEC 9646-7 and ETS 300 406.

This standard is applicable to equipment performing the roles of user agent, registration server, proxy application server and redirect server. It is a new release of TS 102 027-1.

For the purposes of this standard, the terms and definitions given in RFC 3261, ISO/IEC 9646-1, ISO/IEC 9646-7 and the following apply:

* ***Implementation Conformance Statement (ICS)***: statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented

NOTE: The ICS can take several forms: protocol ICS, profile ICS, profile specific ICS, information object ICS, etc.

* ***ICS proforma***: document, in the form of a questionnaire, which when completed for an implementation or system becomes an ICS
* ***Protocol ICS (PICS)***: PICS for an implementation or system claimed to conform to a given protocol specification
	1. **ETSI ES 201 168: Transmission Characteristics of Digital PBXs**

This standard has been produced by ETSI Technical Committee Speech processing, Transmission and Quality aspects (STQ). [10] The present Standard is intended to be used as a specification for the design of Private Branch eXchanges (PBXs) and for the harmonization of PBX transmission parameters throughout Europe. It has been developed based on four Interim ETSs (I-ETSs), one ETS and the first version of the present document, all of which are replaced by the present standard.

In the application of this PBX standard, it should be considered that no network access requirements are contained herein. ETSI is maintaining a set of access requirement documents some of which have formerly been the technical basis for harmonized European regulation. In order to enable a suitable end-to-end speech transmission performance, it will be necessary to comply with the appropriate network access requirements as well.

The standard specifies the transmission requirements for PBXs (through-connecting telecommunications equipment) that:

* are not part of the public network;
* are intended for interconnection either to the public switched network, to a Private Network (e.g., a Corporate Network) or to an IP-Gateway;
* carry 3,1 kHz voice telephony between analogue interfaces, digital interfaces carrying 64 Kbit/s A-law encoded signals and the acoustic interfaces of handset telephony terminals (wired or cordless) that are designed to be used together with the PBX for connections involving digital access to the public switched network;
* are capable of providing, for the purposes of testing, a test point that offers a 64 Kbit/s signal with bit integrity to the digital transmission path (this test point need not be provided in production versions of a PBX);
* carry 3,1 kHz voice telephony, irrespective of whether they carry other services in addition

The document does not apply to:

* Hands-free and loud-speaking telephony terminals;
* the interface between the PBX and system specific telephones (excluding the acoustic interfaces as stated above) irrespective whether they are wired or cordless
	1. **ISO/IEC 15408: Computer Security Certification**

ISO/IEC 15408 is an international standard for computer security certification also known as Common Criteria (CC). It is currently Version 3.1, Revision 4. [8]

Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) through the use of Protection Profiles (PPs). Vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard and repeatable manner at a level that is commensurate with the target environment for use.

ISO/IEC 15408-1: 2005 defines two forms for expressing IT security functional and assurance requirements. The PP construct allows creation of generalized reusable sets of these security requirements. The PP can be used by prospective consumers for specification and identification of products with IT security features which will meet their needs. The Security Target (ST) expresses the security requirements and specifies the security functions for a particular product or system to be evaluated, called the Target Of Evaluation (TOE). The ST is used by evaluators as the basis for evaluations conducted in accordance with ISO/IEC 15408.

The CC contains a set of defined assurance levels constructed using components from the assurance families. These levels are intended partly to provide backward compatibility to source criteria and to provide internally consistent general purpose assurance packages. Other groupings of components are not excluded. To meet specific objectives an assurance level can be augmented by one or more additional components. Assurance levels define a scale for measuring the criteria for the evaluation of PPs and STs. Evaluation Assurance Levels (EALs) are constructed from the assurance components detailed opposite. Every assurance family contributes to the assurance that a TOE meets its security claims. EALs provide a uniformly increasing scale which balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. There are seven hierarchically ordered EALs. The increase in assurance across the levels is accomplished by substituting hierarchically higher assurance components from the same assurance family, and by the addition of assurance components from other assurance families.

The seven EALs are as follows:

* EAL1: functionally tested
* EAL2: structurally tested
* EAL3: methodically tested and checked
* EAL4: methodically designed, tested and reviewed
* EAL5: semi formally designed and tested
* EAL6: semi formally verified design and tested
* EAL7: formally verified design and tested

A CC evaluation is one using the CC as the basis for evaluating the IT security properties. Evaluations against a common standard facilitate comparability of evaluation outcomes. In order to enhance comparability between evaluations results yet further, evaluations should be performed within the framework of an authoritative evaluation scheme, which sets standards and monitors the quality of evaluations. Such schemes currently exist in several nations. Distinct stages of evaluation are identified, corresponding to the principal layers of TOE representation:

• **PP evaluation:** carried out against the evaluation criteria for PPs (CC Part 3)

• **ST evaluation:** carried out against the evaluation criteria for STs (CC Part 3)

• **TOE evaluation:** carried out against the evaluation criteria in CC Part 3 using an evaluated ST as the basis.

• **Assurance maintenance:** carried out under schemes based on the requirements in CC Part 3.

Testing, design review and implementation review contribute significantly to reducing the risk that undesired behavior is present in the TOE. The CC presents a framework in which expert analysis (evaluation) in these areas can take place.

* 1. **RFC 3511: Benchmarking Methodology for Firewall Performance**

The RFC 3511 standard [12], established by the Internet Engineering Task Force (IETF) standards body, discusses and defines a number of tests that may be used to describe the performance characteristics of firewalls. It covers four areas: forwarding, connection, latency and filtering. In addition to defining the tests, this document also describes specific formats for reporting the results of the tests. This document is a product of the Benchmarking Methodology Working Group (BMWG) of the Internet Engineering Task Force (IETF). This memo provides information for the Internet community.

The benchmarking tests include:

* IP throughput
* Concurrent TCP Connection Capacity
* Maximum TCP Connection Establishment Rate
* Maximum TCP Connection Tear Down Rate
* Denial Of Service Handling
* HTTP Transfer Rate
* Maximum HTTP Transaction Rate
* Illegal Traffic Handling
* IP Fragmentation Handling
* Latency
	1. **NSS Laboratory Methodologies**

Beside the above mentioned security test standards, we also mention NSS as one of the well-known testing laboratories working on information security that has presented methodologies for testing various security devices. It seems that they have been relatively well accepted internationally by industry though not yet standardized. Some more common methodologies are listed in *Table 5*.

*Table 5- NSS Laboratory Security Device Test Methodologies [21]*

|  |  |  |
| --- | --- | --- |
|  | **Name** | **Release Date** |
|  | [Next Generation Firewall: Test Methodology v6.0](https://www.nsslabs.com/reports/next-generation-firewall-test-methodology-v60) | March 26, 2015 |
|  | [Distributed Denial of Service (DDoS) Prevention: Test Methodology v2.0](https://www.nsslabs.com/reports/distributed-denial-service-ddos-prevention-test-methodology-v20) | December 17, 2014 |
|  | [Industrial Control Firewall: Test Methodology v1.0](https://www.nsslabs.com/reports/industrial-control-firewall-test-methodology-v10) | December 17, 2014 |
|  | [Virtual Firewall: Test Methodology v1.0](https://www.nsslabs.com/reports/virtual-firewall-test-methodology-v10) | October 22, 2014 |
|  | [Security Stack (IPS): Test Methodology v1.0](https://www.nsslabs.com/reports/security-stack-ips-test-methodology-v10) | July 23, 2014 |
|  | [Server Protection Test Methodology v1.0](https://www.nsslabs.com/reports/server-protection-test-methodology-v10) | July 09, 2014 |
|  | [Breach Detection Systems Test Methodology v2.0](https://www.nsslabs.com/reports/breach-detection-systems-test-methodology-v20-0) | June 06, 2014 |
|  | [Secure Web Gateway Test Methodology v1.5](https://www.nsslabs.com/reports/secure-web-gateway-test-methodology-v15) | June 06, 2014 |
|  | [Endpoint Protection – Evasion and Exploit: Test Methodology v4.0](https://www.nsslabs.com/reports/endpoint-protection-%E2%80%93-evasion-and-exploit-test-methodology-v40) | May 15, 2014 |
|  | [Security Stack (UTM): Test Methodology v1.0](https://www.nsslabs.com/reports/security-stack-utm-test-methodology-v10) | March 19, 2014 |
|  | [Security Stack (NGFW): Test Methodology v1.0](https://www.nsslabs.com/reports/security-stack-ngfw-test-methodology-v10)  | March 19, 2014 |
|  | [Next Generation Intrusion Prevention Systems (NGIPS): Test Methodology v1.0](https://www.nsslabs.com/reports/next-generation-intrusion-prevention-systems-ngips-test-methodology-v10) | March 10, 2014 |
|  | [Distributed Denial-of-Service (DDoS) Prevention: Test Methodology v1.0](https://www.nsslabs.com/reports/distributed-denial-service-ddos-prevention-test-methodology-v10) | January 31, 2014 |
|  | [Hypervisors For x86 Virtualization: Test Methodology v1.0](https://www.nsslabs.com/reports/hypervisors-x86-virtualization-test-methodology-v10) | December 02, 2013 |
|  | [Web Application Firewall: Test Methodology v6.2](https://www.nsslabs.com/reports/web-application-firewall-test-methodology-v62) | September 05, 2013 |
|  | [Security Stack (Network Devices): Test Methodology v1.5](https://www.nsslabs.com/reports/security-stack-network-devices-test-methodology-v15) | August 14, 2013 |
|  | [Online Financial Transaction Isolation: Test Methodology v1.6](https://www.nsslabs.com/reports/online-financial-transaction-isolation-test-methodology-v16) | June 17, 2013 |
|  | [Network Firewall - Data Center: Test Methodology v1.0](https://www.nsslabs.com/reports/network-firewall-data-center-test-methodology-v10) | May 01, 2013 |
|  | [Network Intrusion Prevention Systems (IPS) - Data Center: Test Methodology v1.1](https://www.nsslabs.com/reports/network-intrusion-prevention-systems-ips-data-center-test-methodology-v11) | May 01, 2013 |
|  | [Breach Detection Systems: Test Methodology 1.5](https://www.nsslabs.com/reports/breach-detection-systems-test-methodology-15) | January 29, 2013 |
|  | [Network Intrusion Prevention Systems (IPS): Test Methodology v7.2](https://www.nsslabs.com/reports/network-intrusion-prevention-systems-ips-test-methodology-v72) | January 07, 2013 |
|  | [Phishing Protection: Test Methodology v2.0](https://www.nsslabs.com/reports/phishing-protection-test-methodology-v20) | December 04, 2012 |
|  | [Network Firewall: Test Methodology v4.1](https://www.nsslabs.com/reports/network-firewall-test-methodology-v41) | November 06, 2012 |
|  | [Security Stack: Test Methodology v1.5](https://www.nsslabs.com/reports/security-stack-test-methodology-v15) | November 01, 2012 |

* 1. **IEC 60950-1: Information Technology Equipment – Safety**

This standard is applicable to mains-powered or battery-powered information technology equipment, including electrical business equipment and associated equipment, with a RATED VOLTAGE not exceeding 600 V and designed to be installed in accordance with the Canadian Electrical Code, Part I, CSA C22.1-12; General Requirements - Canadian Electrical Code, Part II, CSA C22.2 No. 0-10; the National Electrical Code, NFPA 70-2014; and the National Electrical Safety Code, IEEE C2-2012.The standard is also applicable to equipment, unless otherwise identified by a marking or instructions, designed to be installed in accordance with Article 645 of the National Electrical Code, ANSI/NFPA 70, and the Standard for the Protection of Information Technology Equipment, NFPA 75-2013. This standard is also applicable to following information technology equipment:

* designed for use as telecommunication terminal equipment and telecommunication network infrastructure equipment, regardless of the source of power;
* designed and intended to be connected directly to, or used as infrastructure equipment in, a cable distribution system, regardless of the source of power;
* Designed to use the AC mains supply as a communication transmission medium (see Clause 6, Note 4 and 7.1, Note 4).
* Components and subassemblies intended for incorporation in these equipment. Such components and subassemblies need not comply with every requirement of the standard, provided that the complete equipment, incorporating such components and subassemblies, does comply;
* external power supply units intended to supply other equipment within the scope of this part of IEC 60950;
* Accessories intended to be used with equipment within the scope of this part of IEC 60950.

Requirements additional to those specified in this standard may be necessary for:

* equipment intended for operation in special environments (for example, extremes of temperature; excessive dust, moisture or vibration; flammable gases; and corrosive or explosive atmospheres);
* electro-medical applications with physical connections to the patient;
* equipment intended to be used in vehicles, on board ships or aircraft, in tropical countries, or at altitudes greater than 2 000 m;
* Equipment intended for use where ingress of water is possible; for guidance on such requirements and on relevant testing, see Annex t.

This standard does not apply to:

* power supply systems which are not an integral part of the equipment, such as motor-generator sets, battery backup systems and distribution transformers;
* building installation wiring;
* Devices requiring no electric power.
	1. **IEC 61000: Electromagnetic Compatibility (EMC)**

Electromagnetic compatibility (EMC) is the branch of electrical engineering concerned with the unintentional generation, propagation and reception of electromagnetic energy which may cause unwanted effects such as electromagnetic interference (EMI) or even physical damage in operational equipment. The goal of EMC is the correct operation of different equipment in a common electromagnetic environment.

EMC pursues two main classes of issue. **Emission** is the generation of electromagnetic energy, whether deliberate or accidental, by some source and its release into the environment. EMC studies the unwanted emissions and the countermeasures which may be taken in order to reduce unwanted emissions. The second class, **susceptibility** is the tendency of electrical equipment, referred to as the victim, to malfunction or break down in the presence of unwanted emissions, which are known as Radio frequency interference (RFI). **Immunity** is the opposite of susceptibility, being the ability of equipment to function correctly in the presence of RFI, with the discipline of “hardening” equipment being known equally as susceptibility or immunity. A third class studied is **coupling**, which is the mechanism by which emitted interference reaches the victim.

Interference mitigation and hence electromagnetic compatibility may be achieved by addressing any or all of these issues, i.e., quieting the sources of interference, inhibiting coupling paths and/or hardening the potential victims. In practice, many of the engineering techniques used, such as grounding and shielding, apply to all three issues.

Electromagnetic compatibility testing for information technology includes:

Emission tests:

• Electromagnetic radiation (radiation and conductivity), based on ISIRI-EN-BS55022 standard

• Transmission by disrupting power lines, based on the standards IEC 61000 2-3 / 3-3

Immunity tests:

• Induction radio frequency electromagnetic fields, according to Standard IEC 61000 4-6

• Radio frequency electromagnetic fields emission, according to Standard IEC 61000 4-3

• Disorders supply lines, based on the standard IEC 61000 4-2

• Electrical pulses bursts, according to Standard IEC 61000 4-4

• Surges, according to Standard IEC 61000 4-5

The structure of the IEC 61000 series reflects the subjects dealt with by Basic EMC publications. As can be seen in the following, they include terminology, descriptions of electromagnetic phenomena and the EM environment, measurement and testing techniques, and guidelines on installation and mitigation. Note that Part 3 does not contain Basic EMC publications but is listed here for completeness as it is part of the 61000 series.

This large and considerably subdivided series of standards and technical reports will eventually consist of nine parts. Since the titles of Parts 7 and 8 are still open, the present structure is as follows:

Part 1: General

* The safety function requirements (what the function does); and
* The safety integrity requirements (the likelihood of a safety function being performed satisfactorily).

Part 2: Environment

* Description of the environment
* Classification of the environment
* Compatibility levels

Part 3: Limits

* Emission limits
* Immunity limits (insofar as they do not fall under the responsibility of product committees)

Part 4: Testing and measurement techniques

* Measurement techniques
* Testing techniques

Part 5: Installation and mitigation guidelines

* Installation guidelines
* Mitigation methods and devices

Part 6: Generic standards

Part 9: Miscellaneous

* 1. **EN 55022: Information Technology Equipment - Radio disturbance characteristics**

EN 55022 is a modified derivative of CISPR 22 and applies to, as the name implies, information technology equipment (ITE). Procedures are given for the measurement of the levels of spurious signals generated by the ITE and limits are specified within the standard for protection of radio services in industrial, commercial or residential environments.

The standard is produced by CENELEC, the European Committee for Electro technical Standardization. CENELEC is the European organization responsible for standardization in electrical and electronic engineering field.

In this standard, ITE is subdivided into two categories denoted class A and class B.

Class B is intended primarily for use in the domestic environment and may include:

* Equipment with no fixed place of use; for example. portable equipment powered by built-in batteries;
* telecommunication terminal equipment powered by a telecommunication network;
* Personal computers and auxiliary connected equipment.

Class A is a category of all other ITE which satisfies the class A limits but not the class B limits. The following warning shall be included in the instructions for use:

* 1. **EN 55024: Information Technology Equipment - Immunity characteristics**

EN 55024 is equivalent to CISPR 24 and applies to, as the name implies, information technology equipment (ITE). EN 55024 defines the immunity test requirements for information technology equipment in relation to continuous and transient conducted and radiated disturbances.

Tests within the standard include Electrostatic Discharges (ESD), Electrical Fast Transients (EFT), Surge, Power Frequency Magnetic Fields, Power interruptions, Radio Frequency Interference (RFI).

1. **Case Study: Testing a Sample Switch**

In this section we present a sample switch test scenario and discuss the results briefly to illustrate the test procedure.

* 1. **RFC 2544**

In this section we present a sample test on a 3Com 4800G switch based on RFC 2544 [1]. This includes throughput, latency and frame loss evaluations.

* + 1. **Throughput**

This part of the test measures the maximum rate at which none of the offered frames are dropped by the device/system under test (DUT/SUT).

The procedure is to send a specific number of frames at a specific rate through the DUT and then count the frames that are transmitted by the DUT. If the count of offered frames is not equal to the count of received frames, i.e. fewer frames are received compared to those transmitted, the rate of the offered stream is reduced and the test is rerun.

As seen in *Figure 5*, the sample device has been able to forward the packets with the maximum load (100%).



*Figure 5- Throughput Test Chart*

*Table 6- Throughput Test Details*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Frame Size** | **Intended Load (%)** | **Offered Load (%)** | **Throughput (%)** | **Aggregated Throughput (fps)** | **Aggregated Throughput max (fbps)** | **Aggregated Throughput (Mbps)** | **Aggregated Theoretical Max (Mbps)** |
| **64** | 100 | 100 | 100 | 35714286 | 35714285.71 | 24000 | 24000 |
| **128** | 100 | 100 | 100 | 20270270 | 20270270.27 | 24000 | 24000 |
| **256** | 100 | 100 | 100 | 10869566 | 10869565.22 | 24000 | 24000 |
| **512** | 100 | 100 | 100 | 5639098 | 5639097.74 | 24000 | 24000 |
| **1024** | 100 | 100 | 100 | 2873564 | 2873563.22 | 24000 | 24000 |
| **1280** | 100 | 100 | 100 | 2307692 | 2307692.31 | 24000 | 24000 |
| **1518** | 100 | 100 | 100 | 1950585 | 1950585.18 | 24000 | 24000 |

* + 1. **Latency**

This test measures the round-trip time taken by a test frame to travel through a network device or across the network and back to the test port. ***Latency*** is the time interval that begins when the last bit of the input frame reaches the input port and ends when the first bit of the output frame is seen on the output port. It is the time taken by a bit to go through the network and back. Latency variability can be a problem. With protocols like voice over Internet protocol (VoIP), a variable or long latency can cause degradation in voice quality.

*Figure 6* and *Table 7* show the minimum, maximum and average latencies for the sample device. The values conform to the claimed values of the vendor.

**

*Figure 6- Latency Test Chart*

*Table 7- Latency Test Details*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Frame Size (Bytes)** | **Intended Load (%)** | **Min Latency (µs)** | **Avg. Latency (µs)** | **Max Latency (µs)** |
| **64** | 100 | 2.71 | 3.82 | 6.50 |
| **128** | 100 | 2.68 | 3.80 | 6.47 |
| **256** | 100 | 2.71 | 3.80 | 6.47 |
| **512** | 100 | 2.69 | 3.79 | 6.46 |
| **1024** | 100 | 2.7 | 3.77 | 6.44 |
| **1280** | 100 | 2.73 | 3.77 | 6.42 |
| **1518** | 100 | 2.8 | 3.78 | 651 |

* + 1. **Frame Loss**

Considering the throughput test of Section 4.1.1, there is no frame loss for this device.

* 1. **RFC 2889**

In this section we present the results of applying RFC 2889 [2] on the same 3Com 4800G switch. This includes Address Caching Capacity (ACC), Address Learning Rate (ALR), Broadcast Frame Forwarding and Latency, Congestion Control, Faulty (with error) Frame Filtering, and Forward Pressure Rate test.

* + 1. **Address Caching Capacity (ACC)**

This test is applied to determine the address caching capacity of a LAN switching device as defined in RFC 2285 [24]. *Table 8* shows a summary of the results of ACC test. As indicated in the table, the caching capacity of the device under test is 28683 addresses at most.

*Table 8- Summary of ACC Test*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Trial** | **Address Count** | **Test status** | **Tx Sig Frames** | **Rx Sig Frames** | **Rx Frames** | **Expected Rx Frames** | **Flood Frames** | **Expected Frames** | **Lost Frames** | **Loss (%)** | **Caching Capacity** |
| 1 | 28683 | Passed | 28683 | 28683 | 28683 | 28683 | 0 | 28683 | 0 | 0 | 28683 |

* + 1. **Address Learning Rate (ALR)**

This test is applied to determine the rate of address learning of a LAN switching device. *Table 9* shows a summary of the results of ALR test. As indicated in the table, the address learning rate of the device under test is 1487997 frames per second at most.

*Table 9- Summary of ALR Test*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Trial** | **Address Count** | **Test status** | **Intended Load (%)** | **Tx Sig Frames** | **Rx Sig Frames** | **Rx Frames** | **Expected Rx Frames** | **Flood Frames** | **Expected Frames** | **Learning Rate (fps)** |
| 1 | 20000 | Passed | 99.99 | 20000 | 20000 | 20000 | 20000 | 0 | 20000 | 1487997 |

* + 1. **Broadcast Frame Forwarding and Latency**

The objective of the Broadcast Frame Forwarding and Latency Test is to determine the throughput and latency of the DUT when forwarding broadcast traffic. The ability to forward broadcast frames will depend upon a specific function built into the device for that purpose. It is therefore necessary to determine the ability of DUT/SUT to handle broadcast frames, since there may be many different ways of implementing such a function. *Figure 7*, *Figure 8*, *Table 10* and *Table 11* show the results of applying the tests on our sample device.

*Table 10- Broadcast Frame Forwarding Test Details*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Frame Size** | **Burst Size** | **Throughput (%)** | **Intended Load (%)** | **Offered Load (%)** | **Result** | **Forwarding Rate** |
| **64** | 1 | 100 | 100 | 100 | Passed | 34226190 |
| **128** | 1 | 100 | 100 | 100 | Passed | 19425675 |
| **256** | 1 | 100 | 100 | 100 | Passed | 10416667 |
| **512** | 1 | 100 | 100 | 100 | Passed | 5404135 |
| **1024** | 1 | 100 | 100 | 100 | Passed | 2753832 |
| **1280** | 1 | 100 | 100 | 100 | Passed | 2211539 |
| **1518** | 1 | 100 | 100 | 100 | Passed | 1869311 |



*Figure 7-Broadcast Frame Forwarding Summary Results*

*Table 11- Broadcast Frame Forwarding Test Details*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Frame Size** | **Min Latency (µs)** | **Avg. Latency (µs)** | **Max Latency (µs)** | **Min Jitter (µs)** | **Avg. Jitter (µs)** | **Max Jitter (µs)** |
| **64** | 2.97 | 3.27 | 3.57 | 0 | 0 | 0 |
| **128** | 3.17 | 3.39 | 3.63 | 0 | 0 | 0 |
| **256** | 2.78 | 3.07 | 3.35 | 0 | 0 | 0 |
| **512** | 2.73 | 3.01 | 3.26 | 0 | 0 | 0 |
| **1024** | 3.14 | 3.37 | 3.68 | 0 | 0 | 0 |
| **1280** | 2.85 | 3.15 | 3.4 | 0 | 0 | 0 |
| **1518** | 3.01 | 3.23 | 3.48 | 0 | 0 | 0 |



*Figure 8-Broadcast Frame Latency Summary Results*

* + 1. **Congestion Control**

The objective of this test is to determine how a DUT handles congestion. Does the device implement congestion control and does congestion on one port affect an uncongested port? This procedure determines if “Head of Line Blocking” and/or “Backpressure” are present.

*Table 12* shows the results of applying the tests on our sample device. The table shows that our sample device does not have “Head of Line Blocking” and does not perform “Backpressure” for congestion control.

*Table 12- Congestion Control Test Details*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **FrameSize (Byte)** | **BurstSize** | **IntendedLoad (%)** | **PortType** | **OfferedLoad (%)** | **FrameLoss (%)** | **HOLBExists** | **BPExists** |
| 64 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 64 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 64 | 0 | 0 | Uncongested | 0 | 0 | **0** | 0 |
| 64 | 0 | 0 | Congested | 0 | 33.33 | 0 | **0** |
| 128 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 128 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 128 | 0 | 0 | Uncongested | 0 | 0 | **0** | 0 |
| 128 | 0 | 0 | Congested | 0 | 33.33 | 0 | **0** |
| 256 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 256 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 256 | 0 | 0 | Uncongested | 0 | 0 | **0** | 0 |
| 256 | 0 | 0 | Congested | 0 | 33.33 | 0 | **0** |
| 512 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 512 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 512 | 0 | 0 | Uncongested | 0 | 0 | **0** | 0 |
| 512 | 0 | 0 | Congested | 0 | 33.32 | 0 | **0** |
| 1024 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 1024 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 1024 | 0 | 0 | Uncongested | 0 | 0 | **0** | 0 |
| 1024 | 0 | 0 | Congested | 0 | 33.32 | 0 | **0** |
| 1280 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 1280 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 1280 | 0 | 0 | Uncongested | 0 | 0 | **0** | 0 |
| 1280 | 0 | 0 | Congested | 0 | 33.32 | 0 | **0** |
| 1518 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 1518 | 1 | 100 | Transmit | 100 | 0 | 0 | 0 |
| 1518 | 0 | 0 | Uncongested | 0 | 0 | **0** | 0 |
| 1518 | 0 | 0 | Congested | 0 | 33.32 | 0 | **0** |

* + 1. **Faulty (with error) Frame Filtering**

The objective of the faulty frames filtering test is to determine the behavior of the DUT under faulty or abnormal frame conditions. The results of the test indicate if the DUT/SUT filters the errors, or simply propagates the faulty frames along to the destination

*Table 13* shows the results of applying the test on our sample device. The table shows that none of the faulty frames are sent to the destination and all are dropped.

*Table 13- Faulty Frame Filtering Test Results*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ErrorType** | **TestStatus** | **IntendedLoad (%)** | **Tx Sig Frame Count** | **Rx Sig Frame Count** | **Tx Non Sig Frame Count** | **Rx Non Sig Frame Count** | **OversizeFrames** | **UndersizeFrames** | **CRC Error Frames** |
| CRC | **Passed** | 100 | 178571430 | 0 | 0 | 92 | 0 | 0 | 0 |
| Oversize | **Passed** | 100 | 9721324 | 0 | 0 | 88 | 0 | 0 | 0 |
| Undersize | **Passed** | 100 | 180722892 | 0 | 0 | 91 | 0 | 0 | 0 |

* + 1. **Forward Pressure Rate**

The Forward Pressure test overloads a DUT/SUT port and measures the output for forward pressure. If the DUT/SUT transmits frames with an inter-frame gap will be less than 96 bits, then forward pressure is detected.

*Table 14* shows the results of applying the test on our sample device. The results show that even if the inter-frame gap is less than 96 bits frames, the device forwards them in the standard form.

*Table 14- Forward Pressure Rate Test Results*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **FrameSize (Byte)** | **ForwardPressure** | **IntendedLoad (%)** | **OfferedLoad (%)** | **OfferedLoad (fps)** | **ForwardingRate (fps)** | **FrameLoss (%)** | **Other Frames** | **Flood Count** |
| 64 | **FALSE** | 101.20 | 101.21 | 36144578.4 | 35714722 | 1.188 | 0 | 0 |
| 128 | **FALSE** | 100.68 | 100.68 | 20408163.6 | 20270571 | 0.673 | 0 | 0 |
| 256 | **FALSE** | 100.36 | 100.36 | 10909091.2 | 10869729 | 0.36 | 0 | 0 |
| 512 | **FALSE** | 100.19 | 100.19 | 5649717.6 | 5639181 | 0.185 | 0 | 0 |
| 1024 | **FALSE** | 100.10 | 100.10 | 2876318.4 | 2873606 | 0.093 | 0 | 0 |
| 1280 | **FALSE** | 100.08 | 100.08 | 2309469.2 | 2307720 | 0.074 | 0 | 0 |
| 1518 | **FALSE** | 100.07 | 100.07 | 1951854.4 | 1950615 | 0.062 | 0 | 0 |

1. **Switch and Router Evaluation Criteria**

*Table 15* and *Table 16* present our proposed switch and router acceptance criteria. These criteria are based on the test results obtained in the “Network Equipment Test and Evaluation Laboratory” (Sharif University of Technology, Tehran, Iran) and the general requirements of different categories of switch and router.

*Table 15- Switch Evaluation Criteria*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **High Availability** | **Environmental. conditions** | **Manage-ability** | **SNMP support** | **Trunk support** | **Vlan support** | **QoS support** | **STP support** | **Avg. delay** | **Through-put** | **Switch category** |
| Opt | Normal home or office environment | Opt\* | Opt | Opt | Opt | Opt | Yes | 1ms | 60% | Home or small office |
| Opt | Temperature 0-40 °CHumidity 10% to 90%Unsaturated | Opt | Opt | Opt | Opt | Opt | Yes | 500µs | 75% | Access layer |
| Opt | As above | Mandat\* | Mandat | Mandat | Mandat | Mandat | Yes | 300 µs | 80% | Distribution layer |
| Mandat | As above | Mandat | Mandat | Mandat | Mandat | Mandat | Yes | <100 µs | >95% | Core layer |
| Mandat | As above | Mandat | Opt | Opt | Mandat | Mandat | Yes | 200 µs | 85% | Industrial |

\* Opt: Optional, Mandat: Mandatory

*Table 16- Router Evaluation Criteria*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Support for High Availability** | **Environmental conditions** | **SNMP support** | **BGP4 support** | **OSPF support** | **RIP support** | **Minimum system Backplane throughput**  | **Router Category** |
| Opt | Normal home or office environment | Opt | Opt | Opt | Opt\* | 1 Mbps | Home or small office |
| Opt | Temperature 0-40 °CHumidity 10% to 90%Unsaturated | Mandat | Opt | Mandat | Mandat\* | 1 Gbps | branch |
| Mandat | As above | Mandat | Mandat | Mandat | Mandat | 10 Gbps | Distribution layer |
| Mandat | As above | Mandat | Mandat | Mandat | Mandat | 1Tbps | Core layer |
| Mandat | Hard conditionsIEC 61850 | Mandat | Opt | Opt | Opt | 10Mbps | Industrial |

\* Opt: Optional, Mandat: Mandatory

1. **Case Study: Testing a Sample Firewall**

In this section, we present a sample test on a Cisco ASA5545-K9 firewall. It is worth noting that measuring the performance a firewall and its impact on firewall security functions (and vice versa) has not traditionally been taken into the consideration according to CC or 15408 Standard. However, more and more organizations are interested in the performance of their security devices because it is now clear that when you send lots of traffic on a security device it may fail to resist or control all rules configured for, and reciprocally, it can slow down the normal or legitimate traffic due to multiple rule control on traversing traffic. That is why we insist on the necessity of performance test beside traditional or improved security test.

* 1. **Performance**

The performance test includes the following measurements:

* IP throughput, frame loss and latency according to RFC 2544.
* IP throughput, frame loss and latency for Internet mix (IMIX) traffic.
* Maximum Capacity.
	+ 1. **Throughput**

In this test we determine the throughput of network-layer data traversing the DUT, as defined in RFC 1242 [25]. The test is based on RFC 2544 discussed in Section 1. The results are presented in *Figure 9* and *Table 26*.



*Figure 9- Throughput Test Chart*

*Table 17- Throughput Test Details*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Frame Size(Byte) | IntendedLoad (%) | OfferedLoad (%) | Throughput (%) | AggregatedThroughput (fps) | AggregatedTheoretical Max (fps) | AggregatedThroughput (Mbps) | AggregatedTheoretical Max (Mbps) |
| 64 | 7.961 | 7.961 | 7.961 | 947730.8 | 11904761.91 | 636.875 | 8000 |
| 128 | 14.148 | 14.148 | 14.148 | 955975.6 | 6756756.757 | 1131.875 | 8000 |
| 256 | 26.523 | 26.523 | 26.523 | 960994.133 | 3623188.406 | 2121.875 | 8000 |
| 512 | 51.273 | 51.273 | 51.273 | 963786.533 | 1879699.248 | 4101.875 | 8000 |
| 1024 | 99.227 | 99.227 | 99.227 | 950446 | 957854.406 | 7938.125 | 8000 |
| 1280 | 99.227 | 99.227 | 99.227 | 763281.333 | 769230.769 | 7938.126 | 8000 |
| 1518 | 99.227 | 99.227 | 99.227 | 645166.267 | 650195.059 | 7938.126 | 8000 |

* + 1. **Latency**

The results of the Latency test are presented in *Figure 10* and *Table 27*.

**

(Byte)

(Byte)

*Figure 10- Latency Test Chart*

*Table 18- Latency Test Details*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Frame Size (Byte) | Min Latency(us) | Avg Latency(us) | Max Latency(us) | Min Jitter(us) | Avg Jitter(us) | Max Jitter(us) |
| 64 | 10.77 | 132.99 | 2420.70 | 0.01 | 14.14 | 1237.85 |
| 128 | 15.19 | 176.91 | 2517.06 | 0.00 | 13.33 | 1311.33 |
| 256 | 19.24 | 218.59 | 3265.43 | 0.00 | 11.34 | 1355.06 |
| 512 | 23.58 | 254.20 | 3297.62 | 0.00 | 7.56 | 1331.40 |
| 1024 | 32.78 | 312.29 | 2458.76 | 0.00 | 0.10 | 1390.23 |
| 1280 | 31.12 | 111.90 | 2437.81 | 0.00 | 0.13 | 1407.95 |
| 1518 | 46.57 | 87.88 | 1587.33 | 0.00 | 0.16 | 1044.07 |

* + 1. **Frame Loss**

The results of the Frame Loss test are presented in *Table 19*.

*Table 19- Frame Loss Details*

|  |  |  |  |
| --- | --- | --- | --- |
| Frame Size(bytes) | IntendedLoad (%) | OfferedLoad (%) | Min FrameLoss (%) |
| 64 | 100 | 100 | 91.69 |
| 64 | 50.5 | 50.5 | 83.52 |
| 64 | 25.75 | 25.75 | 67.77 |
| 64 | 13.375 | 13.375 | 37.81 |
| 64 | 10.281 | 10.281 | 19.12 |
| 64 | 8.734 | 8.734 | 4.79 |
| 128 | 100 | 100 | 85.35 |
| 128 | 50.5 | 50.5 | 70.99 |
| 128 | 25.75 | 25.75 | 43.11 |
| 128 | 19.563 | 19.563 | 25.03 |
| 128 | 16.469 | 16.469 | 11.02 |
| 128 | 14.922 | 14.922 | 1.85 |
| 256 | 100 | 100 | 72.71 |
| 256 | 50.5 | 50.5 | 45.93 |
| 256 | 38.125 | 38.125 | 28.39 |
| 256 | 31.938 | 31.938 | 14.55 |
| 256 | 28.844 | 28.844 | 5.34 |
| 256 | 27.297 | 27.297 | 0.08 |
| 512 | 100 | 100 | 47.42 |
| 512 | 75.25 | 75.25 | 30.15 |
| 512 | 62.875 | 62.875 | 16.38 |
| 512 | 56.688 | 56.688 | 7.24 |
| 512 | 53.594 | 53.594 | 1.89 |
| 512 | 52.047 | 52.047 | 0.00 |
| 1024 | 100 | 100 | 0.18 |
| 1280 | 100 | 100 | 0.14 |
| 1518 | 100 | 100 | 0.12 |

* + 1. **Throughput with IMIX traffic**

IMIX traffic is often used by firewall vendors showing IMIX throughput performance in their data sheets. The IMIX traffic combination used in this test is shown in *Table 20*. The results of the throughput test on IMIX traffic are presented in *Figure 11* and *Table 21*.

*Table 20- IMIX Traffic Combination*





*Figure 11- Throughput with IMIX traffic Test Chart*

*Table 21- Throughput with IMIX traffic Test Details*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| iMIX  Distribution | IntendedLoad (%) | OfferedLoad (%) | Throughput (%) | AggregatedThroughput (fps) | AggregatedTheoretical Max (fps) | AggregatedThroughput (Mbps) | AggregatedTheoretical Max (Mbps) |
| Default | 37.352 | 37.706 | 37.706 | 987770.933 | 2777777.778 | 3016.488 | 8000 |

* + 1. **IMIX Latency**

The results of the IMIX latency test are presented in *Figure 12* and *Table 22*.



*Figure 12- Latency with IMIX Traffic Test Chart*

*Table 22- Latency with IMIX Traffic Test Details*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Min Latency | Avg. Latency | Max Latency | Min Jitter | Avg. Jitter | Max Jitter |
| 16.73 | 202.144 | 2113.36 | 0 | 9.486 | 1219.11 |

* + 1. **IMIX Frame Loss**

The results of the IMIX frame loss test are presented in *Table 23*.

*Table 23- Frame Loss Details*

|  |  |  |  |
| --- | --- | --- | --- |
| iMIX  Distribution | IntendedLoad (%) | OfferedLoad (%) | Min FrameLoss (%) |
| Default | 100 | 100 | 60.62 |
| Default | 50.5 | 50.88 | 22.64 |

* + 1. **Maximum Capacity**

In this test we evaluate the following performance measures:

* **Concurrent TCP Connection Capacity:** The maximum number of concurrent TCP connections supported through the DUT, as defined in RFC 2647. This test is intended to find the maximum number of entries the DUT can store in its connection table.
* **Maximum TCP Connections Per Second (Maximum TCP Connection Establishment Rate):** The maximum TCP connection establishment rate through or with the DUT as defined by RFC 2647. This test is intended to find the maximum rate the DUT can update its connection table.
* **Maximum HTTP Transactions Per Second (Maximum HTTP Transaction Rate):** The maximum transaction rate the DUT can sustain. This test is intended to find the maximum rate at which users can access objects.

The results of this test on our sample firewall is shown in *Table 24*

*Table 24- Maximum Capacity Results*

|  |  |
| --- | --- |
| Test Name | Result |
| Concurrent TCP Connection Capacity | 750,000 |
| Maximum TCP Connections Per Second | 28,528 |
| Maximum HTTP Transactions Per Second | 40,000 |

* 1. **Security Features**

The security features include:

* **Baseline Policy:** Route traffic from one port to another, e.g., route LAN traffic to WAN.
* **Logging:** Log security events like deny connection, detect attacks , ….
* **Packet filtering:** Filter packets based on security rules like filter based on destination IP and Port, source IP , …
* **IP Address Spoofing Protection:** Attacker from the external network may try to access the internal network by spoofing the IP address of an internal IP address.
* **SYN Flood Protection:** The DUT is expected to protect itself and internal servers against SYN flood attack.

The sample firewall has all the above four features. (*Table 25*)

*Table 25- Security Features*

|  |  |
| --- | --- |
| Test Name | Result |
| Baseline Policy | **PASS** |
| Logging | **PASS** |
| SYN Flood Protection | **PASS** |
| IP Address Spoofing Protection | **PASS** |

1. **Security Evaluation Criteria**

The three main tests for security device evaluation are performance, security characteristics and reactions to attacks. The evaluation should be performed based on the results of all these tests.

*Table 26* shows the classification of security devices based on performance measures. The performance measures include throughput, Concurrent TCP Connections, maximum TCP connections and maximum HTTP transaction rate. The tested device is considered to be in one of the categories A, B, C, D or F (fail) according to these measures.

*Table 26- Network Security Device Classification based on Performance Measure Percentage*

|  |  |
| --- | --- |
|  | **Performance Measure Percentage** |
|  | **A** | **B** | **C** | **D** | **F** |
| **Firewall** | 95% | 85% | 75% | 65% | less than 65% |
| **IPS/IDS** | 90% | 80% | 70% | 60% | less than 60% |

*Table 27* presents, as an initial suggestion, the minimum required criteria for network security device evaluation. These criteria are based on security characteristics and reactions to attacks tests. The criteria mentioned in *Table 27* include:

* **Baseline Policy**: Considering that firewall and IPS are active network devices, they ought to have basic routing capability. However, an IDS is a passive device that only monitors the passing traffic so it does not need to have this capability.
* **Logging**: All security devices should be able to log security events for further analysis. Other activities such as users logging to system, or configuration changes , are readily observable through system logs.
* **Packet Filtering Protection**: Regarding the functionality of IPS and firewall, they have to be able to perform packet filtering based on security policies.
* **IP Spoofing Protection**: As the security policies of IPS and firewall are usually expressed with IP addresses, devices should be able to detect IP spoofing for accurate policy application.
* **SYN Flood Attack Protection**: IPS and firewall should be able to detect and prevent SYN flooding since they could not accept new connections in the presence of a SYN flooding attack.
* **Attack Detection and Prevention**: Attack detection and attack detection/prevention are the main jobs of IDS and IPS respectively.

*Table 27- Minimum Required Criteria for Network Security Devices*

|  |  |  |
| --- | --- | --- |
|  | **Security Characteristics** | **Reactions to Attacks** |
| **Device** | **•Baseline Policy** | **Logging** | **Packet Filtering** | **IP Spoofing** | **SYN Flood Attack** | **Attack Detection** | **Attack Prevention** |
| **Firewall** | ✓ | ✓ | ✓ | ✓ | ✓ | - | - |
| **IDS** | - | ✓ | - | - | - | - | - |
| **IPS** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**8. Conclusion**

As IT equipment are widely used in the fields that may impact communication infrastructure, devices, environment or the life of users, we think that new regulations should be defined and applied for them. These regulations must not only take into the consideration traditional radio communication standards (such as SAR, EMC, EMI, safety) but also should have a look on performance or security issues as well as green environment. In this study we categorized IT equipment, surveyed different applicable standards, and proposed several draft criteria for some specific network and security devices. We think that this is the beginning of a challenging though interesting international effort and cooperation for proposing the best practices of such regulations. We hope that this work will encourage more people to contribute to the definition of new and suitable IT equipment Type Approval and test standards.

**References**

1. <https://www.ietf.org/rfc/rfc2544.txt>
2. <https://tools.ietf.org/html/rfc2988>
3. https://tools.ietf.org/html/rfc6076
4. <https://tools.ietf.org/html/rfc7501>

1. <https://tools.ietf.org/html/rfc>7502
2. 7502 ETSI TS 132 409 V7.3.0 (2009-01) Technical Specification Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Performance Management (PM); Performance measurements IP Multimedia Subsystem (IMS) (3GPP TS 32.409 version 7.3.0 Release 7)
3. ETSI TS 132 454 V10.0.0 (2011-04) Technical Specification Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Key Performance Indicators (KPI) for the IP Multimedia Subsystem (IMS) (3GPP TS 32.454 version 10.0.0 Release 10)
4. ETSI, TS. "102 027-3) Methods for Testing and Specification (MTS); Conformance Test Specification for SIP (IETF RFC 3261); Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT) proforma ; SIP ATS & PIXIT." European Telecommunications Standards Institute, Sophia Antipolis, France. (2006)
5. <https://tools.ietf.org/html/rfc4475>
6. ETSI, ES. "201 168 (V1. 1.1):" Corporate telecommunication Networks (CN)." Transmission characteristics of digital Private Branch Exchanges (PBXs).
7. Troy, Gene. "Introduction to the Common Criteria for IT Security (ISO 15408)." (1999)
8. <https://tools.ietf.org/html/rfc3511>
9. <https://www.nsslabs.com/reports/categories/methodologies>
10. International Electrotechnical Commission. "IEC 60950-1." Information technology equipment – Safety – Part1: General requirements” (2005)
11. International Electrotechnical Commission. "IEC 61000-4-7."Electromagnetic Compatibility, General Guide on Harmonics and Inter-harmonics Measurements and Instrumentation” (1991)
12. <http://www.rfemcdevelopment.eu/en/emc-emi-standards/en-55022-2010>
13. <http://rfemcdevelopment.eu/en/emc-emi-standards/en-55024-2010>
14. Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 15: Specific conditions for commercially available amateur radio equipment, ETSI EN 301 489-15 V1.2.1 (2002).
15. <https://tools.ietf.org/html/rfc3261>
16. <https://tools.ietf.org/html/rfc3264>
17. “Network Intrusion Prevention Systems Test Methodology V6.1”, NSS Labs
18. Directive, E. E. C. "European community." Council Directive 98 (1990): 83.
19. ETSI, EG. "201 120:" Public Switched Telephone Network (PSTN)." Method of rating terminal equipment so that it can be connected in series and/or in parallel to a Network Termination Point (NTP).
20. <https://tools.ietf.org/html/rfc2285>
21. https://www.ietf.org/rfc/rfc1242.txt
1. Digital Subscriber Line Access Multiplexer [↑](#footnote-ref-1)