Time Synchronization in IP Networks

J.M.Suri, DDG(I), TEC
B.K.Nath, Dir(I), TEC

Telecommunication Engineering Centre
Khurshid Lal Bhawan
Janpath, New Delhi -1

Contents

Time Synchronization in IP Networks

1.0 Introduction

By design IP networks are very robust and not supposed to fail. But the original design was not meant to make a carrier class IP network like TDM/SDH networks. Because of this approach the time and timing information travelling in an IP network was not considered to be a critical requirement. In IP networks traffic can move from source to destination via multiple routes. If there a route failure, the network is not affected and traffic can still reach the destination via alternate routes. However, in this process, the traffic packets travel across multiple paths travelling through different routers, switches, hubs, gateways etc. The problem is that the time information kept by the different intermediaries are not in sync. This causes the problem of inaccurate server and log files on different systems leading to several other problems.

2.0 Problems due to inaccurate time

2.1 Network Forensics

Due to the limited number of public IPv4 addresses, all telecom operators and ISPs are allocating dynamic private IP addresses to their customers through Network Address Translation (NAT). Using NAT it is possible to use one single public IP address for many connections. Through this method, one single IP address can be shared by many subscribers at different points of time. Therefore, to identify subscribers using one IP address at different point of time, it is important to keep accurate log of the subscribers using that IP address.

The logs of the subscribers are generally maintained by the service providers using the time set on their servers. However, this time is not consistent across different systems. So at any given point of time and despite date and time stamps, service providers are unable to pinpoint the exact subscriber(s) / user(s) due to variation in time across different systems on a network. Non-uniformity of time across different systems is a big hurdle for the LEA (Law Enforcement Agencies) in their investigations because they need to accurately correlate subscribers with the IP addresses at any given time. In case we are in position to synchronize the time across all systems in one network and same time can be implemented in all the IP networks of various operators with an accuracy within few milli seconds then localizing the subscriber details shall be very easy and fairly accurate.

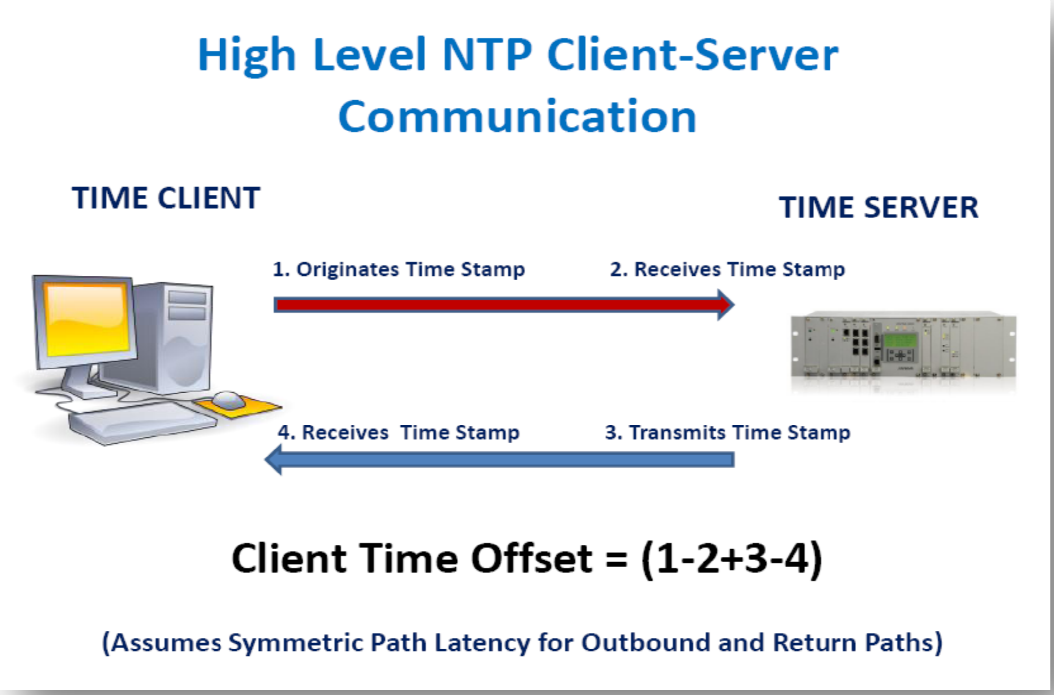
2.2 Reliability of Time dependent services like VoIP

The inaccuracy of time also affects services critically dependent upon time for sequencing and lag, like VoIP. Here accurate server and router log files are essential to IP telephony reliability. Every log file entry is time-stamped to establish the time of events and facilitate the sequencing of events. Log file data and subsequent reports allow administrators to identify the root causes of problems in the network. Because server logs are a compilation of information from different hosts, it is essential that the time stamps be accurate within milliseconds. If they are not, sequencing events becomes problematic, troubleshooting root-cause problems becomes much more difficult, and keeping the VoIP network operational becomes nearly impossible.

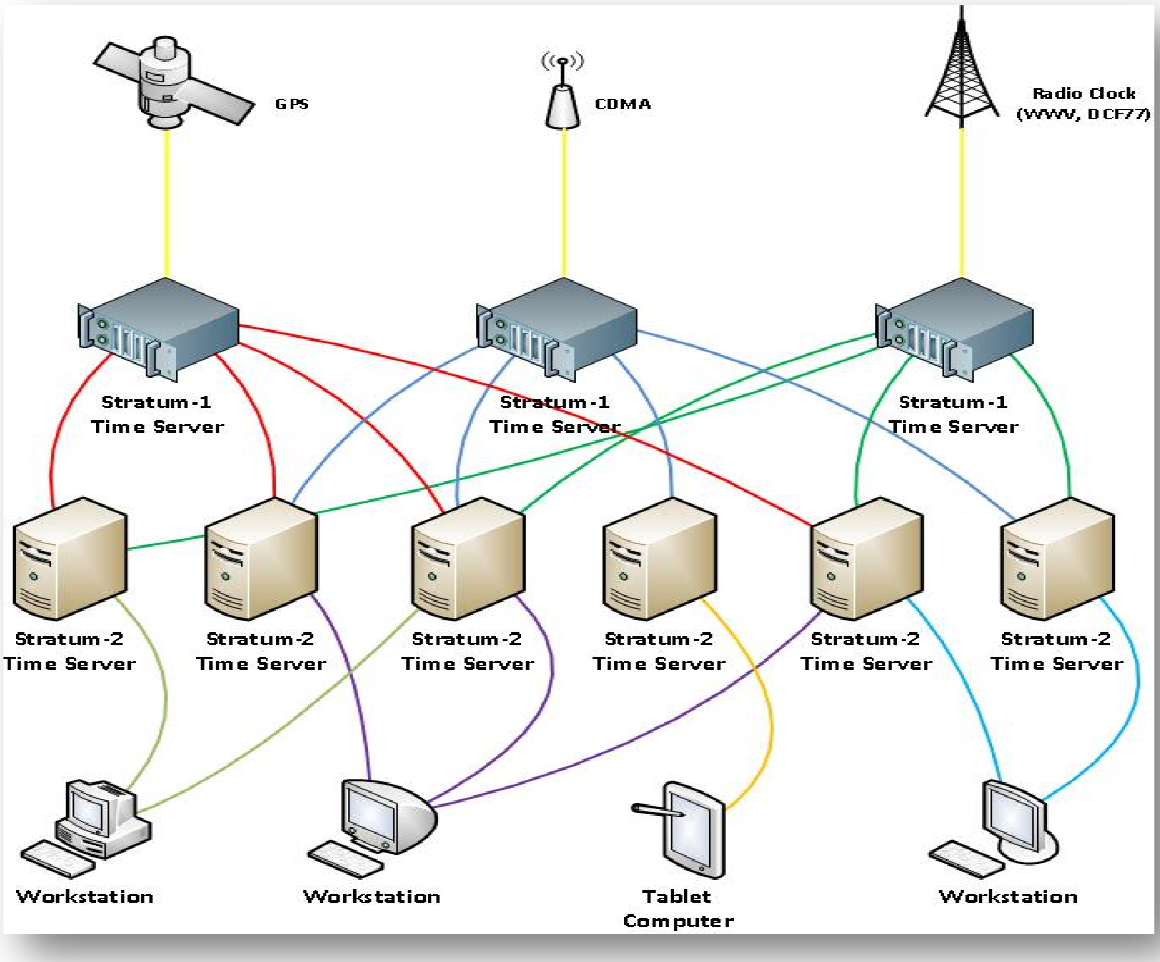
3.0 Various Methods for Network Time Synchronization

The goal of network time synchronization is to help ensure that all embedded system clocks in servers and networking equipment use accurate time. Time on these devices is kept by counting the cycles of the local oscillator in the equipment. Varying in quality, local oscillators usually run fast or slow (determined by measuring their drift from a reference point over time). During synchronization, the time on these clocks is adjusted back to the correct time. There are two widely used primary methods: Network Time Protocol (NTP) and Windows Time Service (W32Time). Another method, which is more rigorous, is the Precision Time Protocol (PTP).

3.1 Network Time Protocol (NTP) - NTP (RFC 1305) synchronizes servers and network devices using a reliable time source, such as a dedicated network time server that references the global positioning system (GPS). It uses the UDP (User datagram Protocol). As shown in Figure below, with NTP a client-initiated packet is time-stamped by the client and the time server; the result is that the client removes its time offset relative to the network time server. Many operating systems and network devices already incorporate support for NTP.



One of the strengths of NTP is that it uses Coordinated Universal Time (UTC), which can be easily accessed through the GPS satellite system. Because UTC is the same worldwide, networks synchronized to UTC avoid interoperability problems with other networks. This synchronization is particularly important when administrators are troubleshooting their network and need to compare log files from various networks. Reliability and accuracy are the primary advantages of the NTP approach to time distribution. NTP uses a stratum hierarchy (figure below). With the time source defined as stratum 0 and the network time servers as stratum 1, servers and clients operate in strata 2, 3, and so on and link their clocks to the primary time source. Because accuracy declines a little in each successive stratum, servers and clients can access multiple sources over diverse network paths, providing redundancy and greater reliability. Complex algorithms allow each server and client to achieve greater accuracy by reducing jitter, rejecting information that varies too widely from that of other sources, and accounting for the drift rate of its own clock oscillator.



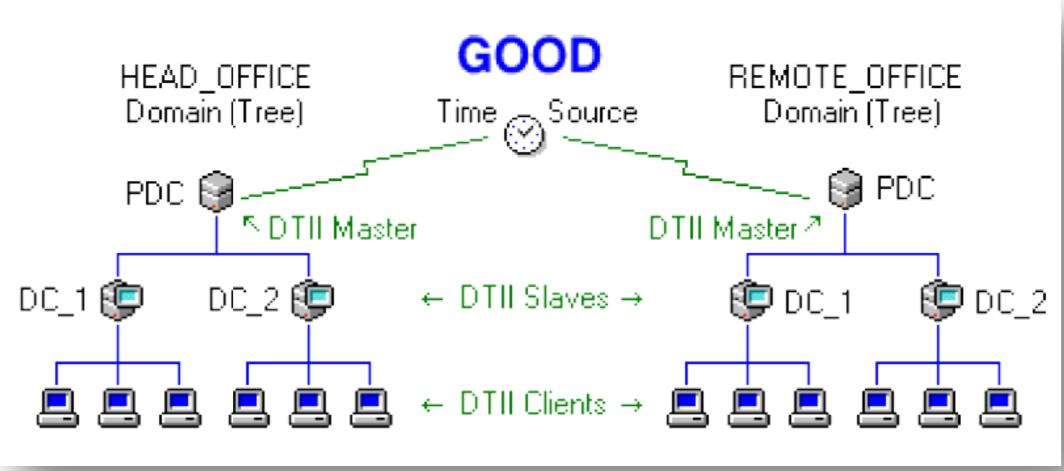
There are two types of NTP relationships between two hosts:

(i) **Client-server Relationship** - In a client-server relationship, the client periodically polls a configured server to determine its concept of the correct time. If multiple servers at the same stratum are available, the client synchronizes with the one that exhibits the least jitter. Servers do not maintain state for clients. An NTP server that receives time from a non-NTP source is normally called a stratum 1 node. Any node that receives time from a stratum 1 node is then called a stratum 2 node, etc. An unsynchronized node will typically report itself as either stratum 0 (protocol messages) or stratum 16 (user display).

(ii) **Peer Relationship**– A peer can provide time on its own or connect to an NTP server. If both the local device and the remote peer point to different NTP servers, the NTP service is more reliable. The local device maintains the right time even if its NTP server fails by using the time from the peer.

3.2 **W32Time -** The second option for network time synchronization is W32Time, supplied with Microsoft Windows and based on the Simple Network Time Protocol (SNTP). The purpose of the W32Time protocol is to make sure that all computers in an organization running Windows 2000 or later use a common time. Time synchronization is important in a Windows 2000 environment because Windows 2000 implements the Kerberos Version 5 authentication protocol, a standards-based authentication protocol defined by RFC 1510.

W32Time works by periodically checking local time on a server or client with the current time on the time source, usually the authenticating domain controller. This process starts as soon as the service turns on during system startup. This protocol attempts synchronization every 45 minutes until the clocks have successfully synchronized three times. When the clocks are correctly synchronized, W32Time then synchronizes at 8-hour intervals, unless a time stamp cannot be obtained or a validation failure occurs. If a failure occurs, the process begins again. By default, Windows-based computers use the following hierarchy -



(W32Time Cascading Hierarchy)

(i) All client desktop computers nominate the authenticating domain controller as their inbound time partner.

(ii) All member servers follow the same process as client desktop computers.

(iii) Domain controllers can nominate the primary domain controller (PDC) operations master as their inbound time partner, or they can use a parent domain controller based on stratum number.

(iv) All PDC operations masters follow the hierarchy of domains when selecting their inbound time partner.

Running W32Time helps ensure that all computers within the enterprise reliably converge to a loosely synchronized common time. Although this loose synchronization satisfies the requirements specified by the Kerberos authentication protocol, W32Time is not designed for use by applications that require greater precision.

3.3 Precision Time Protocol (PTP) - The **Precision Time Protocol** (**PTP**) is a protocol used to synchronize clocks throughout a computer network. On a local area network it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. PTP was originally defined in the **IEEE 1588-2002** standard, officially entitled *"Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems"*. In 2008 a revised standard, **IEEE 1588-2008** was released. This new version, also known as PTP Version 2, improves accuracy, precision and robustness but is not backwards compatible with the original 2002 version. "IEEE 1588 is designed to fill a niche not well served by either of the two dominant protocols, NTP and GPS. IEEE 1588 is designed for local systems requiring accuracies beyond those attainable using NTP. It is also designed for applications that cannot bear the cost of a GPS receiver at each node, or for which GPS signals are inaccessible." Therefore, PTP can be used only in small networks where delay is negligible, like in an office LAN. For larger networks like the WAN, PTP is unsuitable.

4.0 Selection of a suitable method for Countrywide Network Time Synchronization

4.1 Issues with the Implementation of NTP

(i) The NTP protocol is the preferred protocol on the WAN because it can work over larger distances. The implementation is simple and cost effective. Accuracy is also reasonable. Packet delays are reasonably taken care of to give time accuracy within a few milliseconds. However, there are serious issues with NTP server security. NTP uses the UDP protocol on port number 123. However, when such ports are open, these are prone to hacker attacks. In the NTP protocol the NTP server is queried by a client once every 64 second to give the time. Now, if a hacker wants to disturb the network, he can direct DOS (Denial of Service) attacks on the NTP server port 123. Due to these excessive queries from the hacker computer, the actual computers who

query the NTP server for time will not get any reply and slowly their time will drift away. Therefore, while implementing NTP, the solution should, as far as possible, isolate the NTP server from the internet.

(ii) In the NTP protocol, the desired time accuracy has not been defined. Now, if NTP is implemented in a large network, time accuracy will suffer because of packet delays in the network. There may be significant difference between the stratum-0 source time and the time of devices down the line. Therefore, the accuracy window should be defined (perhaps by regulation) and based on that it should be decided as to how many NTP servers will be required and at what locations in the network.

(iii) NTP is generally used for "Application Level Synchronization". The synchronization is coarse and there is no synchronization guarantee.

(iv) The most troublesome problems have involved NTP server addresses hardcoded in the firmware of consumer networking devices. As major manufacturers produce hundreds of thousands of devices and since most customers never upgrade the firmware, any problems will persist for as long as the devices are in service. One particularly common software error is to generate query packets at short (less than five second) intervals until a response is received. When such an implementation finds itself behind a packet filter that refuses to pass the incoming response, this results in a never-ending stream of requests to the NTP server, which make up more than 50% of the traffic of public NTP servers.

4.2 Issues with PTP implementation

(i) PTP implementation gives very accurate time but such accuracy comes at a high cost. High accuracy is not required in all cases. Therefore, PTP is implemented selectively in areas like operating GSM base stations, UMTS Node Bs, WiMax-FDD base stations, etc., where accurate time and frequency are critical for proper operation of the equipment.

(ii) PTP is relevant only for mission critical applications, which use dedicated hardware to minimize on-path issues. There are high end algorithms to eliminate network and equipment jitter.

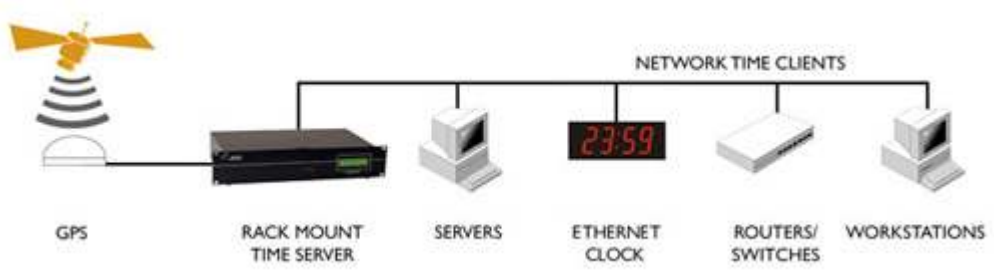
(iii) PTP cannot be implemented in large networks because network delays are significant and time accuracy cannot be maintained as per recommendations.

In view of the advantages and disadvantages of both NTP and PTP, one implementation will not work. Since the size of an IP network spreading across the length and breadth of

the country is large, a mix of different solutions is needed. In a large network, end to end distances are large and many routers and switches will come in the path each adding up some delay for the packet. Therefore, the solution should be based on multiple NTP servers across the country. In this way, the delay will be kept within the limits and the NTP protocol will give fairly accurate time across the network.

5.0 NTP Implementation Structure

Any network can be synchronized locally by using a NTP time server connected to the GPS and/or National atomic clock. A typical implementation in a small network is shown below –



The above shown network can be extended to include more NTP servers syncing with each other for time synchronization in larger networks. The following three structures are available for NTP architecture –

(i) **Flat peer structure** - In a flat peer structure, all the routers peer with each other, with a few geographically separate routers configured to point to external systems. The convergence of time becomes longer with each new member of the NTP mesh.

(ii) **Hierarchical structure** – In a hierarchical structure, the routing hierarchy is copied for the NTP hierarchy. Core routers have a client/server relationship with external time sources, the internal time servers have a client/server relationship with the core routers, the internal customer (non time servers) routers have a client/server relationship with the internal time servers, and so on down the tree. These relationships are called hierarchy scales. A hierarchical structure is the preferred technique because it provides consistency, stability, and scalability.

(iii) **Star structure** - In a star structure, all the routers have a client/server relationship with a few time servers in the core. The dedicated time servers are the center of the star and are usually UNIX systems synchronized with external time sources, or their own GPS receiver.

A hierarchical NTP design is the most preferred design and widely used in different NTP architectures. Hierarchical designs are preferred because they are highly stable, scalable, and provide most consistency. A good way to design a hierarchical NTP network is -

(i) By following the same structure as the routing architecture in place.
(ii) Use a common, single time zone across the entire infrastructure to facilitate the analysis and correlation of events.
(iii) Control which clients and peers can talk to an NTP server, and enable NTP authentication for them only.

For a country like India, the hierarchical structure will be most suitable. The hierarchy can consist of the following stratums -

(i) **Stratum-0** – These will be the independent external master clock, generally the GPS or national atomic clocks, e.g. atomic clock in TEC or NPL or any other national source. Presently in India, the official time signals are generated by the Time and Frequency Standards Laboratory at the National Physical Laboratory in New Delhi, for both Commercial and Official use. The signals are based on atomic clocks and are synchronized with the worldwide system of clocks that support the Coordinated Universal Time (UTC). But, only a few organizations are making use of these signals for time synchronization of their networks and Time stamping of data passing through the network.

(ii) **Stratum-1** - For a large country like India, it would be better if the stratum-1 servers are distributed across the 4 metros- Delhi, Mumbai, Kolkata and Chennai. These Stratum-1 servers will derive their primary clock source from GPS and simultaneously, as a backup from the atomic clocks of National Physical Labaratory. These stratum-1 servers can also have their own in-built atomic clocks. The advantage of in-built atomic clocks is that when the GPS signal fails, these in-built atomic clocks would maintain the accurate time for a considerable period with very miniscule drift, thereby not affecting the time in the dependent networks. These stratum-1 servers will communicate amongst themselves as peers to keep their times in sync.

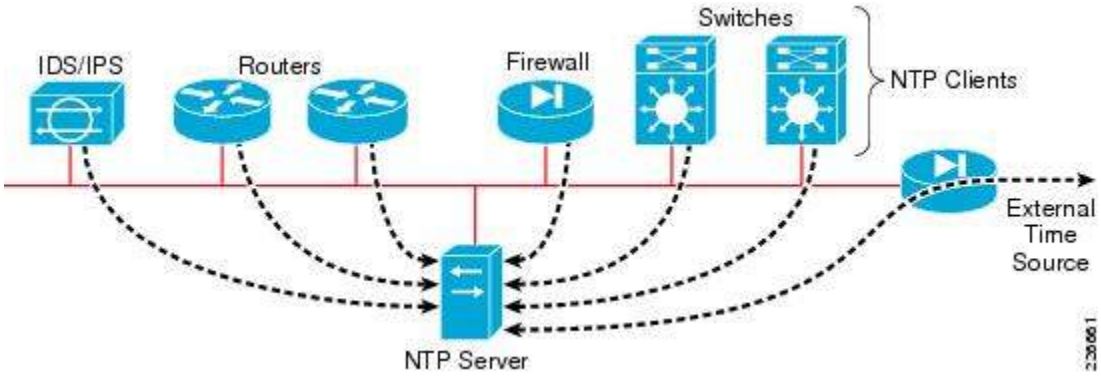
(iii) **Stratum-2** – These servers can be installed by the service providers within their core networks and they can obtain the time signals simultaneously from GPS as well as Stratum-1 servers.

(iv) **Stratum-3** – These servers will be installed by the service providers inside their networks for distribution to various sub-networks/clients. These will obtain the timing signals from the stratum-2 servers.

Since the accuracy of the PTP protocol is better, it can be run amongst the stratum-1 servers for maintaining high accuracy in time. Stratum-2 onwards, the NTP protocol can be implemented.

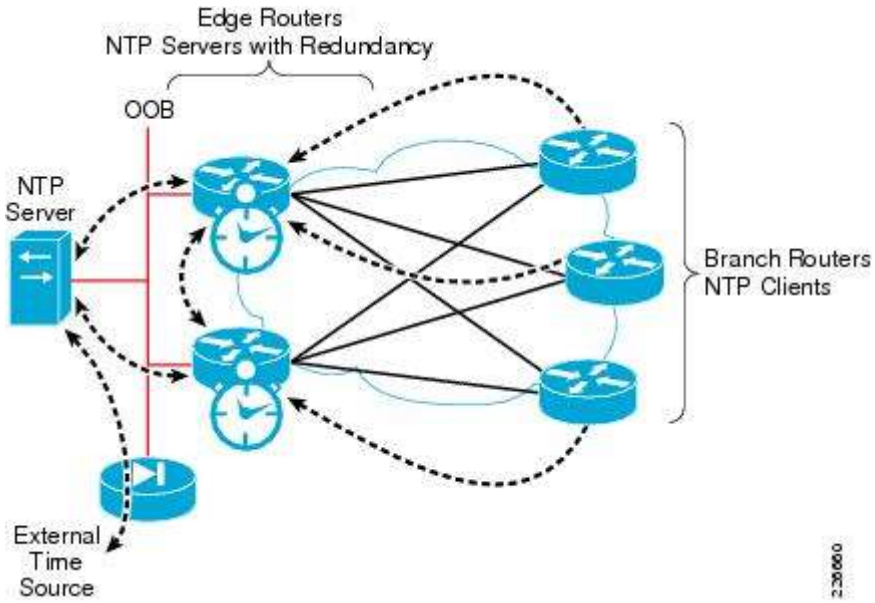
NTP Design at the headquarters / ISP end (Stratum-2)

At the headquarters or main office, an existing OOB (Out of Band) management network can be used. Transporting NTP over the OOB network flattens and simplifies the design. In this scenario, all routers and switches may be configured as clients (non-time servers) with a client/server relationship with the internal time servers located at a secured segment. These internal time servers are synchronized with external time sources/stratum-1 servers. This design is illustrated below -



NTP Design for Remote Offices / subnets at ISP end (Stratum-3)

Branch offices or the sub-networks within the ISP network are typically aggregated at one or more WAN edge routers that can be leveraged in the NTP design. At the headquarters, there is likely an internal time servers at a secured segment. Unless there is an in-house atomic or GPS-based clock, these internal time servers will be synchronized with external time sources/stratum-2 servers. Following the routing design, the WAN edge routers may be configured as time servers with a client/server relationship with the internal time servers, and the branch routers may be configured as clients (non-time servers) with a client/server relationship with the WAN edge routers. This design is depicted below-



6.0 Who should build the infrastructure ?

There are 2 possible ways to implement this infrastructure. Which approach is suitable for a country like India needs to be debated further in a larger forum consisting of industry representatives.

(iv) The government (through TEC) can install the Stratum-1 infrastructure and mandate all the service providers to compulsorily obtain the timing signals from these servers. Here the infrastructure will be owned and maintained by the Government.

(v) It is also possible to ask the service providers to install the complete timing infrastructure on their own. They can have their own stratum-1 servers obtaining the master clock either from NPL or from the TEC Timing infrastructure and sync their networks. Government, by way of regulation, will only declare the required timing accuracy to be maintained in the network hierarchy. Here the infrastructure will be owned and maintained by the service providers.

Different countries follow different models depending upon the network size, number of operators and other possibilities. E.g. in USA, the NIST (National Institute of Standards and Technology) has built the complete Timing infrastructure across different states in the USA and all service providers necessarily have to sync their timings with their time servers.

7.0 Conclusion

Time synchronization among the disparate networks is the need of the hour. Solutions are available in the market but require regulatory enforcement to ask all service providers to strictly implement the Time synchronization solutions in their networks. The basic timing infrastructure up to stratum -1 time servers can be built by the Government and ask all the service providers and ISPs to set up their own infrastructure for stratum-2 time servers onwards, which will derive their time signals from the Stratum-1 servers. This way a coordinated nationwide implementation can be ensured for IP network time synchronization.

8.0 References

[1] *A user's guide to the NPL Internet Time Service*, 2007, NPL, UK

[2] *NTP and PTP: A Brief Comparison*, Symmetricom, 2010

[3] *Cisco IP Telephony Clock Synchronization: Best Practices*, http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps556/prod_white_paper0900aecd8037fdb5.html

[4] http://www.nist.gov

[5] http://en.wikipedia.org/wiki/Network_Time_Protocol, Wikipedia resources on NTP

[6] *1588 V2 – A New Paragon for Packet Synchronization*, White paper by Tech Mahindra, 2011

[7] *Network Time Protocol: Best Practices, Cisco Systems*, http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml