Synchronization for Next Generations Networks

Framework For Synchronization and Timing in the NGN: Deploy Carrier Class NTP to Improve ARPU & Revenue Assurance

Introduction

This paper is one of a series of White Papers and Application Guidelines produced by Symmetricom as part of an overall Framework for Synchronization and Timing in the Next Generation Network (NGN). A list of relevant documentation can be found in Appendix I and at http://ngn.symmetricom.com/resource_center/application_notes.asp.

These papers are intended to help service provider network architects, planners, and engineers, design, and deploy stable, robust Synchronization and Timing architectures to support Next Generation applications and services to be deployed on these networks.

This document specifically addresses the implementation of Network Time Protocol (NTP) services to support Billing and Logging at optimal cost using Symmetricom carrier class NTP blades and servers.

NTP Overview

NTP is a well known, well proven IP technology that currently provides time services with accuracy anywhere from a millisecond to a few seconds. It has traditionally been deployed in the IT data center where it is used to provide timestamps to computers, network elements, PC's, and servers. Accuracy of one second has normally been considered adequate for these applications.

However, these requirements are changing as service provider networks quickly evolve from "best effort" delivery to a model in which mission-critical services that require very accurate and reliable performance guarantees are being deployed and where such guarantees need to be precisely quantified in order to meet strict Service Level Agreements (SLA). Accurate SLA are dependent on precise and consistent time metrics and therefore on accurate and reliable NTP. Moreover, the need for accurate timestamping is especially true for premium services that rely on revenue impacting back office server applications such as those running on billing and logging platforms. Such critical implementations, operating in real-time, typically have stricter requirements than those imposed in the best-effort data service infrastructures.

The synchronization of a network with reliable, accurate timestamps can be a competitive advantage if it enables the control of revenue leakage, the generation of additional revenue, and reduction of churn in a customer base. The key element for these services is the delivery, control, and management of time.

The distribution of time on a network is the domain of NTP. This document will focus specifically on the delivery of time for Billing and Logging services based on servers deployed in the IP NGN.

NTP and NGN Applications

Next Generation Networks are being designed to carry a mix of real-time and best effort data services that range from the most stringent real-time services to time insensitive applications. The common theme of these services is the need to seize and use time from a Coordinated Universal Time (UTC). Source and distribute it using NTP. NTP services are thus found on many network elements, those that serve control plane and back office systems as well as the application and transport layers. The ubiquity of NTP points at a critical difference between NTP services and frequency services or GPS: NTP timestamps are generated and managed by servers that sit at the packet layer in the network.

Table 1 lists some NGN network elements that require an NTP service.

Equipment Category	Elements/ Applications Requiring NTP	Operational/Service Requirement
Network Elements	Routers/Switches/Access Gateways	EMS, event logging, alarms, etc.
	Transmission Equipment - PON, DWDM, ROADM Platforms	EMS, event logging, alarms, etc.
	Wireless Base Stations	Base station timing, billing, location services
	VoIP Switches/Gateways	Call logging, CDR generation
	Media Servers	Call logging, CDR generation
Databases/Servers	Radius/TACACS, AAA, Kerberos, SNMP	Access, security, accounting, CDR generation
	Billing	CDR generation
	SS7	CDR generation
Measurement and Monitoring Probes/Equipment	IP Traffic Monitoring Systems	QoS measurement data
	VoIP Probes	Event logs
	IPTV Measurement Systems	CDRs
Customer Premises	Customer Prem Routers/Switches, VoIP Gateway	Measurements, policy/QoS
	IPTV Residential Gateway	Measurements, policy/QoS
	IPTV STB/DVR	Initialization, measurements, DRM

TABLE 1 Telco NTP applications in the NGN

The use of NTP as a source of time for mission critical services is important for the following reasons:

- Once time is injected into the stratum 1 server it cannot possibly be improved however good the accuracy of the server. Servers are CPU bound and the server OS also takes time to process applications thus timestamp generation is subject to variation depending on the CPU load and on OS coding efficiencies: a heavy load and/or poor code will force slower timestamp generation. Without smart correction mechanisms to measure the delay imposed by CPU churn the NTP will necessarily degrade. This is the standard mode of operation for enterprise class NTP servers.
- The value of NTP is also subject to jitter and propagation delay on the network. The latter is especially pervasive if the NTP server is centralized on a slow WAN but is valid even in the core. This means that timestamps will vary across the network, from relatively good to very poor, with increasing variation as each loaded NTP server is traversed, or as the stratum layers are crossed.
- Real time collection points for revenue generating premium services are particularly important at the edge of the network where calls are originated and terminated. This is also where there will be the most potential for misaligned timestamps. A well engineered NTP system will attempt to correct for the potential variation at the edge of the network by ensuring there is as little variation as possible in the original timestamping mechanism and in distribution of that time service across the network.

NTP Operation

Network elements, including servers, use system clocks that monitor current date/time. The system clock itself is gated by an NTP stack that runs internally, and this is usually updated by NTP distributed from an authoritative source predicated on UTC. Time is then distributed on a network through a hierarchy of NTP servers. Each server is in a "stratum" layer that indicates how far away it is from the original external source of UTC. The lower the stratum the nearer the server is to the time source. Stratum-1 servers thus have access to the external time source: a stratum-2 server gets time from a stratum-1 server, and so on. Up to 15 stratum layers are available to avoid synchronization loops.

The NTP clients in the synchronization subnet choose one of the available lower stratum servers to which they will synchronize. The norm is to synchronize to the lowest accessible stratum level. An NTP client may also act as a server for higher stratum clients (thus the Client /Server structure). In addition, NTP assumes it cannot rely on the time from a single NTP server and prefers access to at least three sources of lower stratum time to which it will apply an agreement algorithm to detect errors in the available time sources. All things being equal NTP chooses the lowest "most accurate" stratum server as the preferred source. Thus although each client will have three or more sources of lower stratum time, most of these will be providing a backup service.

To deliver time services in a robust manner, NTP makes adjustments for the non-deterministic nature of the packet network by estimating network delay between the client and the server, by estimating the clock offset used on a given client, and by estimating the maximum error between host NTP instances. These strategies allow NTP to build a strong set of hierarchical relationships that has a baseline of accuracy that acts as a further filter to allow the NTP to disapprove of a server that is advertising a time that shows a large disparity with the other servers in the tree. Inherently therefore NTP has some reliability and accuracy already built into the protocol, and these have stood the system in good stead over the evolution thus far of enterprise IP applications and of best effort IP LAN and WAN networks. For carrier class and more deterministic NTP operation however, these processes need to be revised and a more precise and accurate NTP instance needs to be engineered into the network. This paper will explain why this is needed in the context of NGN logging, charging, and billing architectures.

NTP Modes

NTP operates on a trust / distrust and elect basis with an architecture based on peered low stratum level servers that feed an hierarchy of higher stratum servers. This ensures network level redundancy for the deployed NTP instances and guarantees that NTP will have access to some level of time source. Within this model there are three modes of operation for NTP: client/server mode, broadcast mode, and active/passive mode.

Client / server mode is the most commonly used architecture for NTP deployments. A client will run a classical remote call procedure poll to a stateless server that will respond to the request with an updated NTP message. The client will then adjust its clock accordingly. With a large number of clients, servers are usually ensembled and peered at the stratum 1 or stratum 2 level to ensure protection at the network layer. In robust implementations one or more of these peers may have a stratum 0 source such as GPS or Cesium clock attached.

Broadcast mode is usually used when it is unimportant to have highly accurate time. Moreover, the broadcast server and all the associated clients must use the same subnet which effectively prevents telco applications for end stations such as Set Top Boxes and Cable Modems. This mode is probably best reserved for non critical relatively small LAN applications.

Symmetric Active/Passive mode is used to enable NTP peers to act as backup to each other. The peers are configured with at least one primary reference source, and auto-reconfigure on loss of a peer in the group. This mode is often used for groups of servers that are intended to act in redundant mode to each other and is considered as most suitable for NTP that will be subject to jitter and delay across a WAN or noisy network. However this mode may inject some problem with NTP convergence times across large NTP subsystems with many peers.

NTP Topologies

NTP distribution can be implemented in flat, star, and hierarchical topologies.

In flat architectures all NTP servers will peer to every other server. The flat architecture does not scale well as each added server will increase the overall convergence time of the NTP service. This is particularly problematic in application of NTP to mission critical or revenue generating services. However, in a fast hermetically engineered LAN this may be the best architecture for highly redundant NTP services.

Star topologies can also be cost effective in a LAN environment. Star configurations imply a large number of client servers using a restricted or highly centralized set of low stratum servers in the core. Such topologies are effective where the campus is high speed and geographically non-dispersed. In such an environment the servers can use an anycast model to provide some additional measure of availability to the NTP service.

The hierarchical topology is preferred for most Service Provider implementations, as it lends itself to good redundancy and a well distributed NTP instance without overly complex convergence mechanisms. The hierarchical configuration will use a classical pyramid structure with ensembling of three or more servers for each client and peering of servers at the same stratum level to give many redundant paths for the NTP service.

NTP Deployment Strategies

The two potential deployment strategies for NTP are the centralized architecture, where one NTP server complex consisting of one or more NTP servers is serving every NTP client on the overall network, and a weighted distributed architecture where a centralized server is complemented by one or more NTP servers distributed to the edge of the network.

Centralized model

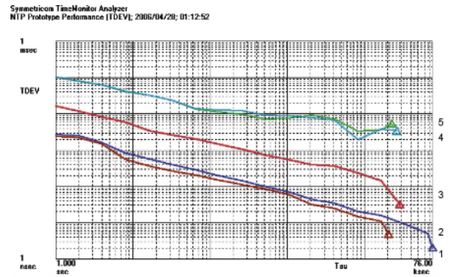
The centralized model is efficient for small scale networks that have a concentric architecture with one PRC and concentrated protection systems around that Data Centre. The NTP servers used are usually enterprise class systems but Symmetricom NTP can be deployed here in an SSU or TimeHub BITS shelf providing a more resilient and reliable high redundancy feature set. The preferred configuration in a centralized deployment would be to run NTP services on top of a complex of high performance severs with real-time OS, and with a low stratum primary reference clock. This configuration would give acceptable Telco grade performance and redundancy models.

The centralized model can suffer from availability or security issues, however. There is always potential for a Denial of Service attack on the Data Center or network Core Operations Center stopping or otherwise negatively impacting the distribution of NTP services across the network.

For security purposes mission-critical database servers (such as billing and logging servers) should be served by a secure high performance co-located NTP. This low stratum NTP should have high security and high availability to protect the uptime of the content server complexes. These NTP servers should not be accessible to clients outside the firewall.

Weighted Distributed Model

As shown in Fig 1 below, jitter in an IP based network is unpredictable and therefore NTP datagram flow behavior patterns will also be unpredictable when delivered over that IP network. This implies that NTP servers should be deployed in the nearest possible CO to reduce the allowable noise budget from the NTP server to the NTP clients. Networks that have significant potentially congested aggregation points between the centralized NTP and the edge distribution point will have to pay particular attention to the location of the NTP service.



- TDEV mask degrades successively as hops are added in the network
- Degradation is a characteristic of the network, not server
- Degradation indicative of relative location of NTP source with respect to IPTV Client - the closer the better

FIG 1 The effect of network jitter on NTP accuracy

Deployment of the NTP servers as near to the edge of the network as possible will ensure maximum availability and also maximum precision of the NTP service to the local clients. Such a deployment should be implemented with a flat NTP architecture to reduce the number of stratum layers between the primary reference source and the NTP clients.

Use of carrier class NTP deployed into SSU will ensure a tightly integrated security and management model and add carrier class reliability and availability to the NTP service. It will also have the desired effect of reducing the stratum layers and flattening the NTP service. Deployment into existing SSU or TimeHub BITS shelves can also prove highly cost effective. The deployment strategy adopted will then meet a set of engineering best-practices for mission-critical services and applications as follows:

- For efficient network operation, integrate the synchronization and timing services over a common platform to achieve better convergence of services.
- For good accuracy and stability performance, reduce the number of stratum layers and network hops between the NTP server and the NTP clients to limit network jitter and asymmetric delays.
- For a robust design and good NTP service availability, decentralize NTP servers and distribute these to the edge of the network on existing SSU shelves.
- NTP servers that are used to distribute NTP to network elements should have the same performance specifications as the centralized NTP servers.
- Variation in timestamping across the overall NTP service on the network should be reduced to the minimum.

From the perspective of the operations department, the deployment of SSU/TimeHub platform in the Central Offices achieves the integration of synchronization and timing services on a common platform and facilitates convergence of the different services.

From a network engineering perspective NTP server deployment in the remote COs minimizes network jitter impact on NTP by reducing the number of hops between the NTP server and the NTP client.

From a pure performance perspective, deployment of NTP in the CO satisfies the accuracy and stability goals of limiting network jitter and asymmetric delays inherent on the NGN IP/MPLS network.

Charging, Billing & Logging Services and NTP

Revenue Assurance

Revenue leakage has classically been considered almost just a cost of doing business on most networks, and mobile networks in particular because of the potential for fraud and revenue loss. However this model is changing. To quote the TM Forum:

> *"Revenue Assurance spans across OSS and BSS because it requires a holistic view of the operator's environment to encompass both OSS systems such as network management and BSS systems such as the billing and CRM systems. We saw a real need to create an industry standard and model for the way operators deal with RA. It was our service provider members that encourage us to take on the challenge and they have stepped up to support the technical work the Revenue Assurance team is doing."*
>
> Martin Creaner, TM Forum President & CTO

Symmetricom believes that the careful management of time services is an integral part of this holistic standards based approach. The idea that NTP is a time delivery service that has to be carefully engineered is a concept that requires a rethink on how NTP services are deployed and used and this is especially true for real time applications such as in billing and logging for services.

Standards Initiatives in Logging and Billing for Revenue Assurance

Telecoms and networking standards bodies have been attempting to harmonize management and business processes such as charging/logging architectures. ITU-T SG4 was recently mandated to discuss accounting, charging and billing of NGN and VoIP with representatives from ATIS/TMOC based on earlier inputs from 3GPP (document NGNMFG-ID-101 / SG 4 TD 135 GEN).

Key (input) specifications agreed were:

- 3GPP 32. 260 (IMS charging)
- 3GPP 32. 240 (charging architecture)
- 3GPP 32. 299 (Diameter)
- ATIS-0300075 (TMOC-AIP-2005-024R10)
- ATIS-0300075.1-2005 (TMOC-AIP-2005-046R6)

These initiatives, intended to facilitate deployment by service providers worldwide, and improve on proprietary architectures that made it difficult to engineer generic solutions. However, one component that has not yet been addressed is the delivery and management of NTP based time services in the context of control and engineering of revenue assurance and business processes.

Charging Architecture

The common high-level charging architecture across domains, subsystems and services is specified in 3GPP TS 32. 240. Figure 5.1 below provides an overview of the architecture. The arrows indicate logical information flows on the different reference points in the architecture. All the elements in this architecture will use NTP as the primary source of time for events to be logged and collated for each call. Most of the elements in this architecture are instantiated by multiple servers.

The IP Multimedia Subsystem (IMS) architecture is a highly distributed server based model. Moreover the IMS FMC charging infrastructure has a multitude of functions that are now distributed across many servers in the data center hosting the HSS /OSS/BSS functions. Billing and logging for example is decomposed into multiple functions that interface with many other servers. Thus one integrated software system on a classical MSC or PSTN switch is now embodied in many servers with much richer and more complex processes and with many potential interfaces. The IMS data center is therefore much more complex, not simpler, than the old TDM model. Importantly, most of the hardware that carried the signaling and charging gateway functions in the non-IMS world was tightly synchronized with hardware such as SS7 STP and other similar network elements, and with the logging processes, because these entities were synchronized with TDM bit aligned frequency services. In addition, the time differences between logging and billing instances that are widely distributed over a number of servers within a data center and also geographically distributed over several different data centers for redundancy purposes, can be exacerbated by the use of poorly synchronized Network Time Protocol servers, or by NTP servers that are subject to wide variation in how they deliver the timestamps to the billing complexes and other elements. The solution for such a problem lies in ensuring simple network guidelines are followed when planning and engineering NTP into the network.

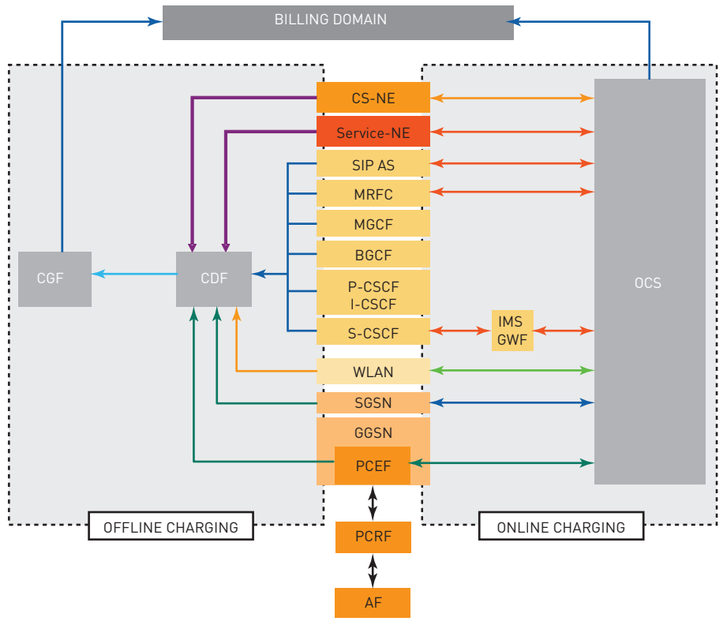


FIG 2 3GPP IMS charging architecture and information flows

Glossary: (Please see Appendix II for a complete glossary).

BGCF	Border Gateway Control Function
CGF	Charging Gateway Function
CS NE	Circuit Switched Network Element
CSCF	Call State Control Function
GGSN	GPRS Gateway Support Node
GMT	Greenwich Mean Time
I-CSCF	Interrogating CSCF
MGCF	Media Gateway Control Function
P-CSCF	Proxy CSCF
PCEF	Policy Control Enforcement Point
PCRF	Policy and Charging Control Rx Subsystem Function
S-CSCF	Serving CSCF
S-CSCF	Serving CSCF
Service NE	NE Service Network Element
SGSN	Serving GPRS Support Node
SIP AS	Session Initiation Protocol Application Server
UTC	Coordinated Universal Time
WLAN	Wireless LAN

Inherently precise and accurate timestamps out of the server that have a common and extremely stable performance independent of the load on the server CPU and of the inherent variation in processing time due to slight fluctuations in the OS stack will give an excellent baseline to the overall NTP service network wide.

Having this as a stratum 1 or stratum 2 service available at the Data Centers where the billing servers are deployed will ensure a consistent reference point for the rest of the network. As the voice gateways, the breakout gateways, the inter-working gateways and media servers all play a role in distributing voice services to the edge of the network, best practice would dictate that this precise NTP service should be available also to these network components. Having a well engineered NTP network architecture that uses high precision time-stamping technology will ensure that there is little leeway for significant differences between the service elements in the network and the billing and logging instances on the network.

This would argue for a robust and highly distributed deployment of carrier class NTP in Central Office locations next to the breakout and signaling inter-working gateways as well as next to the billing and logging server complexes. Ensuring that these NTP complexes are designed as a flat network overlay and as part of an overall synchronization architecture that is secure, and peered, would also constitute a best practice for operational purposes.

The Role of NTP in CDR/IPDR Logging

The Call Detail Record/Internet Protocol Detail Record is the basis for the billing contract with subscribers, for inter-carrier reconciliation, for taxation, and for revenue statements that describe ARPU. Any problems in reconciliation between the logging servers that are used to generate the CDR/IPDR can have an impact on perceived revenue performance, and may even be unacceptable to the host country security services, to the regulatory body establishing operational efficiency requirements, or to the carrier internal auditors. Thus Call Detail Records (CDR) / Internet Protocol Detail Records (IPDR) are at the heart of the carrier revenue assurance architecture. In a simpler TDM world the CDR would be a relatively non complex file that showed start time, stop time and duration of a call with some minimal information about network elements STP or SMSC elements for a premium service such as an SMS (Short Message Service) text over SS7. In the IP NGN however the IPDR is more complex as it includes much more than the basic information and will have many fields, such as the calling number, the receiving number, call start time, call stop time, call duration, the originating network element or exchange ID (MSC, Softswitch, PBX, PSTN 4E or 5E switch identifier), CD/IP record sequence number identifier, route to the recipient, call completion indication (busy, answered, dropped, denied, blocked etc.), call waiting and added value facility usage, call route into and out of the originating and terminating exchanges or MSC, fault conditions, SIP or SS7 gateway information, MAC layer information, and etc. In addition there will be clearly defined parameters to include for each service type defined by IPDR.Org (now part of the TM Forum).

An example is the definition given for Public WLAN access:

Generic Requirements

The Service Provider must be able to accurately report resource usage by all Service Consumers (Home or Visited). For the Service Consumer, these resources comprise the airtime (for basic PWLAN access) and the services delivered (over the PWLAN interface.)

[R1] The IPDR must contain the billable account identifier.

[R2] The IPDR must identify the PWLAN hotspot where the resource was consumed. It must contain the user device's MAC address, access gateway identifier, and the location of Access Point.

[R3] The IPDR must accurately identify the PWLAN access resources used. It must contain local time of session establishment and the local time of session termination. The minimum required timestamp accuracy should be to the second. Local time zone offset with respect to GMT must be provided. Time should be expressed in ISO 8601 format.

[R4] The IPDR must identify the services consumed over PWLAN access interface. It must contain specific usage data. Usage data comprises the number of bytes transmitted and received by the Mobile Station, types of IP services utilized, content type/bytes purchased during the session, etc.

[R5] The IPDR should contain the billing class of service when available.

[R6] The IPDR must contain the termination cause for each session.

[R7] The IPDR must contain access payment method used by the Service Consumer. If no payment was made (i.e. service was free), it should be recorded in the IPDR.

[R8] The IPDR must contain unique identifiers of all providers and partners. It must uniquely identify the Access Provider and the Service Provider. The IPDR MAY optionally contain fields for identifier that specify the partners namely Venue Owner, Content Provider.

Reproduced from" Service Specification – Public WLAN Access Version 3.5-A.0.1 November, 2004© 1999-2004 IPDR.org.Inc"

http://www.ipdr.org/public/Service_Specifications/3.X/PWLANAccess3. 5-A. 0.1.pdf

A detailed example of NGN IPDR fields is taken from the IPDR. org DOCSIS charging architecture:

IPDR xsi:type="DOCSIS-Type">

<IPDRCreationTime> 2004-11-10T07:11:05Z </IPDRCreationTime>

<CMTSHostName> cmts01. mso. com </CMTSHostName>

<CMTSipAddress> 10. 40. 57.11 </CMTSipAddress>

<CMTSsysUpTime> 2226878 </CMTSsysUpTime>

<CMTScatvIfName> Int0/1 </CMTScatvIfName>

<CMTScatvIfIndex> 456 </CMTScatvIfIndex>

<CMTSupIfName> Int/0/1/4 </CMTSupIfName>

<CMTSupIfType> 205 </CMTSupIfType>

<CMTSdownIfName> int/0/1/2 </CMTSdownIfName>

<CMmacAddress> 00-D2-89-0A-35-ED </CMmacAddress>

<CMipAddress> 55.12. 48.121 </CMipAddress>

<CMdocsisMode> 1.1 </CMdocsisMode>

<RecType> Interim </RecType>

<serviceIdentifier> 349 </serviceIdentifier>

<serviceClassName> Basic </serviceClassName>

<serviceDirection> 2 </serviceDirection>

<serviceOctetsPassed> 38336164 </serviceOctetsPassed>

<servicePktsPassed> 91713 </servicePktsPassed>

<serviceSlaDropPkts> 458 </serviceSlaDropPkts>

<serviceSlaDelayPkts> 9 </serviceSlaDelayPkts>

<serviceTimeCreated> 1247523 </serviceTimeCreated>

<serviceTimeActive> 9794 </serviceTimeActive>

Reproduced from Network Data Management – Usage (NDM-U) For IP-Based Services Service Specification – Cable Labs® DOCSIS® 2. 0 SAMIS Version 3.5-A. 0 November, 2004 © 1999-2004 IPDR, Inc

http://www. ipdr. org/public/Service_Specifications/3. X/DOCSIS(R)3 5-A. 0. pdf

These examples show that the previously simple CDR has now become a complex IPDR that contains both network and application layer references as well as references to time services. As with the NGN data center itself, the complexity of service types and the evolution of services from being embedded in the TDM physical layer (L1) to being constructed in the Application layer (L7) has forced the IPDR to become more information rich and thus more unwieldy to collect, parse, and assemble. Moreover, as we have seen, the IPDR is collected from an increased number of network instances depending on the specified service layer, and application, and for each of these there are well defined interfaces that act as collection points. These collection points all have integrated NTP services. The proliferation of collection points and the increase in both number and variety of fields collected means that there is much more scope for IPDR mismatch and reconciliation problems on NGN than on the relatively simple TDM voice only network. The very complexity of the IPDR in the NGN therefore demands that the NTP service be more finely tuned and more reliable and not less so. Best effort NTP is no longer good enough for such a rich and purposeful service and application environment.

NTP Network Engineering for Logging, & Billing Services

The NGN is a packet based network built on Ethernet Layer 2 transport technologies and Layer 3 IP packet services with a business model for service delivery based on congestion based provisioning. NTP services, like all packet services, can be negatively impacted by the congestion based service provisioning.

However, real-time services are always carefully engineered from the distribution servers to the edge distribution point and to the end consumer to avoid timeout and other service affecting events. Problems arise at congested aggregation points where content is finally delivered from the network onto the edge platforms. Careful L2/L3 traffic engineering can ensure that a given IP flow will be propagated with the correct QoS over this service infrastructure. Unless the NTP service is similarly treated, it will necessarily suffer from network induced delay.

For logging and charging instances, the recommendation is to flatten the NTP architecture and deploy a carrier class NTP server infrastructure that delivers a consistent timestamp referenced to the highest quality clock on the network – the clock delivered by the SSU. Given that the hardware generated timestamp will not be impacted by the NTP server software or by CPU churn under load, the NTP delivery can be considered predictable as it enters the network, with either no significant delta from the reference source or with a well determined (i.e. deterministic) delta that allows NTP to be finely engineered.

The target deployment for such an NTP service is the data center that hosts the NGN HSS/OSS/BSS complex servers. By deploying a carrier class highly stable, highly redundant carrier class stratum 1 NTP server next to the HSS servers we can be sure that we have pulled the servers into tight time alignment. The ideal would be that these servers are stratum 2 or at most stratum 3, with very few NTP layers between them and the Primary Reference Source. Because of the deterministic timestamping technology of the Symmetricom Carrier Class NTP server, and its consistent and predictable behavior under load, the network is always operating under an optimally configured and consistent time reference out of the server and onto the wire. If the HSS/OSS/BSS complex is configured to have minimal network congestion between the stratum 1 NTP and the billing and logging servers, there will necessarily be very little jitter and wander of the NTP timestamp. Removal of this variation will increase the accuracy of the inherent time service that the logging servers use to log CDR/IPDR relevant parameters, and that are eventually probed by the billing and charging elements to develop and propagate an accurate invoice. This presents further arguments for a flattened NTP network, with a minimum of stratum layers, and the use of peered Carrier Class NTP servers. It is not necessary however to peer the Symmetricom NTP blades in a classical mulit-server ensemble, but to simply peer the SSU that host the NTP to ensure that the peering is at the very highest layer of reliability and of clock stability and accuracy.

This cannot be accomplished by the best effort architectures. A classical NTP ensembling is not designed for high precision, but simply to create timestamp presence and access to "some" NTP service if the server loses its lower layer stratum reference and is no longer able to run on internal holdover. Thus there is a contradiction between the operation of best effort enterprise class NTP and the need for a fine-tuned time service that is not subject to the random impact of server loss, CPU overload, network induced delay, routing flaps, and different OS client servo engineering. By removing as much of the unpredictability as possible from the NTP service whenever it touches logging and billing services, the carrier can remove inconsistencies in CDR/IPDR generation in the network, and reduce the problems inherent in CDR/IPDR reconciliation and mismatch.

Finally, as the ability to engineer at a finer level of time granularity has improved, the overall time requirements on the network have tightened. These requirements are being driven by security and legal intercept needs, by overall server performance improvements, by a general desire to reduce tolerance in service provision where the usage of network resources can be translated directly into a financial statement, and by concerted efforts to control revenue leakage and improve revenue assurance.

Carrier Class NTP Return On Investment

Symmetricom customers have already deployed the Carrier Class NTP blades to serve the HSS/OSS/BSS data center infrastructures and in every case these customers have found an extremely compelling return on investment. Simple calculations serve to exemplify the nature of the problem and the result of deploying a well architected and fine tuned NTP service to reconcile IPDR.

The example shown in FIG 3 is taken from a second tier mobile carrier in the G8. This carrier was suffering from significant revenue loss that was traced to continual failure to correctly reconcile the final logging servers in the two primary data centers used for assembling and collating IPDR and CDR. The failure was eventually put down to a poor NTP installation, with enterprise class servers running at a high CPU load and continually failing over to ensembled peer servers that were also then being overloaded with the additional requests and subject to CPU churn. The impact on time services was to cause high and accumulated variation of timestamps across the network to the IPDR information collection points, and then to see this variability reflected back in the information sent to the logging servers where the event logs were assembled. Rather than maintain the best effort model with many stratum layers of NTP and a reliance on network layer redundancy typical of a well engineered campus /LAN architecture the network architects decided to flatten the NTP architecture, remove as much variation as possible from the two data centers used as primary assembling points for the IPDR information, and ensure that there was as much determinism in the NTP delivery as possible.

The result was interesting. This SP has revenues of approximately US $50b per year. The NTP problem was causing a failure to reconcile that led to revenue leakage of approximately 0.005, or US $25m per year. Working with this raw sum as primary loss the carrier could impute some US $3.5m of additional cost to inter-carrier mediation services, reconciliation processes, and customer service complaint resolution. Additional sums in operations personnel and engineering time were spent in trying to diagnose and troubleshoot the cause of the problems, and to resolve it by installing more enterprise class servers -an action and expenditure that actually did not and could not solve the problem. The overall shareholder value of the total sums spent (once operating margins and EBITDA was factored) was estimated at some $300m - a significant enough sum to attract the attention of the company auditors.

Total Revenue per year (medium carrier)	CDR Leakage due to misaligned billing and logging services	Revenue Loss per year	Carrier Class NTP ROI per redundant blade pair
$50 B	0.005	$25 M	< 1 day

FIG 3 Sample Return on Investment for Carrier Class NTP Blades

The solution was to deploy the carrier class NTP blade in redundant pairs at the primary data centers and near principle collection points on the network. The overall architecture was considerably flattened and the NTP service became more deterministic and predictable. The NTP blades populated the SSU and the SSU primary clock source was thus bought closer to the collection points and to the many different logging and assembling servers operating in the HSS/OSS/BSS centers. The overall result was a reduction in the mismatch from $25m to $2m per year – a very significant change. The investment moreover removed the number of reconciliation and mediation processes needed. Operational cost reduction was therefore also achieved. The ROI of the total NTP blade investment, according to this customer, was in the order of a few days.

Symmetricom Carrier Class NTP Servers

This section describes the operational advantages of Symmetricom's Carrier Class NTP implementation.

Carrier Class NTP Requirements

NTP server equipment that is designed to ensure carrier class availability services must meet a number of carrier class reliability requirements including:

- Dual processors
- Sub-second transparent service restoration
- Network access availability (Network interface redundancy)
- Redundant power supply
- Redundant fan trays
- Carrier-grade operating system

These attributes are integral to Symmetricom's Carrier Class NTP solution.

Converged Architecture

The introduction of a NTP blade in a Symmetricom carrier class SSU 2000 or TimeHub platform will converge synchronization and timing services and will cost effectively optimize and scale the existing synchronization and timing infrastructure.

The SSU 2000 and TimeHub shelves implement a highly scalable blade architecture, with hot-pluggable modular components, that allows service providers to cost effectively scale services without disruption as they grow and deploy new synchronization and timing services.

Deploying the carrier class NTP consists simply of plugging the new card into the platform and takes advantage of the fact that central offices are often already outfitted with a BITS or SSU shelf. The highly scalable blade architecture makes it possible to accommodate several pairs of redundant cards in a single chassis.

Power & Space Saving

The low power consumption of a blade platform system over a stand alone server is a cost benefit. The SSU/TimeHub platform provides a single power source shared by all the blades (output cards and NTP server cards) within the platform. Reduced rack-space is another major benefit of a blade platform compared to traditional rack-mounted servers.

Operational Simplicity

Other obvious benefits are simplification of installation, cable management, network engineering, and integrated network management.

The SSU/TimeHub offers an integrated and flexible management environment that allows the provisioning of all the synchronization cards available on the platform eliminating the need for more than one management system per synchronization system. This allows the operator to leverage the experience of the operations staff on managing the existing BITS services and consequently reduces the overall costs and complexity of deploying NTP services. For efficient network operations, a best practice statement is to integrate all synchronization and timing services into a common platform.

Redundancy and Reliability

A system failure as well as a network failure must be transparent. Therefore the hardware and software of the NTP server equipment must be designed to support carrier-class availability to permit timely restoration of the NTP timing service in the event of software, equipment or network failures.

In a design where NTP server equipment takes over for a failed NTP server, IP Address failover is required to ensure transparency to the clients. Clearly, this is preferred for logging and charging services because the client in the collection points and data center servers may not allow multiple IP addresses, and "Hitless" switching is transparent to the client, hence will not introduce any timing related impairments.

Two external NTP servers may require server based clients to detect a failure and manage the potential new path delay while switching to a new server. Since a server is a shared resource a large number of logging servers will experience transients and collection points will likely see these at different times if the NTP service is forced to converge on an ensembled server.

The use of an external load balances may be an alternative to "tie" two NTP servers together and present as one to the external world. However, load balancing may add a single point of failure, significant packet delays, and management complexity.

UTC Reference Failure / PRS Failure

For robust IPDR collection it is recommended that the NTP servers should be deployed as stratum 1 or stratum 2 servers. The stratum 1 NTP servers are directly connected to the stratum 0 Primary Reference Source (PRS).

In the event of loss of the PRS, it is important to be able to maintain very accurate time. Blade based servers installed in BITS/SSU shelves are protected by redundant oscillators and redundant clocks to hold very tight timing accuracy during holdover events.

The stratum 2 NTP servers may also, and in addition, take advantage of the inherent NTP model redundancy which allows them to be a client of several stratum 1 NTP servers and establish peer relationships with other NTP servers at stratum 2.

Network Interface Redundancy

Network ports and networking equipment module redundancy are important elements of timing and synchronization system availability. Network interfaces failures can be the source of outages. At each NTP server level, the NTP server equipment can be equipped with redundant network ports to increase the network interface availability. When a link fails, the NTP server can transparently transfer the NTP communications to the backup network physical port.

Network Path/Route Redundancy

Network communication path protection/restoration mechanisms are important elements of timing and synchronization system availability. The network must have the ability to switch or reroute the traffic across redundant or alternate links around the failed elements (links or nodes), especially in locations where failures affect a large population of customers. It is recommended that network planning practices for route redundancy be considered in NTP system configuration.

Meeting carrier class availability targets of 99.9999% uptime will always be onerous, therefore, it is recommended that existing synchronization and timing infrastructure deployed in telecom offices be utilized as far as possible to serve the NGN IPDR applications. This can be rapidly and simply achieved by adding NTP capability with the required accuracy and availability to the Central Office BITS/SSU equipment which, in most cases, is equipped with holdover capabilities and/or a Primary Reference Source.

Management of NTP

The provisioning of NTP servers should include the configuration of the following:

- external clocks
- relationships with other NTP servers (peers, servers)
- a drift file to store the current value of the frequency error
- the authentication scheme
- NTP restrictions (restrict NTP server access from certain source addresses)
- process initiation and termination

The NTP server management provided by Symmetricom not only provides these provisioning capabilities it is also be able to proactively identify potential problems and quickly diagnose the problems after they occur.

Conclusion

The IPDR/CDR is the heartbeat of the carrier revenue model. NGN service providers are determined to ensure more consistent logging techniques and charging architectures that take account of and exploit the rich functionality found in the IP application layer. The IPDR is designed to facilitate this charging architecture. The NGN billing and logging service is thus becoming more and more complex, with different collection architectures for different network layer services and different applications. As can be seen from this paper, these architectures themselves are in the process of being robustly defined, and while excellent standards work has been done to specify charging statements on the network, there are still some elements of revenue assurance that remain a challenge for the operator.

One of the areas of possible neglect concerns the fundamental time service delivered by NTP that is used to tag the service information collection points in the network and that is also used by the assembly and collation servers in the HSS/OSS/BSS data centers themselves. NTP has previously been considered an attribute of the network with little consideration of the implications of a poor implementation. Best effort time service has effectively been taken for granted. It may still deliver time, but it remains best effort.

With more critical view of business processes now taking hold in the OSS / BSS Management in the network, with a focus on revenue generation on the one hand and revenue loss mitigation on the other, carriers are now realizing that with a small but critical investment they can improve on their existing NTP architectures, take control of this fundamental function and engineer it to improve revenue assurance, reduce revenue leakage, and thus improve ARPU and shareholder value. This is attainable by a relatively simple cost effective deployment of Symmetricom carrier class NTP blades into existing SSU and Timehub shelves already deployed in the network.

Symmetricom is a leading supplier for NTP Servers, and carrier class Building Integrated Timing Supplies and Synchronization Supply Units (BITS and SSU). We have leveraged design experience from multiple generations of equipment to develop carrier class NTP blades to fit into our advanced generation BITS and SSU systems. The blade form factor takes full advantage of the existing synchronization infrastructure in the telecom network to provide the highest level of stability, availability, and protection of any NTP solution.

Time services are critical to the network, accuracy and precision of time services are critical to revenue generation, carrier class NTP delivers such services with minimum disruption, maximum efficiency, and most importantly, with a compelling ROI.

Appendices

Appendix I: Documentation

1) PTP deployment Guide :Synchronization for GSM and UMTS Backhaul Networks Using Packet Time Protocol (IEEE 1588v2).

2) Synchronization for Next Generation Networks: Network Timing Protocol Applications and Implementation Guidelines.

3) TimeHub 5500 BITS Platform
The TimeHub 5500 is a fully NEBS certified Building Integrated Timing Supply. The TimeHub is in wide deployment in the USA.
The Data Sheet for the TimeHub 5500 can be found at :
http://ngn. symmetricom. com/pdf/datasheets/ds-timehub-5500. pdf

4) SSU 200) and SSU 2000e
The SSU 2000 and SSU 2000e are NEBS/ ETSI certified respectively and compliant Synchronization Service Units widely deployed in the USA and internationally. .
The Data Sheet for the SSU 2000 (NEBS version) can be found at:
http://ngn. symmetricom. com/pdf/datasheets/ds-ssu-2000. pdf

The Data Sheet for the SSU 2000e (ETSI version) can be found at:
http://ngn. symmetricom. com/pdf/datasheets/ds-ssu-2000e. pdf

2) Symmetricom Carrier Class NTP Blade
The Data Sheet for the Carrier Class NTP blades for the Timehub 5500 can be found at:
http://ngn. symmetricom. com/pdf/datasheets/DS_TH_NTPcrd. pdf

The Data Sheet for the Carrier Class NTP blades for the SSU 2000 / SSU2000e can be found at: http://ngn. symmetricom. com/pdf/datasheets/DS_SSU2K_NTPcrd. pdf

Appendix II: Glossary

ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BITS	Building Integrated timing Supply
BGCF	Border Gateway Control Function
BSS	Business Support Systems
C2P	Circuit to Packet
CO	Central Office
CSCF	Call State Control Function
CSN	Circuit Switched Network
CS NE	Circuit Switched Network Element
CGF	Charging Gateway Function
CPU	Central Processing Unit
CSN	Circuit Switched Network
DIAMETER	RFC 3588security protocol - successor to RADIUS (see below)
DSL	Digital Subscriber Line
ESN	Electronic Serial Number
ETSI	European Telecommunications Standardization Institute
GGSN	GPRS Gateway Support Node
GMT	Greenwich Mean Time
GPS	Geosynchronous Positioning System
GW	Gateway
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
IS	IPDR Store
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
IT	IPDR Transmitter
ITU-T	International Telecommunications Union – Telecommunications Standardization Section
KERABOS	Security encryption key algorithm used to validate datagram transfers
MAC	MediaAccess Control
MG	Media Gateway
MGCF	Media Gateway Control Function
MSC	Mobile Switch Center
MSP	Mobile Service Provider
NDM	Network Data Management
NE	Network Element
NGN	Next Generation Network
NTP	Network Time Protocol
OSS	Operations Support System
PBX	Private Branch Exchange
P-CSCF	Proxy CSCF
PCEF	Policy Control Enforcement Point

PCRF	Policy and Charging Control Rx Subsystem Function
PLMN	Public Land Mobile Network
PSN	Packet Switched Network
PSTN	Public Switched Telephone Network
PSN	Packet Switched Network
OS	Operating System
QoS	Quality of Service
RADIUS	Remote Access Dial-In Usage Server
S-CSCF	Serving CSCF
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SIP AS	Session Initiation Protocol Application Server
SLA	Service Level Agreement
SP	Service Provider
SSU	Synchronization Service Unit
SS7	Signaling System 7
STP	Signal Transfer Point
TDM	Time Division Multiplexing
TM Forum	TeleManagement Forum
UTC	Coordinated Universal Time
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
xDSL	Digital Subscriber Line(type x)
XML	eXtensible Markup Language

References

[1] RFC-1305, *Network Time Protocol (Version 3). Specification, Implementation, and Analysis, Internet Engineering Task Force Request for Comments*, March 1992.

[2] RFC-2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, Internet Engineering Task Force Request for Comments*, Oct. 1996.

[3] ISO/IEC 13818-1, *Information Technology Generic coding of moving pictures and associated audio information Systems*

[4] *NTP Performance Analysis*, David Mills, http://www.eecis.udel.edu/~mills/database/brief/perf/perf.ppt

[5] *Cisco ISP Essentials version 2. 9*, June 2001

[6] IETF RFC 4732, Internet Denial-of-Service Considerations, M. Handley, et al., November 2006

[7] http://www.cs.wisc.edu/~plonka/netgear-sntp/

[8] ATIS IPTV IIF (Inter-working Interoperability Forum) ATIS-0800001,

[9] ATIS IPTV IIF (Inter-working Interoperability Forum)ATIS-0800002,[10] 3GPP TR 21. 905: "Vocabulary for 3GPP Specifications".

[11] 3GPP TS 23 882: "Report on Technical Options and Conclusions (Release 7)".

[12] 3GPP TS 23 401: "GPRS enhancements for LTE access".

[13] 3GPP TS 23 402: "Architecture Enhancements for non-3GPP accesses".

[14] 3GPP TS 32 240: "Charging architecture and principles".

[15] 3GPP TS 32. 251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[16] 3GPP TS 32. 252: "Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging".

[17] 3GPP TS 23. 203: "Policy and charging control architecture".

[18] 3GPP TS 23. 078: "Customized Applications for Mobile network Enhanced Logic (CAMEL); Stage 2".

[19] 3GPP TS 29. 078: "Customized Applications for Mobile network Enhanced Logic (CAMEL); CAMEL Application Part (CAP) specification".

[20] 3GPP TS 23. 234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[21] 3 GPP TS 32. 299: "Telecommunication management; Charging management; Diameter charging application".

[22] Symmetricom Carrier Class NTP Data Sheet.

[23] Symmetricom TimeHub 5500 Data Sheet.

[24] Symmetricom SSU2000 /SSU 2000e Data Sheet.

[25] Service Specification – Public WLAN Access Version 3. 5-A. 0.1 November, 2004 © 1999-2004 IPDR. org. Inc

[26] Network Data Management – Usage(NDM-U) For IP-Based Services Service Specification – Streaming Media (SM) Version 3. 5-A. 0.1 November, 2004 © 1999-2004 IPDR. org, Inc.

[27] Network Data Management – Usage (NDM-U) For IP-Based Services Service Specification – Voice over IP (VoIP) Version 3. 5-A. 0.1 November, 2004 © 1999-2004 IPDR. org, Inc.

[28] Resource Data Collection, Analysis & Control (RDC) For IP-Based Services Service Specification – IP Television (IPTV) Version 3. 5-A. 0. 0 October 31, 2006 © 1999-2006 IPDR. org, Inc.

[29] Network Data Management – Usage (NDM-U) For IP-Based Services Service Specification – Cable Labs® DOCSIS® 2. 0 SAMIS Version 3. 5-A. 0 November, 2004 © 1999-2004 IPDR. org, Inc

SYMMETRICOM, INC.
2300 Orchard Parkway
San Jose, California
95131-1017
tel: 408.433.0910
fax: 408.428.7896
info@symmetricom.com
www.symmetricom.com