MTR 05B0000013

MITRE TECHNICAL REPORT

U.S. Air Force Network Time Service

Fixed Installation Case Study

05/2005

Robert Lesch
Glenn Bell

Sponsor: GIGSG/ES **Contract No.:** FA8721-05-C-001
Dept. No.: D480 **Project No.:** 0305300FC0

MITRE
Center for Air Force C2 Systems
Bedford, Massachusetts

Approved by:

_____

Mr. Thomas Reale
Chief Engineer, GIGSG/ES

Abstract

The Fixed Installation Case Study presents an approach for deploying time synchronization services to Air Force installations in accordance with the Air Force Network Time Service Profile. The study proposes a method for implementing time services utilizing existing commercial products and is intended to provide guidance in developing an implementation plan. Time services are obtained from UTC(USNO) via the Global Positioning System (GPS) and distributed over the Local/Metropolitan Area Network using the Network Time Protocol (NTP). Furthermore, high precision clocks are utilized to provide stability and availability.

The case study is intended as guidance for developing a detailed implementation plan. This document should not be construed as the only, or even the best, solution for the dissemination of enterprise time services.

KEYWORDS: CII Time Synchronization CITS UTC

Table of Contents

List of Figures

List of Tables

1 Introduction

The Fixed Installation Case Study was developed by GIGSG/ES in support of the Air Force Network Time Service (NTS) Architecture and the Combat Information Transport System (CITS) Program Office. This study was produced at the direction of the GIGSG/ES Chief Engineer.

The study depicts a proposed method for distributing synchronized time services within a fixed installation facility in accordance with the Air Force Network Time Service Profile.

The NTS Profile provides the enterprise architecture for the Air Force Time Service. It defines the interfaces between the enterprise service and consumer organizations. It further defines the following key performance parameters which ensure service consistency and coherency across the enterprise.

Accuracy - All systems shall maintain time within an acceptable deviation from Coordinated Universal Time as provided by the U.S. Naval Observatory UTC(USNO).

The NTS Enterprise will provide time accuracy to ±100 ms of UTC(USNO).

Traceability – All systems shall trace their time synchronization to UTC(USNO).

Availability – All systems shall utilize DoD provided delivery mechanisms to synchronize time.

This case study extends the NTS Profile by illustrating how a specific consumer – in this case the Network Control Center at a fixed installation – could provide the time service to their user community.

1.1 Scope

- This case study depicts just one of many possible ways to implement NTS within a fixed installation. It is not the intent of this paper to describe all of the possible options available to a fixed installation in implementing NTS.
- The case study focuses on leveraging existing equipment to reduce implementation costs.
- The case study does not attempt to show how time might be used once it is distributed within the fixed installation.
- The case study does not attempt to address other types of time consumers e.g., airborne platforms.
- The case study is not intended as an NTP tutorial. It does attempt to provide enough information about NTP to put the implementation decision in their proper context.

- The case study does not specify the interactions between the fixed installation and NTS. Refer to the Network Time Service Profile for a complete description of the service and its interactions with consumers.

2 Network Time Service Architecture

The Air Force Network Time Service Profile provides the enterprise architecture governing time synchronization across the Air Force and the Department of Defense. The service profile introduces five mechanisms for the delivery of synchronized time. The five mechanisms are Two Way Satellite Time Transfer (TWSTT), Global Positioning System (GPS), Radio Frequency (RF), Network Time Protocol (NTP), and Modem.

This case study utilizes the Global Positioning System to synchronize base reference clocks and the Network Time Protocol to distribute time services throughout the local/metropolitan area network.

2.1 Global Positioning System

GPS is managed by the Department of Defense and provides a precise geo-positioning and highly accurate (±200 ns) time synchronization service to any user worldwide, free of charge. GPS employs a constellation of at least 24 medium earth orbit satellites, each synchronized with UTC(USNO). Each satellite in the constellation carries redundant atomic clocks to ensure precise timekeeping and availability.

GPS operates in two modes. The Standard Positioning System (SPS) provides time accuracies to within 340 ns and is provided for most non-military applications. SPS may be degraded or disabled regionally, by the DoD, to deny its use during a period of conflict.

The Precise Positioning System (PPS) provides time accuracies to within 200 ns. PPS is provided for military applications and is protected via cryptography. *Systems used for combat, combat support, or combat service support missions must use PPS capable GPS receivers operating in the Precise Positioning System (PPS) mode.* (CJCS, pE-3).

Both Standard and Precise Positioning System based equipment is commercially available and provided by multiple vendors.

2.2 Network Time Protocol

2.2.1 NTP Overview

The Network Time Protocol (NTP) is designed to synchronize time across an IP-based network. NTP has been an Internet standard for over 20 years and has evolved through four major releases. NTP runs over the User Datagram Protocol (UDP), using port 123 as both the source and destination. NTP refers to both the protocol used to distribute and synchronize time and the software that implements the protocol. Unless otherwise specified, the protocol is indicated when NTP is referenced in this document.

Version	Date	Description	Current State
ICS	18 April 1981	The Internet Clock Service (RFC 778) is the precursor for the current Network Time Protocol	Obsolete
1	July 1988	NTPv1 (RFC 1059) introduced symmetric (peer), as well as client/server mode.	Obsolete
2	1 Sept 1989	NTPv2 (RFC 1119) introduced symmetric-key authentication. XNTP software implemented the protocol	Obsolete, Backwards compatibility provided by NTP Software.
3	March 1992	NTPv3 (RFC 1305) introduced formal correctness principles and advanced algorithms, as well as introducing the broadcast mode.	Commonly used protocol, implemented in NTPv4 software. Versions of NTP software prior to 4.0.99k may be susceptible to a remotely exploitable vulnerability.
4	In Development	NTPv4 will provide new features regarding automatic configuration (e.g. manycast mode), reliability, Internet traffic reduction, and authentication (using public-key cryptography). A new kernel clock model can keep time with a precision of up to one nanosecond.	IETF Draft in process. Portions of the NTPv4 protocol implemented in NTPv4 Software.
SNTP	October 1996	SNTP (RFC 2030) provides a simple mechanism for distributing time. Many of the algorithms in NTP are not implemented in SNTP	Widely used in Microsoft systems to distribute time between domain controllers and clients.

Table 1 - Network Time Protocol History

An NTP network gets its time from an authoritative time source associated with Coordinated Universal Time (UTC) (e.g., the USNO) through one of the five delivery mechanisms described in the NTS Profile. NTP then distributes this time across the network based on the associations specified among the various machines that are running NTP software. An NTP Client issues messages to its Server over a polling interval that changes based on network conditions. Based on these messages, it possible for a Client to determine how far off its clock is from that of its Server and to make the necessary adjustments.

Despite its name, NTP is more than a communication protocol. It includes a set of algorithms for overcoming the difficulties in synchronizing clocks that must communicate with each other over networks that introduce unknown or variable delays. Additionally, NTP

tracks the error rate, or drift, inherent in system clocks and attempts to compensate during periods when a NTP server is not available.

NTP uses the concept of Stratum to describe how far removed a Server is from an authoritative time source. A Stratum 1 Time Server is directly connected to an authoritative source. Stratum 2 Servers obtain their time from on or more Stratum 1 Servers, while Stratum 3 Servers obtain their time from Stratum 2 Servers, and so on.

NTP does not immediately synchronize time across machines. It may take minutes or even hours for the ultimate degree of synchronization and accuracy to occur. NTP averages the results of several exchanges to reduce the effects of variable network latency so it may take a few minutes for NTP to reach agreement on the average latency. It also takes several adjustments for NTP to reach synchronization. This steering of time, rather than an abrupt reset, reduces unintended consequences of suddenly changing a machines clock time. The bottom line is that users should not expect NTP to immediately synchronize time across a network.

SNTP is a subset of NTP, essentially consisting of just the communication protocol and a simplified formula for interpreting time-stamps. At the protocol level SNTP is just like NTP, and NTP servers can respond to requests from NTP and SNTP clients. SNTP's timing algorithm differ from those of NTP in that its takes the time stamps at face value and sets the clock accordingly while NTP has an in-depth validation process for interpreting the time stamp.

SNTP can only receive time from NTP servers and cannot be used to provide time services to other systems. In addition, SNTP does not authenticate messages and is therefore SNTP clients are more vulnerable than NTP clients.

Windows™ machines in a domain use SNTP to automatically synchronize with the Primary Domain Controller.

2.2.2 Association Modes

The relationship between a time producer (Server) and a time consumer (Client) can be configured to operate in one of several modes. The specific modes available depend on the version NTP being used, with the following three modes being available in NTP 3

- Client/Server mode
- Symmetric Active/Passive (Peer)
- Broadcast

Machines running NTP can operate in different modes with respect to different machines. For example: a Stratum 2 machine can function as a Client of a Stratum 1 machine, while

serving as a Peer to another Stratum 2 machine, and serving as a Server to one or more Stratum 3 Clients

Each of these modes is described in greater detail below.

2.2.2.1 Client/Server Mode

Client/Server mode is the most common configuration of NTP. In a typical configuration, a Client sends an NTP message to one or more Servers and processes the replies as they are received. Information included in the reply allows the Client to determine how far of its clock is off and adjust its time to match that of the Server. The response also includes information about the Server's accuracy and Stratum.

A Client is configured in client mode by using the *server* command and specifying the DNS name or address of the Server. Configuring an association in client mode indicates the Client wishes to obtain time from the Server, but is not willing to provide time to the Server.

2.2.2.2 Symmetric Active/Passive (Peer) Mode

An NTP Peer is member of a group of same stratum NTP Servers that are tightly coupled. Unlike the Client/Server mode, where the Server will respond to Client requests but not use the Client as a potential source of time, a Peer Server will both respond to the requests of other Peers and attempt to use these requests as a better source of time. This has the effect of compensating for drift across peers and keeping the enterprise in better overall synchronization.

It is common to have one or more same Stratum Servers configured in Client Server mode with higher Stratum Clients, while Peered with one another. This provides protection against malfunctions in which one or more of the Servers fails to operate or provide incorrect time.

A Peer is configured by using the *peer* command and specifying the DNS name of IP address of the other Peer. The other Peer should be configured in the same way. If the other Peer is not configured in this way, a Peer association is activated upon the arrival of symmetric active message. Since an intruder can impersonate a Peer and inject false time values, it is recommended that this mode always be authenticated.

2.2.2.3 Broadcast Mode

An NTP Server can operate in broadcast mode in which the Server sends periodic time updates to a broadcast address. Clients listen for time updates at the broadcast address. Because broadcast messages are not forwarded by routers, a Server must be on the same subnet as its Clients. Broadcast mode is best suited for installations consisting of a few Servers and a large number of Clients, and where accuracy and security requirements are less restrictive.

The primary advantages of the broadcast mode are:

- Simplified configuration. Clients do not need to be configured for a specific Server, allowing all Clients to use the same configuration file
- Reduced network traffic because message flow is only one-way.

The primary disadvantage of the broadcast mode is reduced accuracy of time calculations. Because the communication is only one-way, the Client uses an estimate of the delay to the Server when calculating the time. When a broadcast Client first receives a broadcast, the Client estimates this delay by engaging in a brief series of exchanges with the Server in traditional Client/Server mode.

A broadcast Server is configured using the *broadcast* command and a local subnet address. A broadcast Client is configured using the *broadcastclient* command which allows the Client to respond to broadcasts received on any interface

This mode should always be authenticated because it is possible for an intruder to spoof a broadcast Server and introduce false times into the system. Broadcast mode is also more vulnerable to denial of service attacks than the other methods.

2.2.3 NTP Architecture Structures

NTP architectures generally utilize one of the following three structures:

- Flat
- Hierarchical
- Star

In a Flat Structure, all routers peer with each other and a few separate routers are configured to point to one or more external time sources. A primary drawback of this structure is that the convergence of time becomes longer as members are added to the structure.

In a Hierarchical Structure the routing hierarchy is reused for the NTP hierarchy:

- Core Routers serve as Stratum 2 Time Servers and typically receive their time from one or more external time sources via a Client/Server relationship.
- Internal Routers serve as Stratum3 Time Servers and typically receive their time from one or more of Stratum 2 Servers via a Client/Server relationship.
- Internal Clients receive their time from the Stratum 3 Servers via a Client/Server relationship.
- This pattern is then repeated down the networking hierarchy as necessary.

In a Star Structure, all routers receive their time from a few Time Servers via a Client/Server relationship. These Servers are the center of the star and are typically synchronized with one or more external time sources.

A Hierarchical Structure is the generally preferred technique because it is the most scalable of the three architecture structures. The Case Study architecture is based on the Hierarchical Structure for precisely that reason.

3 Using Existing Resources to Implement NTP

Implementing NTP at a fixed installation does not have to be an expensive proposition. Configuring existing routers as time servers and utilizing existing Windows™ Domain Controllers to synchronize SNTP clients provides an efficient and low-cost method for maintaining and distributing time via NTP.

A router's system clock can be set by a number of sources including NTP and SNTP. In turn, the router can be configured to distribute its time to other systems via several methods including NTP. This allows a router to serve as both a Server and Client in an NTP architecture.

A router maintains time internally based on UTC. It also maintains information about the local time zone and day light savings time so that it can display the local time correctly given the local conditions. The system clock also maintains information on whether its time is authoritative or not. A router will redistribute its time only if it is authoritative. Non-authoritative time is available for display purposes only.

Cisco's implementation of NTP supports Stratum 1 service in modern[1] releases of the Cisco IOS software. If the release supports the NTP *refclock* command, a radio or atomic clock can be connected to the router. Certain releases support either the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only) or the Telecom Solutions GPS device.

Certain low-end Cisco (1600 & 1700 series) routers only support SNTP. These routers can receive time from NTP Servers but cannot be used to provide time to other systems. As such they are unsuitable as Time Servers.

Windows™ 2000/XP/2003 machines in a domain utilize SNTP and W32time to synchronize with the Windows™ Domain Controller. This synchronization is essential to the internal functionality and management of the Windows™ Domain and occurs automatically.

---

[1] IP Versions of Cisco IOS 11.x or above.

3.1 Architecture Trade-Offs and Performance

The bandwidth requirements for NTP are minimal. Unencrypted NTP packets are 90 bytes. A broadcast server will send out a packet every 64 seconds. A non-broadcast client/server configuration requires 2 packets per transaction. When first started, transactions will occur about once per minute decreasing gradually to once per 17 minutes under normal conditions. Poorly synchronized Clients will tend to poll more frequently than well synchronized Clients. A well synchronized Client will use approximately 0.6 bits/second per Server. [Cisco]

Minimizing network traffic while maintaining the desired clock accuracy is a key consideration in designing an NTP architecture. The following steps can be taken to ensure that NTP does not unnecessarily over burden the network:

- Clients should be associated with local Servers and not central Servers that are connected over the WAN. In terms of this paper, the local server would be the clients default router.
- Central Servers (generally Stratum 1 and 2) should use non-broadcast modes which allow better time distribution.
- The Peer mode should be utilized for same Stratum Servers which allows for better overall synchronization across the network and provides for greater reliability and accuracy in the event that one or more of the Servers malfunction.

4 Time Distribution within a Fixed Installation

4.1 Overview

The case study depicts a fixed installation consisting of a Network Control Center (NCC) and two buildings (Building X and Building Y) connected via a network. The installation accesses NTS via a GPS terminal as described in the SV-1(b) of the Network Time Service Profile.

Each building consists of a mix of Unix-based and Windows™ 2000 machines. Existing network resources - Cisco routers and Windows™ domain controllers - serve as the mechanism for distributing time in order to keep implementation costs low. When implementing NTP, an installation should verify that its routers support NTP.

4.2 The Implementation

Time is distributed from NTS to users within the fixed installation as depicted in the figure below:

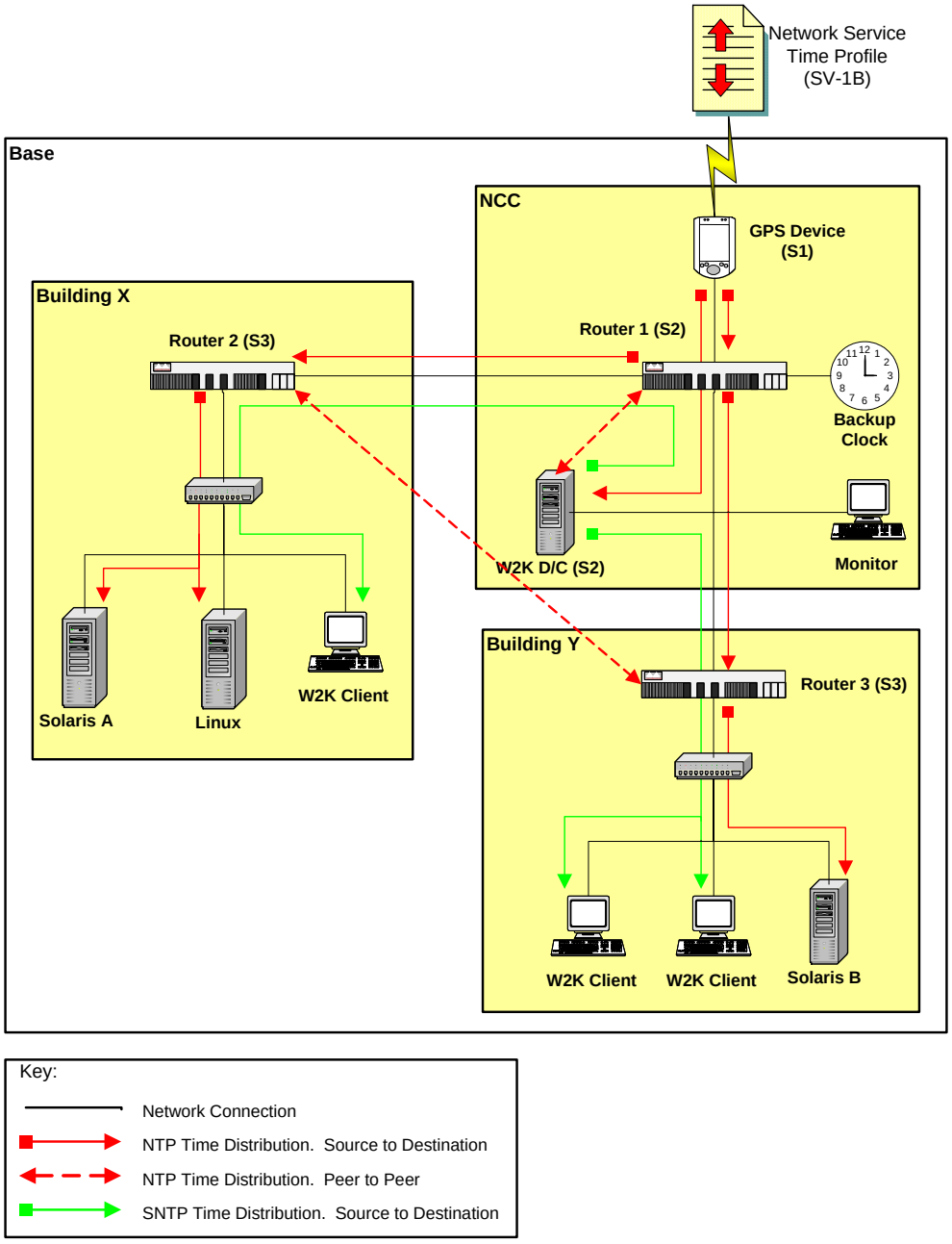

Figure 1 - Proposed Network Topology

The following machines play a role in distributing time within the installation:

Name	Description
GPS Device	A Precise Positioning System GPS receiver providing Stratum 1 Time Service and serves as the connection point to UTC(USNO).
Router 1	A Stratum 2 Time Server that is responsible for distributing time across the subnets located in Building X and Building Y. Also referred to as the Core Router.
Backup Clock	A high precision cesium or rubidium clock that allows Router 1 to maintain time more accurately. Optional depending on the need of the installation. This clock provides enhanced stability in the event of a GPS failure.
Monitor	Provides the capability for system administrators to configure, monitor, and audit time services within their installation. Use of the Network Time Toolkit is encouraged.
Windows™ Domain Controller	A Stratum 2 Time Server that distributes time, via SNTP, to Windows™ systems in the domain.
Router 2	A Stratum 3 Time Server that distributes time to Clients located in Building X.
Router 3	A Stratum 3 Time Server that distributes time to Clients located in Building Y.
Solaris Systems A and B	Solaris based Time Clients that receive time from their building's router via NTP.
Linux System	Linux based Time Clients that receive time from their building's router via NTP.
Windows™ Clients	Stratum 3 Clients that receive time from the Windows™ Domain Controller.

Table 2 - Network Time Service Devices

Time is distributed among the various machines at the installation as follows:

- The GPS device accesses the enterprise NTS as specified in the SV-1b of the Network Time Services Profile. Time provided via GPS is accurate to 200 ns using the Precise Positioning Service. The PPS Service is mandated for combat, combat support, and combat service support missions [7].
- The GPS device provides time to Router 1 and the Windows™ Domain Controller via NTP.
- Router 1 and the Windows™ Domain Controller request time from and provide time to one another via NTP.
- The Windows™ Domain Controller provides time to the Windows™ systems in the domain via SNTP.
- Router 1 provides time to Router 2 and Router 3 via NTP.
- Router 2 and Router 3 request time from and provide time to one another via NTP.

- Router 2 provides time to the Solaris A system and Linux system via NTP.
- Router 3 provides time to the Solaris B system via NTP.

Highlights of the implementation include:

- The use of local Time Servers in each subnet reduces network traffic and increases accuracy.
- Peering of the Stratum 2 Servers (Router 1 and the Windows™ Domain Controller) and the Stratum3 Servers (Router 2 and Router 3) allows for better overall synchronization across the network and provides for greater reliability and accuracy in the event that one or more of the servers malfunction or the connection to enterprise NTS is lost.
- The implementation can be extended to additional buildings by specifying a Client/Server relationship between a router in that building (acting as a Stratum 3 Server) and Router 1. That Stratum 3 Server should also be peered with the Stratum 3 Servers (Router 2 and Router 3) in the other buildings.

The following associations have been used to configure NTP:

Time Producer	Stratum	Time Consumer	Stratum	Protocol	Mode
USNO	Stratum 0	GPS Device	Stratum 1		
GPS Device	Stratum 1	Router 1	Stratum 2	NTP	Client/Server
GPS Device	Stratum 1	Windows™ Domain Controller	Stratum 2	NTP	Client/Server
Router 1	Stratum 2	Windows™ Domain Controller	Stratum 2	NTP	Peer
Windows™ Domain Controller	Stratum 2	Router 1	Stratum 2	NTP	Peer
Router 1	Stratum 2	Router 2	Stratum 3	NTP	Client/Server
Router 1	Stratum 2	Router 3	Stratum 3	NTP	Client/Server
Router 2	Stratum 3	Router 3	Stratum 3	NTP	Peer
Router 3	Stratum 3	Router 2	Stratum 3	NTP	Peer
Router 2	Stratum 3	Solaris Server A	Stratum 4	NTP	Client/Server
Router 2	Stratum 3	Linux Server	Stratum 4	NTP	Client/Server
Router 3	Stratum 3	Solaris Server B	Stratum 4	NTP	Client/Server
Windows™ Domain Controller	Stratum 2	Windows™ Devices	Stratum 3	SNTP	N/A

Table 3 - NTP Associations

4.3 Security Considerations

The time kept on a machine is critical resource and it is recommended the security features of NTP be utilized. NTP provides two security features: an access list-based restriction scheme and an encrypted authentication scheme.

Authentication keys can be used for the purposes of time synchronization, monitoring, and remote administration. NTP authentication makes use of a key which consists of the following information:

- A public key number - a 32 bit integer that can range from 1 to 4,294,967,295
- A secret key string - an arbitrary string of 32 characters, including all printable characters and spaces.

To authenticate a message, both the client and server must have a matching key number and key string defined. Therefore the key(s) must be distributed in advance. With NTP

version 3, authentication keys must be manually distributed to each of the client systems. NTP version 4 can use an automatic public key distribution.

NTP also provides the capability to define access control list to restrict access to its services based on IP addresses and host names.

4.4 Sample Configurations

The following sample configurations were taken from the Cisco- Network Time Protocol - Best Practices Whitepaper [4] and modified for the purposes of this case study. When implementing NTP at a facility, care should be taken to verify the settings appropriate for the specific devices in use at that facility. Additionally, Hardening Cisco Routers provides a thorough discussion of implementing NTP distribution through Cisco Routers.

Sample configurations have been provided for the Router 1 and the Solaris B devices

The name of a device or system enclosed in brackets indicates that its host name or IP address should be provided.

4.4.1 Router 1 Configuration

Allows NTP to update the hardware calendar chip

ntp calendar-update

Configures the Cisco IOS software as an NTP master clock with a Stratum of 2

ntp master 2

Configures Telecom-Solutions GPS time source connected via the Routers auxiliary port

line aux 0
    ntp refclock telecom-solutions pps cts stratum 1

Enable NTP Authentication. Cisco routers only support the MD5 key type.

ntp authenticate
ntp authentication-key <key #> md5 <key>
ntp trusted-key <key #>

Create access list for Peers and Clients for extra security. In this example 3 represents the group number for Peers and 4 the group number for Clients.

*access-list 3 permit [*Windows™ *D/C]*
access-list 4 permit [Router 2]
access-list 4 permit [Router 3]

Restrict access for Peers and Clients

ntp access-group peer 3
ntp access group serve 4

Configure Peer relationship with the Windows™ Domain Controller

*ntp peer [*Windows™ *D/C] <key #>*

4.4.2 Solaris B Configuration

Enable authentication and setup the authentication key pair for Client which must match that of its server

ntp authenticate
ntp authentication-key <key #> md5 <key>
ntp trusted-key <key #>

Specify Router 3 as the time server for Solaris B

ntp server [Router 3]

References

[1] [IETF RFC 1305] D. Mills, “Network Time Protocol (Version 3) Specification, Implementation”, IETF RFC 1305, March 1992.

[2] [IETF RFC 2030] D. Mills, “Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI”, IETF RFC 2030, October 1996.

[3] "Air Force Network Time Service Profile, V1.0", U.S. Air Force ESC/NI2, 28 January 2004.

[4] "Cisco - Network Time Protocol: Best Practices White paper", http://www.cisco.com/warp/public/126/ntpm.pdf. (Cisco Web site)

[5] D. Deeths and G. Brunette, "Using NTP to Control and Synchronize System Clocks - Part II: Basic NTP Administration and Architecture", Sun Microsystems, August 2001, http://www.sun.com/blueprints

[6] Thomas Akin, “Hardening Cisco Routers”, O’Reilly and Associates, February 2002

[7] 2003 CJCS Master Positioning, Navigation and Timing Plan CJCSI 6130.01C, 31 March 2003, Chairman of the Joint Chiefs of Staff (CJCS).

Distribution List

Internal

D320

B.D. Metcalf

D340

K.J. Miller

D400

J.K. Derosa

D460

K.A. Cabana

R.J. Lesch

D480

E.J. Harding-Laramee

R.S. Swarz

G.S. Bell (8)

D520

J.G. Scarano

Project

T.J Reale

External

GIGSG/CD
5 Eglin St.
Hanscom AFB, MA 01731

Mr. Thomas Powis

GIGSG/ES
5 Eglin St.
Hanscom AFB, MA 01731

LTC Michael H. Horn

Mr. Bert Hopkins

Dr. Margaret Corasick