

SYNCHRONIZING TIME SOURCES AND SETTING UP RELIABLE TIME SERVICES IN A LAN

A Technical Brief from GarrettCom®, Inc., – for use with MNS-6K-SECURE version 14.1 and higher

August 2008

SUMMARY

Networks and devices on a network need to synchronize time for various services. They do that by referencing an authoritative source for time information – usually a server called an NTP server – that replies back to time synchronization queries. Time needs to be synchronized for a variety of reasons. These include logs using *syslog*, for security issues – including but not limited to time stamping video surveillance images, for intrusion detection attempts and other security breaches.

It is a good idea to have a defined IP address within a LAN which acts as a trusted NTP source. Being a local NTP source, upstream network traffic is reduced as all devices periodically poll for time synchronization. Devices can poll the local time server, and receive a response quickly, improving efficiency.

Video surveillance cameras need to synchronize their time information as well, especially if the surveillance information is recorded and time stamped. Most surveillance cameras depend on an NTP server for synchronizing time.

One such NTP server can be a Magnum 6K switch with MNS-6K-SECURE v14.1 software. Video capture devices can be synchronized using the 6K's time sync capabilities. Other devices such as time clock card readers, door access devices, etc., that may be connected to an Ethernet network can be synchronized using this method. PC's running Windows XP, Vista or other operating systems such as Linux can also be synchronized in the same manner from the same 6K server.

This technical brief shows how the capabilities available with MNS-6K-SECURE allow a network administrator to set up a reliable time source for a LAN segment. This process can be repeated reliably across several LAN segments if needed.

BACKGROUND

The standard timescale used by most nations of the world is Coordinated Universal Time (UTC), which is based on the Earth's rotation about its axis. Time Zone offsets are typically set to the UTC, including GMT, which is an approximation of UTC.

International Atomic Time (TAI, from the French name Temps Atomique International) is a high-precision atomic time standard that tracks proper time on Earth's period. TAI is the principal realization of Terrestrial Time, and the basis for Coordinated Universal Time (UTC) which is used for civil timekeeping all over the Earth's surface. The Gregorian calendar, which is based on the Earth's rotation about the Sun, uses the UTC to designate things such as time, date, month, year, etc. The UTC timescale is modified with

respect to International Atomic Time or Temps Atomique International (TAI) by inserting leap seconds at intervals of about 18 months. UTC time is disseminated by various means, including radio and satellite navigation systems, telephone modems and portable clocks.

In 1981, the time synchronization technology was documented in the now-historic Internet Engineering Note series as IEN-173. The first specification of a public protocol developed from it appeared in RFC-778. The first deployment of the technology in a local network was as an integral function of the Hello routing protocol documented in RFC-891, which survived for many years in a network prototyping and test bed operating system called the Fuzzball. There was considerable discussion during 1989 about the newly announced Digital Time Synchronization Service (DTSS), which was adopted for the Enterprise network. The DTSS and NTP communities had much the same goals, but somewhat different strategies for achieving them. One problem with DTSS, as viewed by the NTP community, was a possibly serious loss of accuracy, since the DTSS design did not discipline the clock frequency. The problem with the NTP design, as viewed from the DTSS community, was the lack of formal correctness principles in the design process.

Simple Network Time Protocol (SNTP) and Network Time Protocol (NTP) are described in RFC-1769 as well as in RFC-2030. SNTP is compatible with NTP as implemented for the IPv4, IPv6 and OSI protocol stacks.

The article available from NIST <http://tf.nist.gov/timefreq/service/pdf/computertime.pdf> provides details on time synchronization services. Then, <http://physics.nist.gov/GenInt/Time/time.html> provides a walk through the history of time and time synchronization on the NIST site. There are many other interesting articles on network time available on the Internet.

STRATUM – WHAT IS IT?

NTP uses a hierarchical system of "clock strata". The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. (Note that this is different from the notion of clock strata used in telecommunications systems.)

Stratum 0

These are devices such as atomic (cesium, rubidium) clocks, GPS clocks or other radio clocks. Stratum-0 devices are not attached to the network; instead they are locally connected to computers (e.g. via an RS-232 connection.) The atomic clock at the NIST Denver facility is an example of the Stratum 0 clock.

Stratum 1

These are computers attached to Stratum 0 devices. Normally they act as time servers for timing requests from Stratum 2 servers via NTP. These computers are also referred to as time servers. Time servers from NIST and USNO are examples of Stratum 1 servers.

Stratum 2

These are computers that send NTP requests to Stratum 1 servers. Normally a Stratum 2 computer will reference a number of Stratum 1 servers and use the NTP algorithm to gather the best data sample, dropping any Stratum 1 servers that seem obviously wrong. Stratum 2 devices will peer with other Stratum 2 devices to provide more stable and robust time for all devices in the peer group. Stratum 2 devices normally act as servers for Stratum 3 NTP requests.

Stratum 3

These devices employ exactly the same NTP functions of peering and data sampling as Stratum 2, and can themselves act as servers for lower strata, potentially up to 16 levels. NTP (depending on what version of NTP protocol in use) supports up to 256 strata.

This is summarized in the figure below.

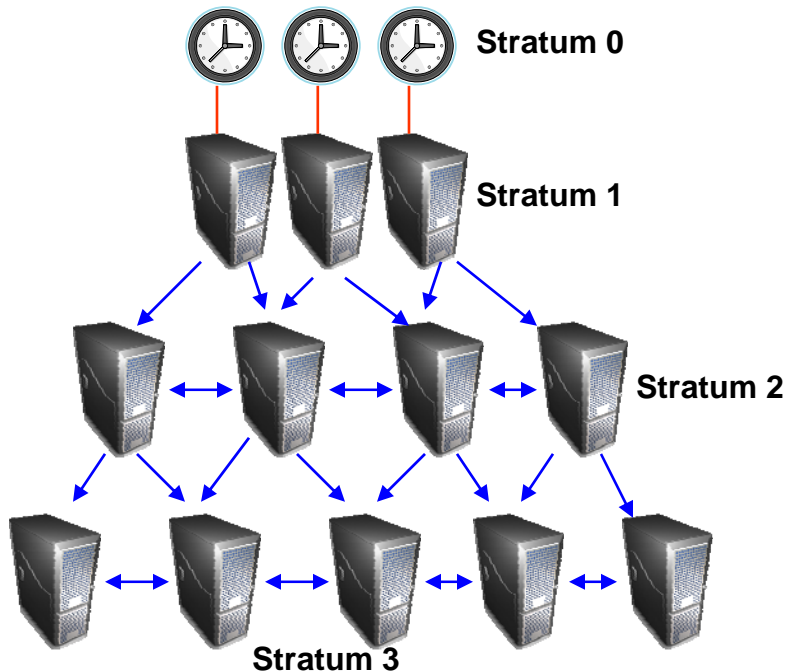


FIGURE 1 – *Different Stratum NTP servers*

Special purpose receivers are available for many time dissemination services, including the Global Position System (GPS) and other services operated by various national governments. For reasons of cost and convenience, it is not possible to equip every computer with one of these receivers. However, it is possible to equip some number of computers, routers or switches acting as primary time servers to synchronize a much larger number of secondary servers and clients connected by a common network.

Several Magnum 6K switches with MNS-6K-SECURE can act as Stratum 2 or Stratum 3 servers. To synchronize itself, make sure the SNTP client is configured to synchronize information from other Stratum 1 or Stratum 2 servers.

NTP.ORG – ROLE THE WEB SITE PLAYS

www.ntp.org provides a portal for users providing time synchronization services across the globe. Instead of accessing each individual time server and overloading the time server, the portal allows organizations to join the time synchronization pool. So for example, as of this writing, examining <http://www.pool.ntp.org>, the site shows that there are over 900 servers in Europe and over 500 servers in North America. In accessing the time from the Internet, instead of accessing the individual server, this tech brief will show how the pool can be used. The example shown in this Tech Brief is that of North America, however, local time server pool can be used by finding the appropriate pool for the continent.

SETTING UP THE TIME SERVICE

It is assumed that the Magnum 6K family of switches have MNS-6K-SECURE version 14.1 and higher.

STEP 1 – CONFIGURE THE IP ADDRESS AND DNS USING CLI

The IP address is first setup for the switch. This is done using the “ipconfig” command as shown below. Here we set the IP address of the switch to be 192.168.5.5 with a 24 bit mask. The router for the network will be 192.168.5.1. The router is setup to provide firewall services. Since the SNTP services use port 123, the router is setup to allow requests on port 123 originating from the secure side of the network to pass through the firewall.

```
Magnum6K25e # ipconfig ip=192.168.5.5 mask=255.255.255.0 dgw=192.168.5.1
```

```
IP Parameters Set.
```

```
Magnum6K25e #
```

Figure 2 – Setting the IP address

Next we set up the DNS server entry. This is done as shown below.

```
Magnum6K25e # show dns
```

```
DNS Server Address : Not Configured.
```

```
Domain Name       : Not Set
```

```
DNS Status        : Disabled.
```

```
Magnum6K25e # set dns server=68.97.166.1 enable
```

```
Domain Name Server Set.
```

```
DNS Enabled
```

```
Magnum6K25e # show dns
```

```
DNS Server Address : 68.97.166.1
```

```
Domain Name       : Not Set
```

```
DNS Status        : Enabled.
```

```
Magnum6K25e #
```

Figure 3 – Set up a DNS client by pointing the client to the DNS server configured for your network. Make sure the DNS service is enabled. Domain name can also be set and is not shown in the example above

After the DNS client is setup properly, one should be able to ping a host using the ping command. Make sure the host name is specified in the ping command instead of the IP address.

ALTERNATE STEP 1 – CONFIGURE THE DNS USING SWM

The above DNS can also be configured using SWM.

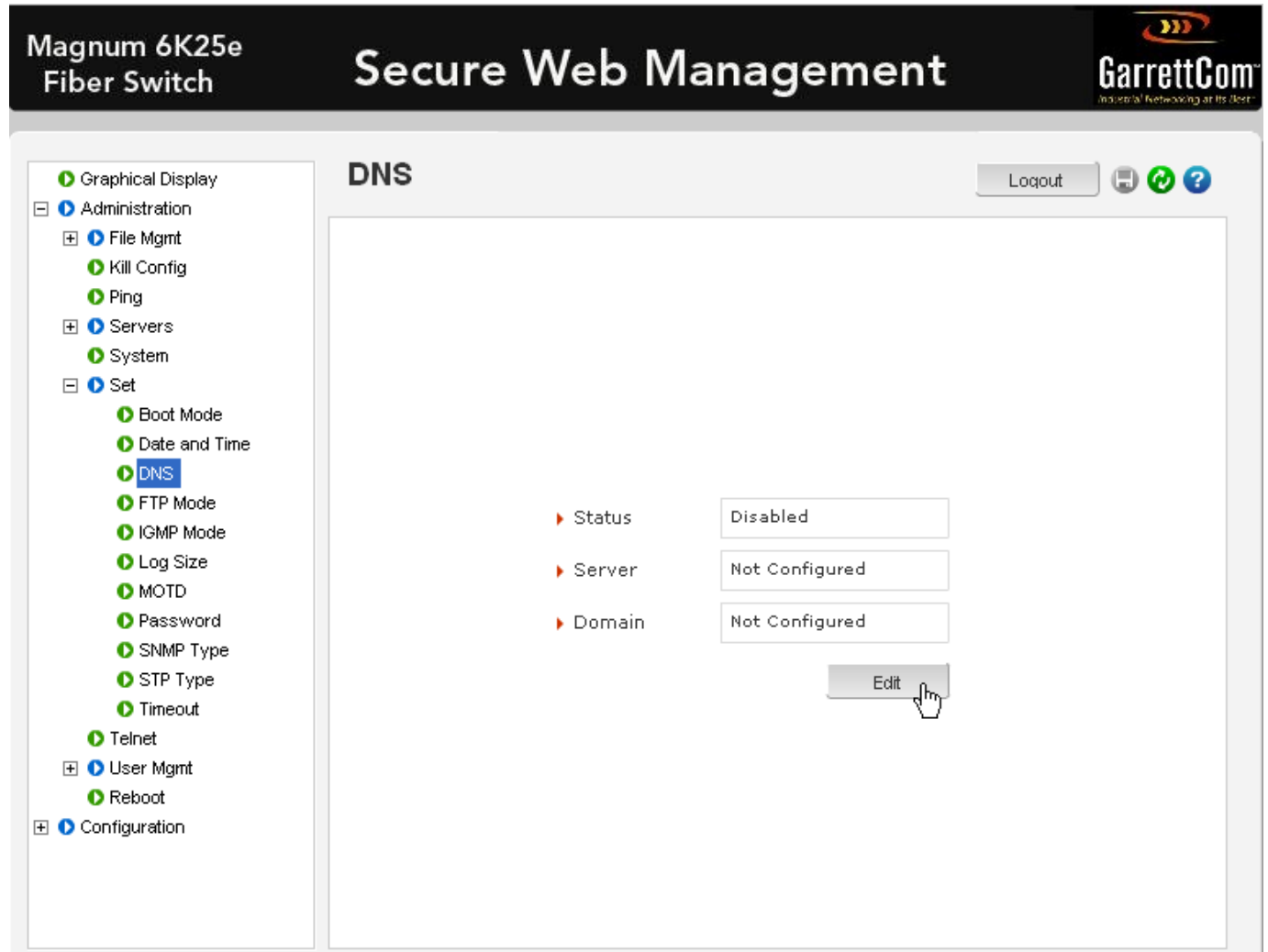


Figure 4 – Setting up DNS using SWM. Click on the edit button to configure DNS.

After Edit, enter in the value of the DNS server and make sure the DNS client is enabled.

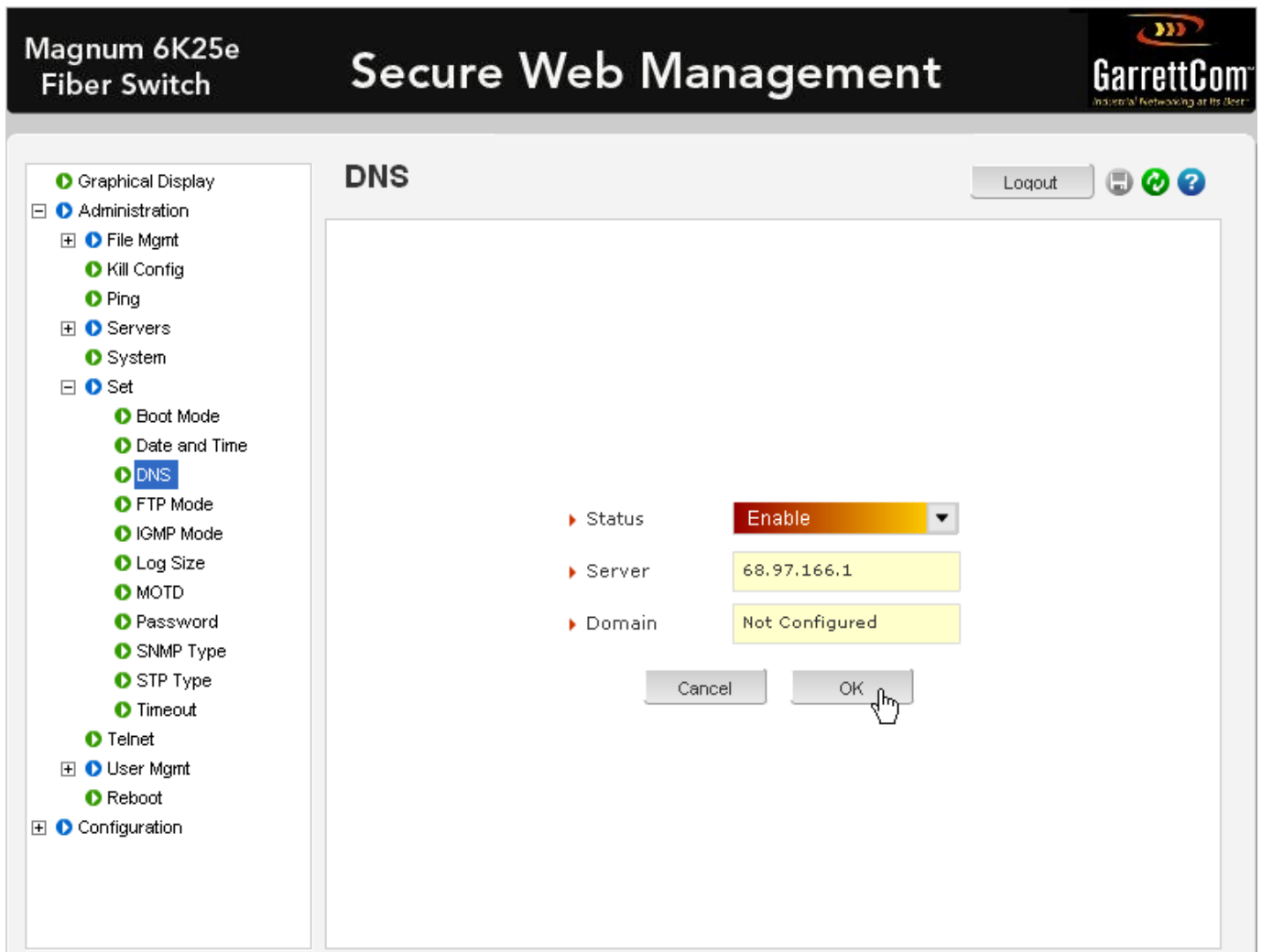


Figure 5 – Setting up the DNS client

Once done, it is always a good idea to save the changes made so far.

STEP 2 – SETUP SNTP CLIENT USING CLI

The SNTP client is setup to synchronize the time from Stratum 1 servers on the network. It is advised to use the pool of NTP servers available for the geography. To find that out visit <http://www.pool.ntp.org>

The commands used are shown below. IN the example below, we add the pool of NTP servers in North America. From the www.pool.ntp.org site we find out the pool is north-america.pool.ntp.org. The client is setup to sync with this pool once a day at 9:30pm.

If needed another pool can be added or another Stratum 1 source can be added and that pool can be synchronized approximately 12 hours from the north-america.pool.ntp.org sources. The same steps will be repeated.

Also ensure the time zone and the UTC offsets are set correctly. It is also recommended to set the time zone. In the example below the time zone is set to PST or GMT -8 hours.

```
Magnum6K25e # set daylight country=USA
```

Success in setting daylight savings to the given location/country USA

```
Magnum6K25e # set timezone GMT=- hour=8 min=0
```

Success in setting timezone

```
Magnum6K25e # sntp
```

```
Magnum6K25e (sntp) ## setsntp server=north-america.pool.ntp.org timeout=5 retry=2
```

SNTP server is added to SNTP server database

```
Magnum6K25e (sntp) ## sync hour=2 min=00
```

```
Magnum6K25e (sntp) ## sntp enable
```

SNTP is enabled.

```
Magnum6K25e (sntp) ## exit
```

```
Magnum6K25e # show date
```

System Date : Tuesday 08-12-2008 (in mm-dd-yyyy format)

```
Magnum6K25e # show time
```

Time : 12:07:04 A.M DST

Figure 6 – Setting up the daylight savings time, time zone and SNTP client to synchronize information from Stratum one pool in North America. Note – every 2 hours the SNTP reference clock is checking with the reference source for accuracy

When the SNTP service is started, the time is synchronized. Make sure the time and date are shown correctly.

ALTERNATE STEP 2 – SETUP SNTP CLIENT USING SWM

This can also be done in SWM as shown below.

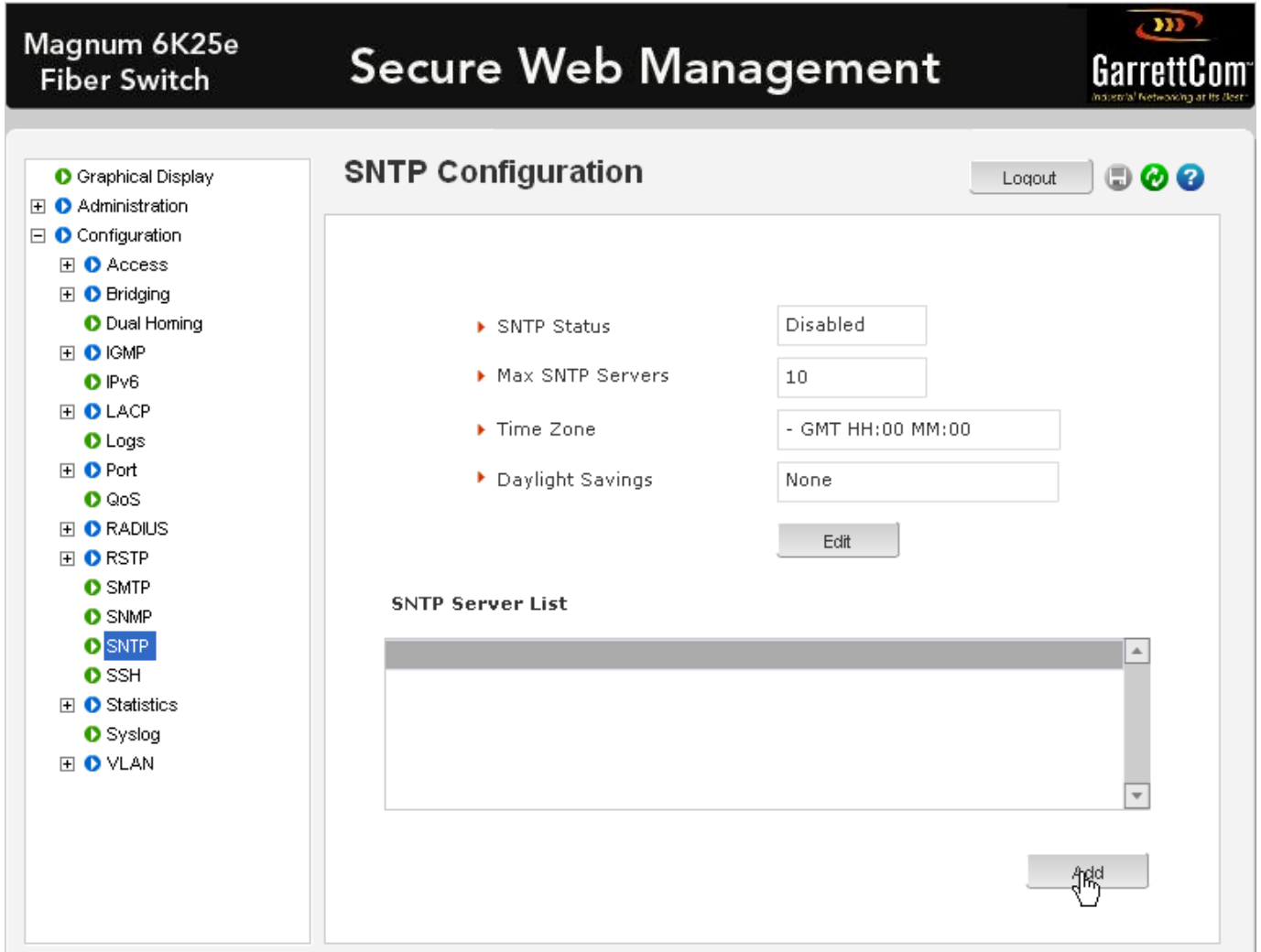
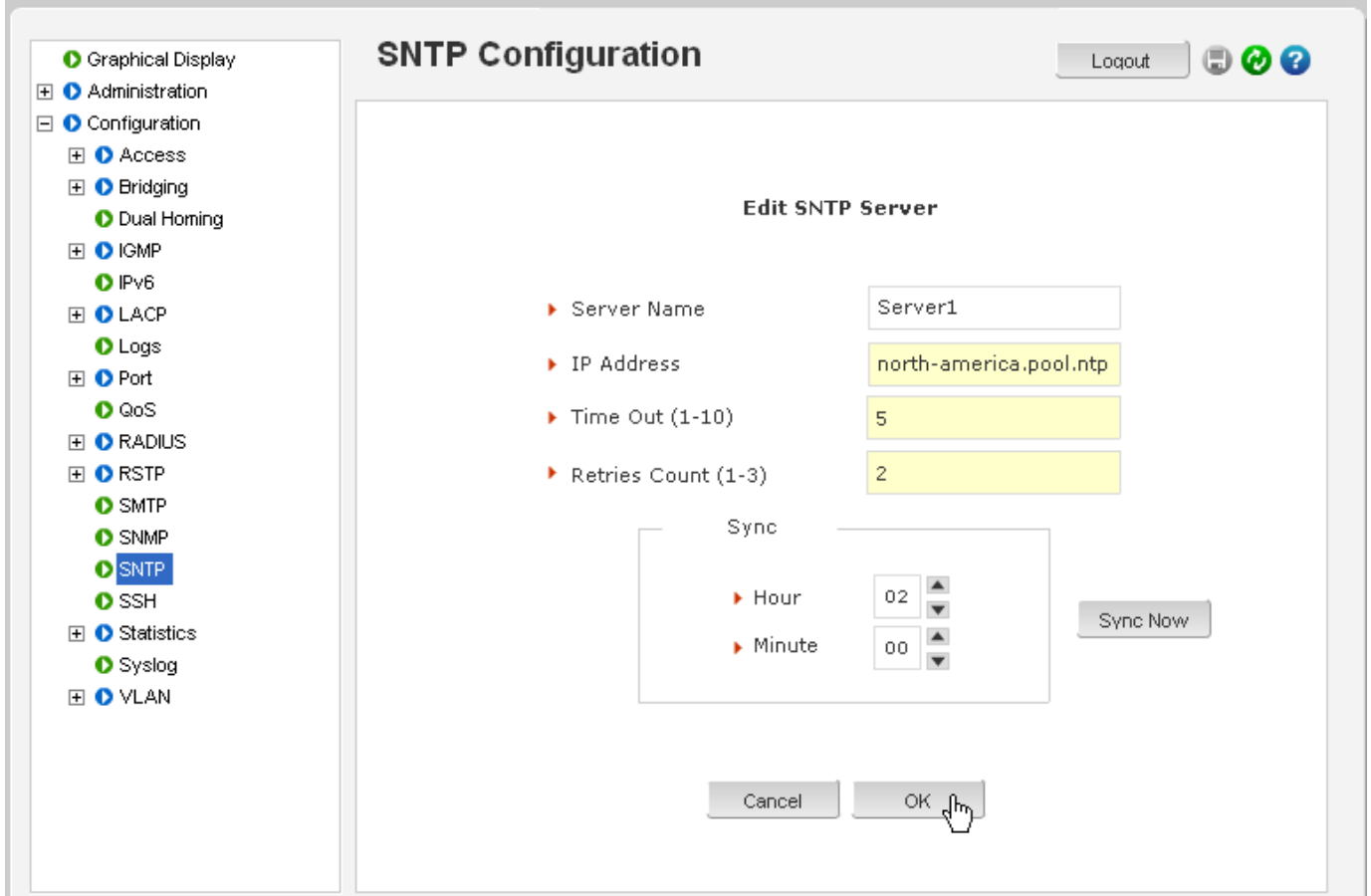


Figure 7 – Select the SNTP Client screen. Add the servers to synchronize clock information from



SNTP Configuration

Logout [Refresh] [Home] [Help]

Edit SNTP Server

- ▶ Server Name: Server1
- ▶ IP Address: north-america.pool.ntp
- ▶ Time Out (1-10): 5
- ▶ Retries Count (1-3): 2

Sync

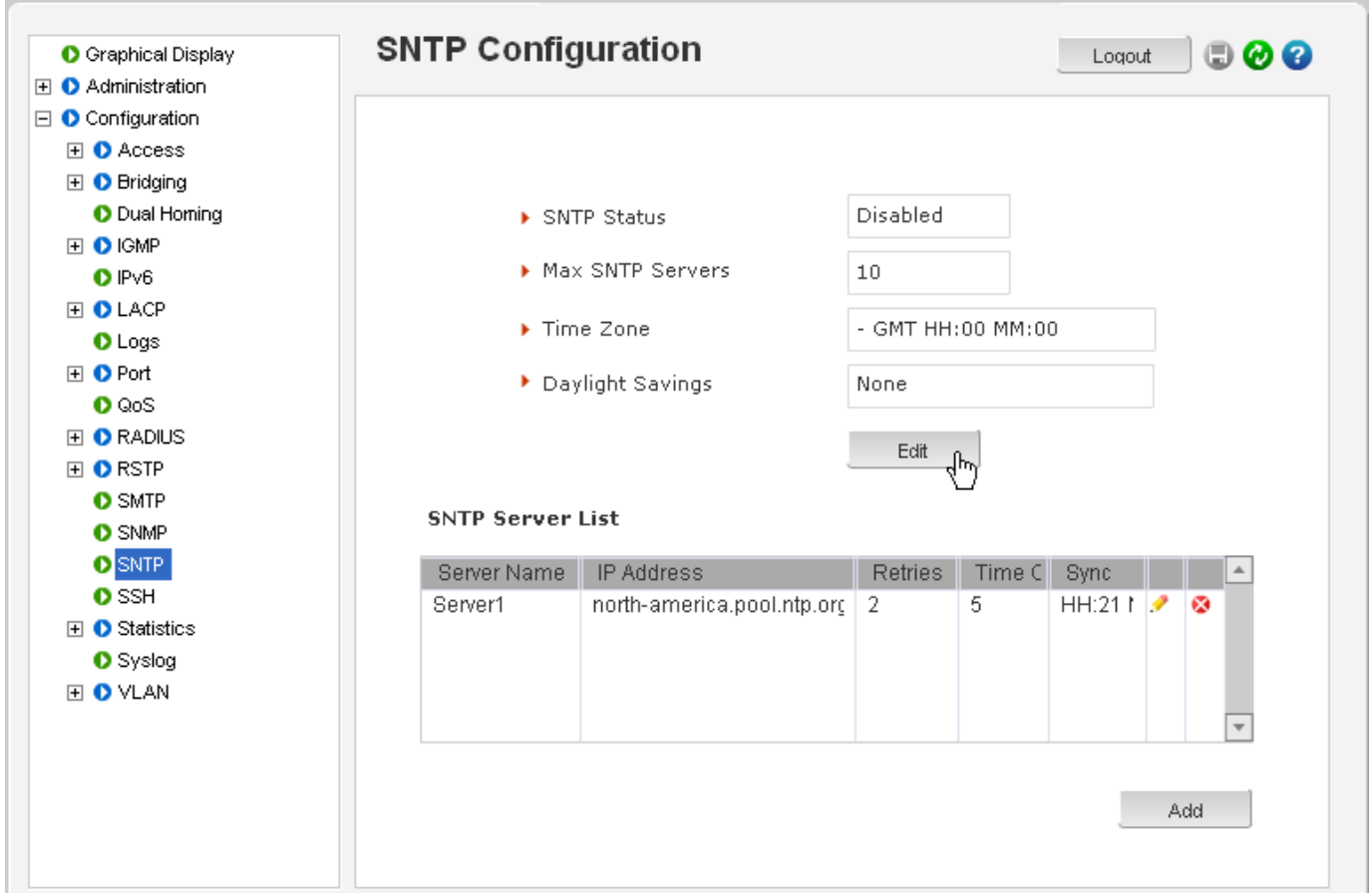
- ▶ Hour: 02
- ▶ Minute: 00

Sync Now

Cancel OK



Figure 8 – Add the north-america.pool.ntp.org as the source, timeout and retries on the SNTP screen as shown above. Also set the time when the service should try synchronizing again. Note in the “Sync” box, the Switch will synchronize with the source defined every 2 hours.

Additional NTP servers can be added as shown above. Next add information on time zone as shown below.



The screenshot shows the 'SNTP Configuration' page in the Secure Web Management interface. On the left is a navigation menu with 'SNTP' selected. The main area contains configuration fields for SNTP Status (Disabled), Max SNTP Servers (10), Time Zone (- GMT HH:00 MM:00), and Daylight Savings (None). An 'Edit' button is visible below these fields. Below the configuration is an 'SNTP Server List' table with one entry: Server1, IP Address north-america.pool.ntp.org, Retries 2, Time C 5, and Sync HH:21. There are also 'Add' and 'Logout' buttons.

SNTP Configuration

Logout  

▶ SNTP Status

▶ Max SNTP Servers

▶ Time Zone

▶ Daylight Savings

SNTP Server List



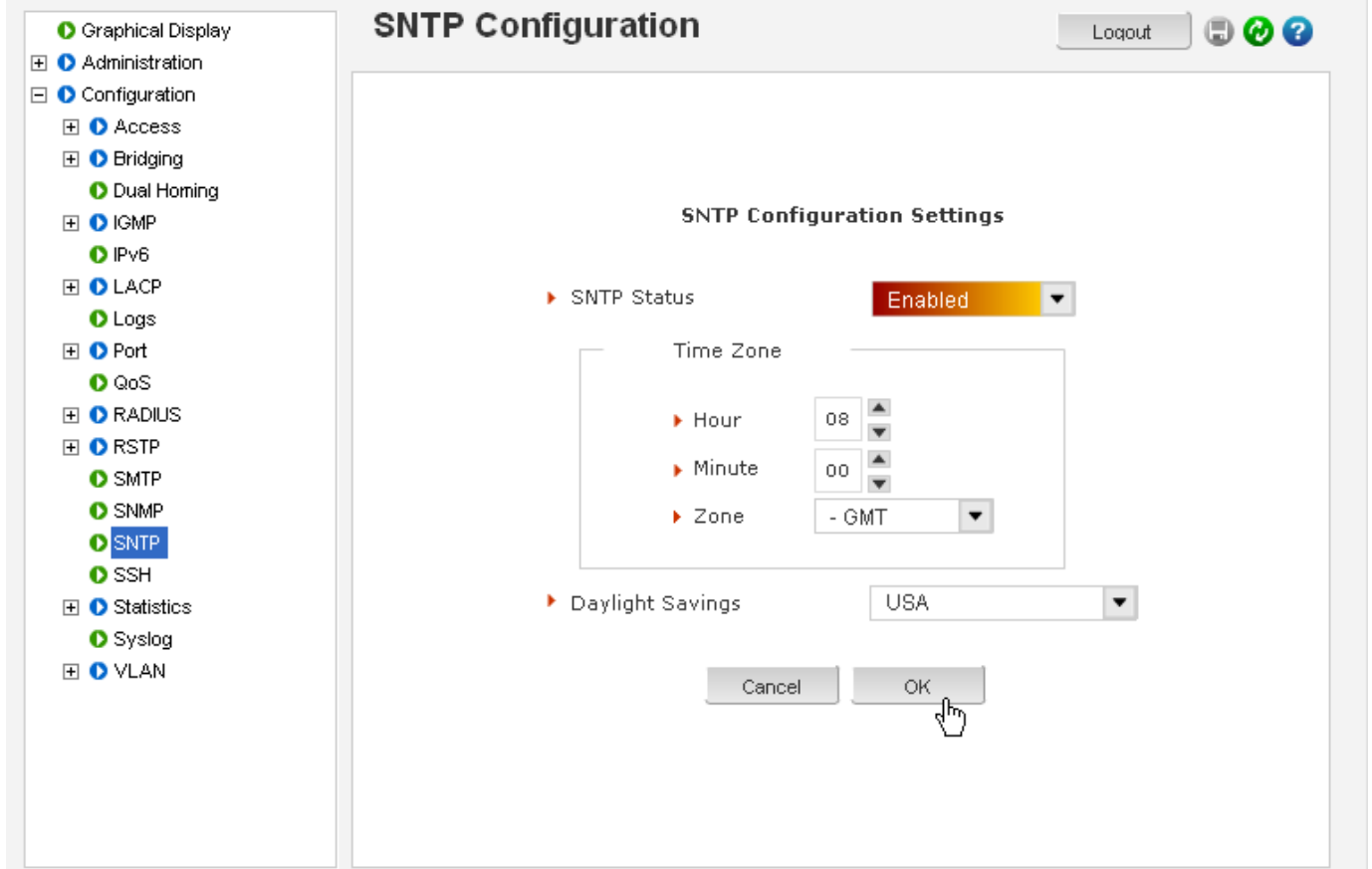
Server Name	IP Address	Retries	Time C	Sync			
Server1	north-america.pool.ntp.org	2	5	HH:21			

Figure 9 – Add the time zone, Daylight saving and other relevant information. Also enable SNTP client during this process



SNTP Configuration

Graphical Display
Administration
Configuration
Access
Bridging
Dual Homing
IGMP
IPv6
LACP
Logs
Port
QoS
RADIUS
RSTP
SMTP
SNMP
SNTP
SSH
Statistics
Syslog
VLAN

Logout

SNTP Configuration Settings

▶ SNTP Status **Enabled**

Time Zone

▶ Hour 08

▶ Minute 00

▶ Zone - GMT

▶ Daylight Savings USA

Cancel OK

Figure 10 – Setup the time zone (GMT -8) Daylight Saving Time to be of USA and start SNTP client as shown above

If needed, click on the edit button as shown below

- ▶ Graphical Display
- ⊕ Administration
- ⊖ Configuration
 - ▶ Access
 - ▶ Bridging
 - ▶ Dual Homing
 - ▶ IGMP
 - ▶ IPv6
 - ▶ LACP
 - ▶ Logs
 - ▶ Port
 - ▶ QoS
 - ▶ RADIUS
 - ▶ RSTP
 - ▶ SMTP
 - ▶ SNMP
 - ▶ **SNTP**
 - ▶ SSH
 - ▶ Statistics
 - ▶ Syslog
 - ▶ VLAN

SNTP Configuration

Logout  

- ▶ SNTP Status
- ▶ Max SNTP Servers
- ▶ Time Zone
- ▶ Daylight Savings

SNTP Server List



Server Name	IP Address	Retries (Time Ou	Sync		
Server1	north-america.	2	5	HH:21 MM:30		

Figure 11 – Click on the edit icon to edit the current entries made for SNTP server

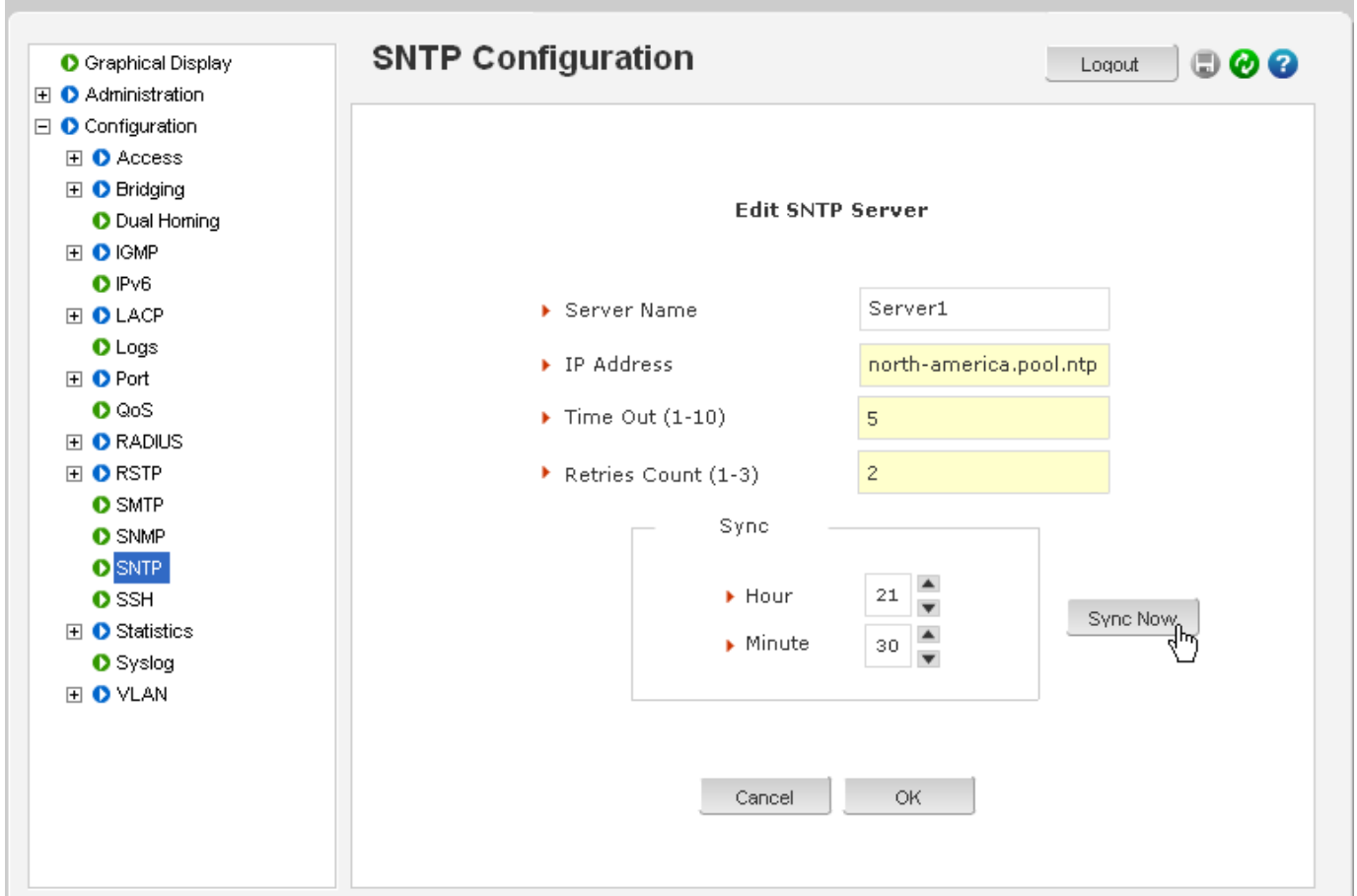
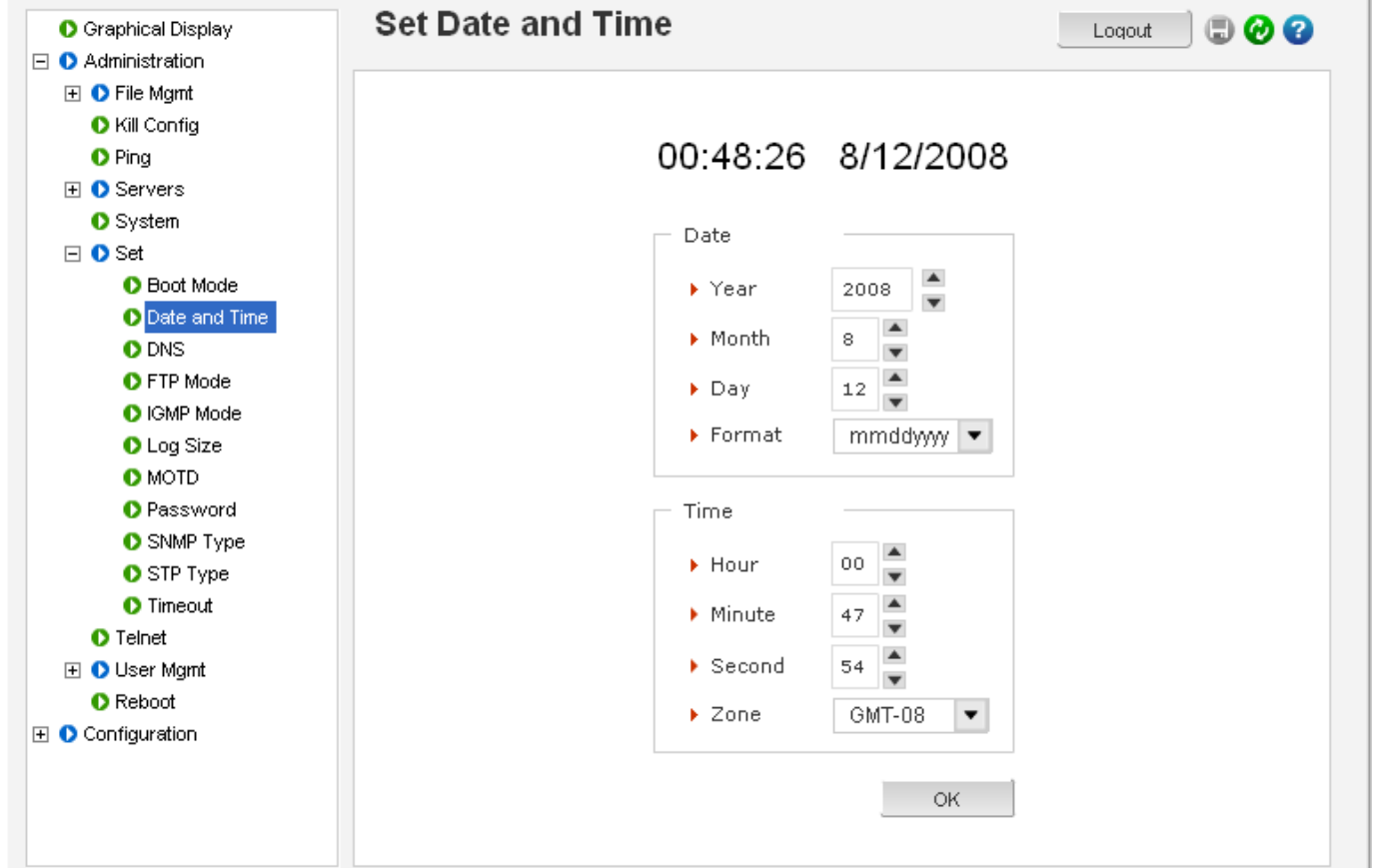


Figure 12 – The Sync Now button can force a synchronization with the time server specified

As discussed above – check if the date and time are correct and the time synchronization has taken place.



Set Date and Time Logout [Printer] [Refresh] [Help]

00:48:26 8/12/2008

Date

- Year: 2008
- Month: 8
- Day: 12
- Format: mmddyyyy

Time

- Hour: 00
- Minute: 47
- Second: 54
- Zone: GMT-08

OK

Navigation Menu:

- Graphical Display
- Administration
 - File Mgmt
 - Kill Config
 - Ping
- Servers
- System
- Set**
 - Boot Mode
 - Date and Time**
 - DNS
 - FTP Mode
 - IGMP Mode
 - Log Size
 - MOTD
 - Password
 - SNMP Type
 - STP Type
 - Timeout
- Telnet
- User Mgmt
- Reboot
- Configuration

Figure 13 – Check to see if the date and time are correct after the SNTP services have been started

STEP 3 – SETUP NTP SERVER ON MNS-6K-SECURE USING CLI

Once the sources are defined, one can start NTP server as shown below.

```
Magnum6K25e # sntpserver
Magnum6K25e (sntpserver)## sntpserver start
SNTP server started.
Magnum6K25e (sntpserver)## show sntpserver
SNTP SERVER Running
Magnum6K25e (sntpserver)## exit
Magnum6K25e # save
Saving current configuration...
Configuration saved
Saving current event logs...
Event logs saved
Magnum6K25e #
```

Figure 14 – Starting the NTP services

It is a good idea to save the configuration after this using the “save” command as shown above.

ALTERNATE STEP 3 – SETUP NTP SERVER ON MNS-6K-SECURE USING SWM

Once the sources are defined, one can start NTP server using SWM as shown below.



Figure 15 – Enable the SNTP server as shown

RECOMMENDED NEXT STEPS

First thing to do is to setup as series of redundant time servers to provide redundancy. At least two switches should be setup as time servers.

Next, make sure all devices synchronize their time from the time servers which have been setup. This will reduce the traffic bandwidth over the WAN to synchronize time.

For the security conscious, block port 123 except for the designated time servers on the network. Only allow the time servers on a LAN segment to reach out on port 123 to the designate addresses to synchronize time.

Perform an audit – especially video surveillance cameras – to ensure that they have the proper time stamp for the images being captured and stored.

It is always a good idea to secure the Magnum 6K Switch which is the NTP reference for the sub domain so that users cannot change the configuration on it. Using device access control mechanisms such as user names, passwords, TACACS+ etc. secures the device.

Ensure the syslog capability is activated to capture the logs in a central place. Ensure the logs are sorted and stored in a chronological order for proper analysis.

CONCLUSION

Once the NTP server is defined and started, other devices can synchronize the time settings from the server defined. It is a good idea to define two or three such time servers so that they can provide local alternate sources for time synchronization. Local time servers not only reduce the WAN traffic for time synchronization; it also allows the security conscious network administrators to further secure the network.

SUMMARY OF COMMANDS USED

The commands used and the purpose are summarized below.

`ipconfig ip=192.168.5.5 mask=255.255.255.0 dgw=192.168.5.1`
IP parameters for the switch

`show dns`
displays the DNS settings

`set dns server=68.97.166.1 enable`
Sets the DNS server and enables the DNS client

`set daylight country=USA`
Sets the daylight saving time Country information

`set timezone GMT=- hour=8 min=0`
Sets the GMT offset for the time zone

`sntp`
Enter the SNTP client configuration

`setsntp server=north-america.pool.ntp.org timeout=5 retry=2`
Sets the external or internal SNTP stratum 1/2/3 sources

`sync hour=21 min=30`
Sets the time at which this device should synchronize with external or internal Stratum 1/2/3 sources

`sntp enable`
Starts the SNTP client and performs the initial synchronization with the defined servers

`exit`
Exit from the SNTP setup

`show date`
Displays the date – use that to see if the date has synchronized

`show time`
Displays the time – use that to see if the time has synchronized

GarrettCom, Inc.
47823 Westinghouse Dr. • Fremont, CA 94539
PH: (510) 438-9071 • FAX: (510) 438-9072
Email: mktg@garrettcom.com • Web: www.GarrettCom.com

©2008 GarrettCom, Inc. Printed in United States of America
GarrettCom, Inc. reserves the right to change specifications, performance characteristics and/or model offerings without notice.
GarrettCom is a registered trademark of GarrettCom Inc. Magnum, S-Ring, Link-Loss-Learn, Converter Switch, Convenient Switch and Personal Switch are trademarks of GarrettCom, Inc. NEBS is a registered trademark of Telcordia Technologies. UL is a registered trademark of Underwriters Labs.

