वर्गीय आवश्यकताएँ

सं:टीईसी/जीआर/आईटी/एनटीएस-००१/०२/मार्च-१९

(सं:टीईसी/जीआर/एसडबल्यू/एनटीएस-एस०१/०१/फ़रवरी २०११ को अधिक्रमित करता है)

GENERIC REQUIREMENTS

No.: TEC/GR/IT/NTS-001/02/MAR-19

(Supersedes No. TEC/GR/SW/NTS-S01/01/FEB 2011)

एन टी पी सर्वर

(नेटवर्क टाइम प्रोटोकॉल सर्वर)

NTP SERVER

(Network Time Protocol Server)

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलाल भवन, जनपथ, नई दिल्ली–११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release 2: MARCH, 2019

Price: ₹ 800/-

FOREWORD

Telecommunication Engineering Centre(TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR), Essential Requirements (ER) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support to DOT on technology issues
- Testing & Certification of Telecom products

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This GR specifies the Generic Requirements of Network Time Protocol Server (NTPS) that enables service providers to synchronise the clocks of IP network and NGN based elements over a network to a common time base.

HISTORY SHEET

S.No.	*GR No.*	*Title*	*Remarks*
1.	TEC/GR/SW/NTS – S01/01/ FEB. 2011	Generic Requirement for NTP Server	Issue No. 1
2.	TEC/GR/IT/NTS-001/02/MAR-19	Generic Requirement for NTP Server	Issue No. 2

REFERENCES

S.NO.	Title	Document number
I : TEC GR/IRs		
1.	Electromagnetic Compatibility	TEC/SD/DD/EMC-221/05/OCT-16
2.	Standards for Environmental testing of Telecommunication Equipment	SD:QM-333
II : ITU Recommendations		
1.	ITU-T G.811, ITU-T G.812, ITU-T G.813	
III : IETF Recommendations		
1.	RFC 778, RFC 891, RFC 868, RFC 956, RFC 1305, RFC 1361, RFC 2030, RFC 3971, RFC 4330, RFC 5905 and RFC 5908	
IV: Other Standards		
1.	IEC 61000-4-2	
2.	IEC 61000-4-4	
3.	IEC 61000-4-3	
4.	IEC 61000-4-5	
5.	IEC 61000-4-6	
6.	IEC 61000-4-11	
7.	CISPR 11	
8.	Class A of , CISPR 32	
9.	ISO 9001:2000 9001:2015 to check	
10.	IS 8437 (1993) (equipment & IEC publications is 60479-1 (1984))	
11.	IS 13252 (2003) (equipment & IEC publications 60950 (2001-10)	

CHAPTER -1

1.0 Introduction

1.1 This document specifies the Generic Requirements of Network Time Protocol Server (NTPS) that enables service providers to synchronise the clocks of IP network and NGN based network elements to a common time base.

1.2 Rubidium or Oven controlled crystal oscillator OCXO (as per ITU G.812) based NTP servers can provide a highly stable timing reference. NTP servers with oscillators that have a higher Q factor provide a more stable timing reference. Rubidium or OCXO shall meet the ITU G.811 standard during the hold over period.

1.3 Standard reference clocks to NTP servers shall be Stratum 0 reference clocks.

1.4 NTP server is used in ICT network, such as Femto cell, for time distribution to IMS billing or logging of servers and soft-switches.

1.5 NTP and SNTP are protocols traditionally used to distribute time of day information. Packet-based methods are adaptive in nature, since they do not require the support of a network-wide synchronization reference. Therefore, the performance is impacted by packet delay variation in the network. In order to minimize the impact from the packet network using NTP packets, specific algorithms may need to be implemented at the client side.

1.6 The published standards for synchronization over packet networks are NTP (RFC 1305), SNTP (RFC 4330). SNTP based on RFC 2030 was obsoleted by RFC 4330. However, RFC 4330 is further obsoleted by RFC 5905. Publication of Version 4 of NTP that provides guidelines for deployment in telecommunications applications has been released (RFC 5905).

1.7 This document describes the functional, interconnectivity and other mandatory requirements of NTP Server. Desirable requirements have been described in Chapter 10.

1.8 For all ITU-T Recommendations, ETSI, 3GPP and IETF standards/ RFC referred in this document, the latest release shall be applicable.

1.9 For all TEC documents referred in this document, the latest issue with all associated Amendments, Addendum and Corrigendum shall be applicable.

2.0 DESCRIPTION

In the present IP based environment accurate time stamps are essential to everything from maintenance point of view and forensic analysis of distributed attacks, for charging information based on time- sensitive transaction. Time is also important to the function of routers and networks as it provides the frame of reference between all network elements. In case of security also the logs between each routers and network servers are to be correlated so that the picture of any incident may be developed reliably. All these functions are furnished by synchronization of time by use of a protocol called Network Time protocol (NTP).

2.1 Architecture

Figure 1 shows the connectivity of NTP Server (NTPS) which shall provide the correct network time in the simple computer network using the Network Time protocol (NTP). A NTP server is used to get the correct time from a time source and adjust the local time.

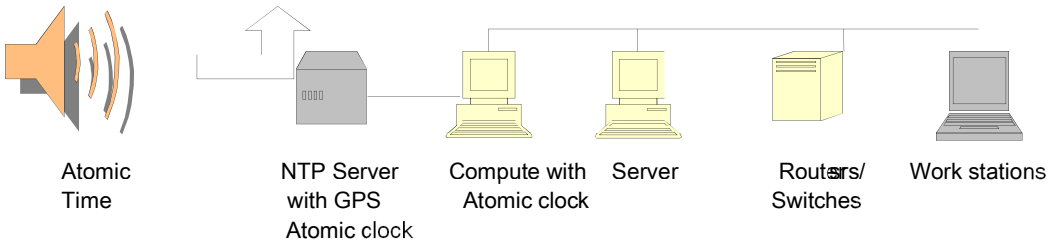

Figure 1

Stratum 0 serves as a reference clock and is the most accurate and highest precision time server (e.g., atomic clocks, GNSS clocks, and radio clocks.) Stratum 1 servers take their time from Stratum 0 servers and so on up to Stratum 15. (Refer Figure-2). A Stratum- 0 based Stratum 1 NTP server

can synchronise the time on network elements including computers by supplying the correct time for IP Network. The communication on a client is established through an exchange of packets with one or more stratum servers.

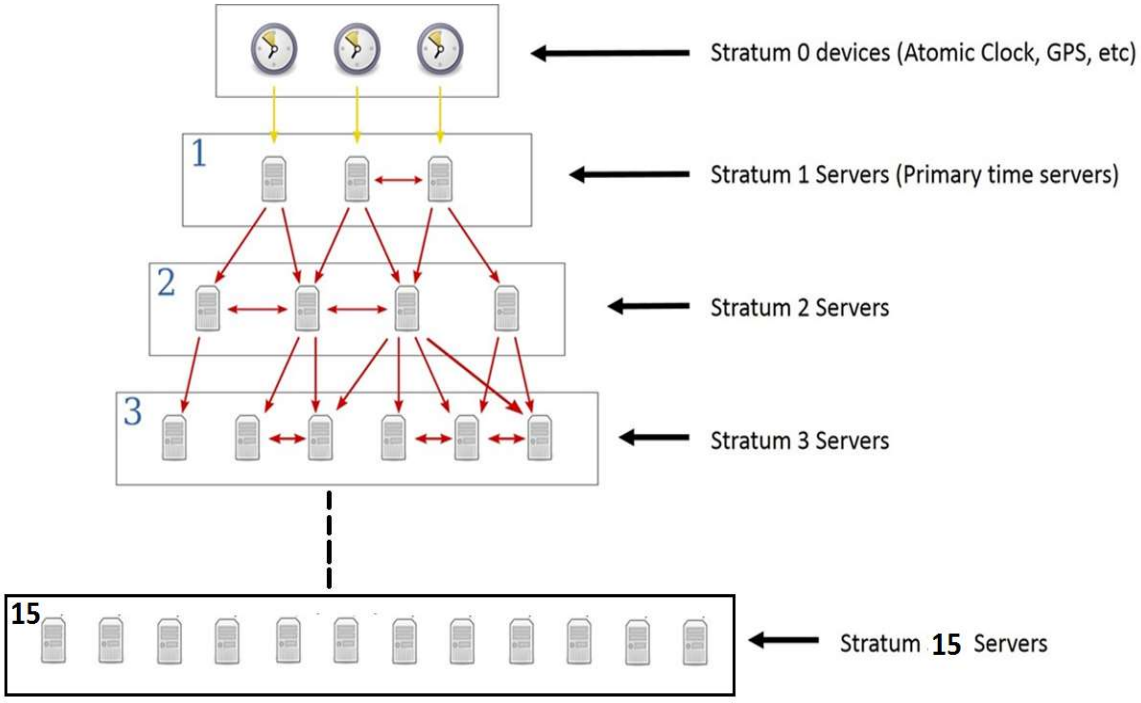

Figure-2

2.2 The network shall not use the Internet Time Server for synchronization due to the asymmetrical latency received in time.

2.3 The network shall use the dedicated network time server due to security risks in obtaining Internet time.

2.4 The NTP server shall be installed behind the firewall/SBC and thus it shall be kept on best security from internet side.

The use of NTP server in NGN Architecture is shown in Figure-3.

The NTP server is connected to the IP Networks or the Soft switch so that the Network is fully synchronised.

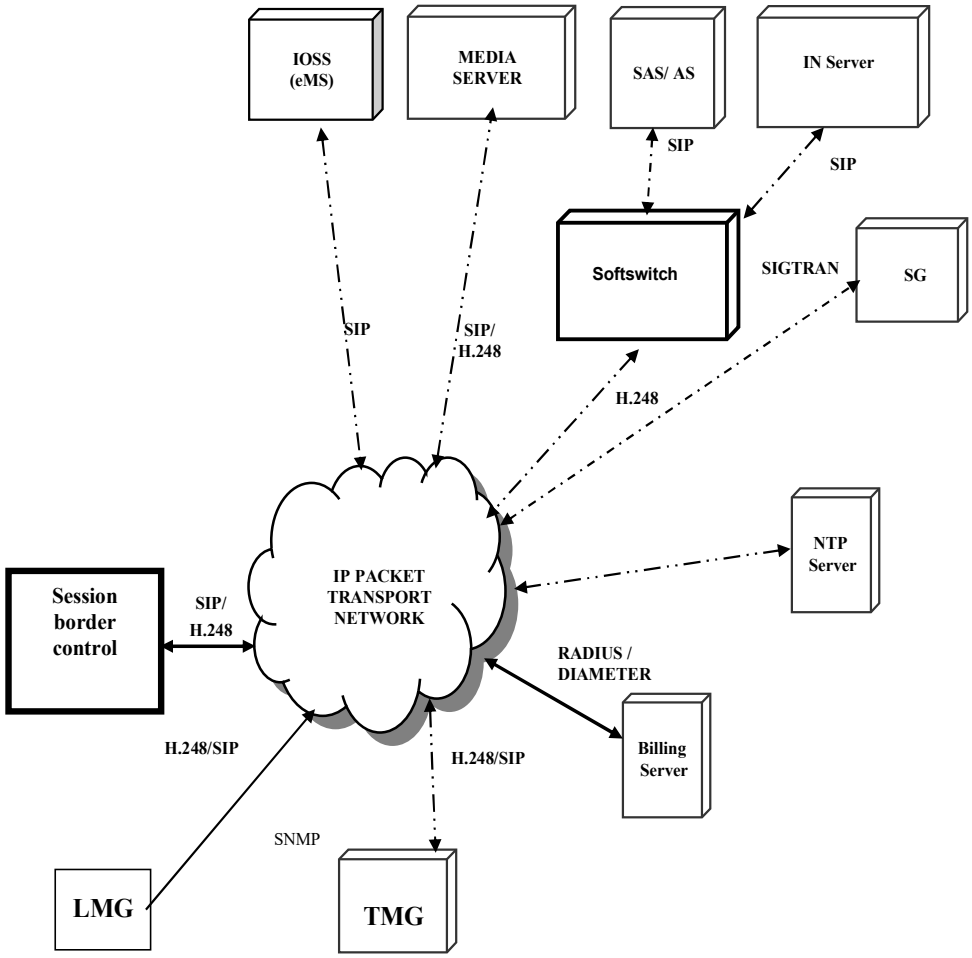

Figure 3: Use of NTP Server in NGN Environment

3.0 FUNCTIONAL REQUIREMENTS

3.1 General Requirements

3.1.1 NTP Server shall enable service providers to connect its network to most accurate time device and synchronise the network to external source.

3.1.2 The NTP Server shall use fault-tolerant, highly scalable, open-ended state-of-the-art hardware, software and networking technologies and provide carrier-grade performance.

3.1.3 NTP Server shall have capability to support NGN elements for synchronisation.

3.1.4 NTP Server shall have in-built rate limiting capability to protect against overload conditions.

3.1.5 NTP server shall be capable of handling a minimum of 250 **and a maximum of 4,00,000** authenticated transactions per second.

The NTP server are categorised as per following parameters: -

Product type	Accuracy	Capability Request / Sec	Quartz type
Type 1	Internal to GPS typically in a range of +/-10us to +/-100us	250 request / sec	TCXO Or OCXO
Type 2	Internal to GPS typically in a range of +/-10us to +/-100us	250 – 1500 req/sec per	TCXO Or OCXO
Type 3	Internal to GPS	10000	OCXO /

	typically < +/-50ns	request / sec	DOCXO / Rubidium
Type 4	Internal to GPS typically < +/-50ns	40000 request / sec	Rubidium
Type 5	Internal to GPS typically < +/-50ns	120000 request/sec	Rubidium
Type 6	Internal to GPS typically < +/-50ns	400000 request/sec	Rubidium

3.1.6 The server should be capable of accepting poll intervals of different timing.

3.1.7 The server shall have flexibility to respond to poll intervals of varied timings. However, a client shall not have a provision for poll interval less than 15 seconds under any condition. The server shall be capable of handling the request of the client server and the client shall use this exponential backoff to increase in the poll interval even when the server does not respond within reasonable time. The NTP server shall have the capability to be configured to perform as Local server too so that a client shall invariably be able to use it to avoid unnecessary traffic on backbone traffic.

3.1.8 Provision shall exist for the operator to configure IP addressing as per requirement. In case of default firmware, server IP address can be configured using DHCP server or the IP address provided by the server administrator.

3.1.9 The DNS server shall be used for resolving domain name/URL/IP addresses, enabling the operator to ensure effective load balancing among server clique and change IP address binding to canonical names. Further a client shall be capable to re-resolve the server IP address at intervals not less than the 'time to live field' in DNS response. A client shall support the

NTP access-refusal mechanism so that no more sending of request by client are allowed.

3.2 **Protocols and Standards**

3.2.1 NTP Server shall comply with the following Protocols/ specifications:

For operational details of NTP: RFC 868

- NTP Version 3 as per RFC 1305
- Simple NTP(SNTP) Version 4 as per RFC 4330
- NTP Version 4 as per RFC 5905

3.2.2 In addition to above, support of following NTP RFCs (as per their references) is required:

S.No.	Name of RFC	Reference& No.
1	For DHCP V6	5908

3.3 **Applications / Services**

NTP Server shall provide following types of NTP based Services/Applications as per the network operator's requirements:

S. No.	Type of NTP Server	Use of NTP server	Type of NTP support
1	Solid state NTP server	It is based on LINUX platform. This NTP server incorporates Atomic radio clock with remote antenna connects to Ethernet. It can be used with other NTP servers for enhanced time synchronization security.	SNTP and NTP
2	Standalone NTP server	It receives accurate time from GPS satellites and using NTP, it	NTP V3.

		can provide this synchronized time via Ethernet port to any computer, server or switch that conforms to NTP v3.	
3	GNSS NTP server	It connects directly to the network and obtains time from GPS and provides an accurate source of time for the network.	NTPv2, NTPv3, NTPv4 and SNTP
4	NTP Time server	It can synchronise the time across computer network .It combines a GPS receiver with in built solid state computer and offers straight forward configuration and management via a network interface.	SNTP and NTP
5	NTP Time server	It provides Stratum 1 NTP resource for accurate time across an entire network. It can be used to synchronise the time on to all elements to the correct time.	NTP v4.

4.0 INTERCONNECTIVITY AND INTEROPERABILITY REQUIREMENTS

4.1 Interconnectivity of NTP server shall be as per the Stratum level used in the network.

4.2 Stratum levels define the accuracy from the reference clock. A reference clock is a stratum -0 device that is accurate and has no delay. Stratum -0 servers cannot be used in the network but they are directly connected to computers which then operate as stratum-1 servers.

4.3 A NTP server that is connected to the stratum-0 device is called stratum-1

server. Thus stratum -1 server is directly linked (not over network path) to a reliable source of Coordinated Universal Time (UTC) such as GPS etc. transmissions.

4.4 Stratum-1 NTP servers shall have internal offset/accuracy to UTC as < 10 micro seconds when connected through a PRC / GNSS source. However this shall vary to <100 micro seconds when network is taken in to account.

4.5 Stratum-2 NTP server shall have 0.5 to 100 ms accuracy to UTC time. Subsequent stratum-3 servers shall add 0.5 to 100ms inaccuracy additionally.

4.6 NTP Server shall be capable to be used as the Stratum 1 or stratum 2 server in the network.

4.7 Use of NTP servers in Peer configuration:

4.7.1 The interconnectivity and interoperability of NTP server in Stratum 2 can be as given in Fig. 3. The input in NTP server is from Stratum-1.

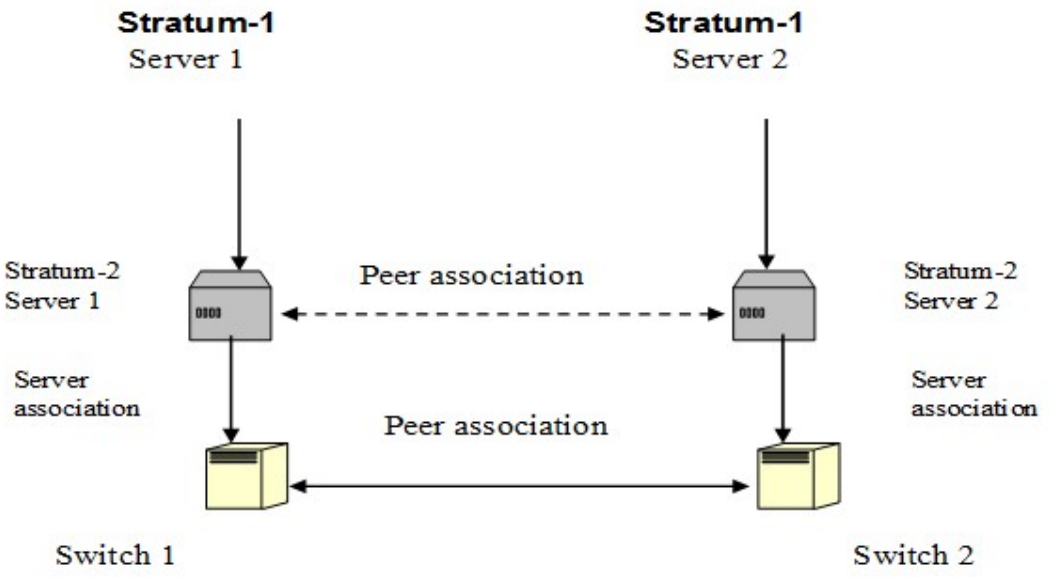

Figure-4

4.7.2 In the above figure 4 the use of NTP servers in the Peer and server association is shown. The peer and server association may be created between two networking devices.

4.7.3 A peer can provide time on its own or connected to an NTP server. It can

be used for local device and remote peer point to different NTP servers. The local device maintains the right time even if its NTP server fails by using the time from peer. The Figure-4 shows the network with two NTP stratum 2 servers and two switches. Switch 1 and switch 2 are NTP peers. Switch 1 uses stratum 2 server1, while switch 2 uses stratum 2 server 2.

4.7.4 NTP servers can be configured to provide redundancy in case an NTP server fails. For configuration to an NTP server, there shall be at least one running NTP server available. The peer association shall be used only when the clock is reliable i.e. the network is connected to a reliable NTP server.

4.7.5 If there is a peer configured alone server then it shall be used as backup. If there are two servers, the several devices can be configured to point to one server and the remaining devices point to other server. The peer association can be configured between these two servers to create a more reliable NTP configuration. If there is only one server then all devices can be configured as clients to that server.

4.7.6 The number of entities to be configured in servers and peers shall be operator specific.

5.0 QUALITY REQUIREMENTS

5.1 QUALITY REQUIREMENT: The NTP server shall comply all the quality requirements as required for IP based systems as per TEC Standard SD QM 333.

5.2 **Operational Requirement (OR):** The NTP server shall meet the following maintenance & operational requirements:

i. The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.

ii. The removal or addition of any interface cards shall not disrupt traffic on other cards.

iii. All critical modules shall be identified and shall be provided in full redundant configuration.

iv. The equipment shall have a redundant processor configuration working

in active and hot standby mode

v. Suitable Visual indication shall be provided for displaying healthy, unhealthy operation conditions.

vi. A single point failure on the equipment shall not result in network or network management system downtime.

vii. In the event of a bug found in the software, the manufacturer shall provide patches and firmware replacement if involved, free of cost. Compatibility of the existing hardware shall be maintained with future software/firmware.

viii. The normal operation of NTP Server shall not be affected while undertaking software updates, enhancement of services or correction to programs or functional blocks.

ix. A user-friendly Graphical User Interface (GUI) workstation shall be provided for interaction with NTP Server.

x. Test programs shall include fault tracing for detection and localization of system faults.

xi. Facilities shall be in-built to ensure automatic system reconfiguration on detection of any major software fault.

xii. In the event of a full system failure, a trace area shall be maintained in non-volatile memory for analysis and problem resolution.

xiii. A power down condition shall not cause loss of connection.

xiv. The hardware and software components shall not pose any problems in the normal functioning of all network elements wherever interfacing with Service Provider's network for voice, data and transmission systems, as the case may be.

xv. The equipment shall be carrier grade having an availability figure of better than 99.999% over a year. The MTBF (Mean Time Between Failure) and MTTR (Mean Time To Restore) predicted and observed values shall be furnished along with calculations by the manufacturer.

xvi. MTBF for NTP Server shall not be less than 1,00,000 Hours. The MTBF and MTTR calculations shall be provided by the OEM.

xvii. Alarms:

a. The NTP server shall allow the setting of specific levels of performance threshold for the various parameters of measurement. Any threshold crossing shall be duly reported as an alarm on a real time basis. The equipment shall be capable of detecting different alarm conditions such as:
   i. System power supply unit fail alarm
   ii. Absence of any reference signal or detection of Alarm indication signal (AIS) on the incoming reference.
   iii. Change in reference
   iv. Entry into hold over mode of operation
   v. Local clock failure alarm
   vi. the failure of an NTP signal
   vii. Detecting the hardware fault within the equipment.
b. Alarms shall be identified as “minor”, major” and critical by suitable LEDs. Provision shall exist to extend these alarms to an audio or visual alarm system.
c. It shall be possible to transmit the alarms to a remote location also.

6.0 EMI/EMC Requirements

6.1 General Electromagnetic Compatibility (EMC) Requirements

The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from an accredited test agency.

6.1.1 Conducted and radiated emission (applicable to telecom equipment):

Name of EMC Standard: “CISPR 22 (2008) /CISPR 32 - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits:-

i. To comply with Class A of CISPR 22 (2008)/CISPR 32.

ii. The values of limits shall be as per TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16.

iii. For Radiated Emission tests, limits below 1 GHz shall be as per Table 4 (a1) or 5 (a1) of TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16 for measuring distance of 3m.

6.1.2 **Immunity to Electrostatic discharge:**

Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits: -

i. Contact discharge level 2 {± 4 kV} or higher voltage;

ii. Air discharge level 3 {± 8 kV} or higher voltage;

6.1.3 **Immunity to radiated RF:**

Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"

Limits:-

For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)

i. Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and

ii. Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

For Telecom Terminal Equipment without Voice interface (s)

Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

6.1.4 **Immunity to fast transients (burst):**

Name of EMC Standard: IEC 61000- 4- 4 {2012) "Testing and

measurement techniques of electrical fast transients/burst immunity test"

Limits:-

Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines;

6.1.5 **Immunity to surges:**

Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test"

Limits:-

i. For mains power input ports: (a)2 kV peak open circuit voltage for line to ground coupling (b) 1 kV peak open circuit voltage for line to line coupling
ii. For telecom ports: (a) 2 kV peak open circuit voltage for line to ground (b)2 kV peak open circuit voltage for line to line coupling.

6.1.6 **Immunity to conducted disturbance induced by Radio frequency fields:**

Name of EMC Standard: IEC 61000-4-6 (2013) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio-frequency fields”

Limits:-

Under the test level 2 {3 V r.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

6.1.7 **Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):**

Name of EMC Standard: IEC 61000-4-11 (2004) “Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests”

Limits:-

i. a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500ms)
ii. a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms)

iii. a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

iv. a voltage interruption corresponding to a reduction of supply voltage of >95% for 10ms.

Note 1: Classification of the equipment:

Class B: Class B is a category of apparatus which satisfies the class B disturbance limits. 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 the telecommunication networks
- Personal computers and auxiliary connected equipment.

Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected.

Class A: Class A is a category of all other equipment, which satisfies the class A limits but not the class B limits.

Note 2: The test agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted.

Note 3: For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16 and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (g) and TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16. The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 11	EN 55011
CISPR 22	EN 55022
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11

7.0 Safety Requirements

7.1 The equipment shall conform to IS 13252 part 1: 2010 "Information Technology Equipment – Safety- Part 1: General Requirements" [equivalent to IEC 60950-1 {2005} Information Technology Equipment – Safety- Part 1: General Requirements"] and IS 10437 {1986} "Safety requirements for radio transmitting equipment" [equivalent to IEC publication 60215].

7.2 The manufacturer/supplier shall submit test reports in respect of compliance to this requirement from an ISO 17025 accredited agency.

8.0 SECURITY REQUIREMENTS

8.1 Suitable safe guards shall be provided in the man-machine communication programs to debar unauthorized persons from making any changes in the data contents stored in memory.

8.2 The man-machine language shall have facility for restricting the use of certain commands or procedures to certain staff/terminals.

8.3 Authentication in NTP Server

8.3.1 NTP server is vulnerable to security threats, whether from a malicious hacker who wants to alter the timestamp to commit fraud or a DDoS attack (Distributed Denial of Service - normally caused by malicious malware that

floods a server with traffic) that blocks server access. NTP is equipped with its own security measures in the form of authentication.

8.3.2 Authentication verifies that each timestamp has come from the intended time reference by analysing a set of agreed encryption keys that are sent along with the time information. NTP, using Message Digest encryption (MD5) to un-encrypt the key, analyses it and confirms whether it has come from the trusted time source by verifying it against a set of trusted keys. Trusted authentication keys shall be listed in the NTP server configuration file

8.3.3 Authentication is highly important in protecting a NTP server from malicious attack. NTP version operating in Windows 2000 or latest, recommends that a hardware source is used as a timing reference as Internet sources can't be authenticated.

8.3.4 NTP is vital in keeping networks synchronised but equally important is keeping systems secure. Whilst network administrators spend thousands in anti-viral/malware software many fail to spot the vulnerability in their time servers.

8.3.5 Authentication for NTP has been developed to prevent malicious tampering with system synchronisation just as firewalls have been developed to protect networks from attack but as with any system of security it only works if it is utilized.

8.3.6 To avoid security risks from malicious users, the NTP server shall use MD5 encryption (Message Digest Encryption 5) techniques.

8.4 Requirement Specific to leap year Problem

The system hardware/software shall not pose any problem due to change in date and time by events such as changeover of leap year etc, in normal functioning of the system.

9.0 OTHER MANDATORY REQUIREMENTS

9.1 NTP Server shall support IP addressing as per IP v4 as well as IPv6.

9.2 Power Supply

Option 1:

The equipment shall be capable of working with –40 V to –57 V. D .C. input from power supply.

Switching mode Power Supply (SMPS) and VRLA battery to be used shall be as per TEC Generic Requirements No. GR/SMP –01 and GR/BAT-01 Respectively. Power supply and battery shall be modular and expendable to support the ultimate equipment configuration.

Option 2:

AC Mains supply of 220 Volts with a tolerance of -15% to + 10% would be available. The frequency may be 50 Hz + 2 Hz. UPS and other power requirements are to be specified by the system developer. Relevant TEC Specification/ Generic Requirements as applicable may be referred

Purchase may specify the power requirement as per option1 or 2.

10.0 DESIRABLE REQIUREMENTS (Operator Specific Requirements)

10.1 This chapter describes the desirable requirements for NTP Server.

10.2 For procurement purposes, Purchaser shall specify the requirements in respect of different clauses including, but not limited to the following:

1. Dimensioning parameters e.g. handling capacity shall be indicated.
2. Physical interfaces required.
3. The software related licenses for the support interfaces shall be ensured.
4. Qualitative Requirements (QR): The purchase shall specify quality standards like ISO 9001: 2008 certification.
   The quality plan describing the quality assurance system followed by the manufacturer shall conform to the guidelines given by QA unit of Service Provider from time to time.
5. Environment Conditions: The purchaser shall specify the requirements of Environment Conditions that the system will satisfy as specified in Quality Measure Manual for relevant category of equipment.
6. Power Supply requirement option to be specified as per clause 9.2.
7. The equipment MTBF and MTTR predicted and observed shall be

furnished by the manufacturer based on the guidelines issued by QA wing of the operator.

8. The exact requirement for number of interfaces shall be indicated at the time of procurement by tendering authority.
9. Number of copies (hard and soft) of following documents required shall be specified by the purchaser.

i. System description documents
ii. System operation and maintenance documents
iii. Training documents
iv. Installation Documents
v. Repair related documents

Further details of documentation required have to be specified by the purchaser.

Abbreviation

3GPP	3rd Generation Partnership Project
CDMA	Code Division Multiple Access
CISPR	Comité international spécial des perturbations radio-électriques (Special International Committee on Radio Interference)
EMC	Electro Magnetic Compatibility
eMS	Element Management System
GR	Generic Requirements
GSM	Global System For Mobile Communication
NTPS	NTP Server
QA	Quality Assurance
RF	Radio Frequency
RFC	Request for comment
RTP	Real-time Transport Protocol
SNTP	Simple NTP
UTC	Coordinated Universal Time

End of document