9 Network Time Protocol

Introduction

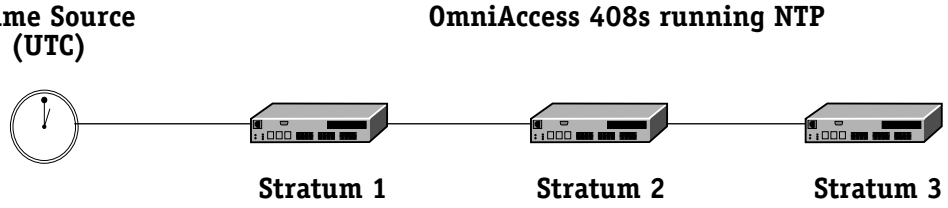
The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within a millisecond on LANs, and up to a few tens of milliseconds on WANs relative to a primary server synchronized to Coordinated Universal Time (UTC) (via a Global Positioning Service receiver, for example). Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability. Some configurations include cryptographic authentication to prevent accidental or malicious protocol attacks.

It is important for networks to maintain accurate time synchronization between network nodes. The standard timescale used by most nations of the world is based on a combination of Universal Coordinated Time (UTC), (representing the Earth's rotation about its axis) and the Gregorian Calendar (representing the Earth's rotation about the Sun). The UTC timescale is disciplined with respect to International Atomic Time (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.

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 computers with these clocks, which then act as primary time servers to synchronize a much larger number of secondary servers and clients connected by a common network. In order to do this, a distributed network clock synchronization protocol is required which can read a server clock, transmit the reading to one or more clients, and adjust each client clock as required. Protocols that do this include the Network Time Protocol (NTP).

Stratum

Stratum is the term used to define the relative proximity of a node in a network to a time source (such as a radio clock). Stratum 1 is the server connected to the time source itself. (In most cases the time source and the stratum 1 server are in the same physical location.) An NTP client or server connected to a stratum 1 source would be stratum 2. A client or server connected to a stratum 2 machine would be stratum 3, and so on, as demonstrated in the diagram below.



The farther away from stratum 1 a device is, the more likely there will be discrepancies or errors in the time adjustments done by NTP. A list of stratum 1 and 2 sources available to the public can be found on the Internet.

♦ Note ♦

It is not required that NTP be connected to an officially recognized time source (for example, a radio clock). NTP can use any time source to synchronize time in the network.

Using NTP in a Network

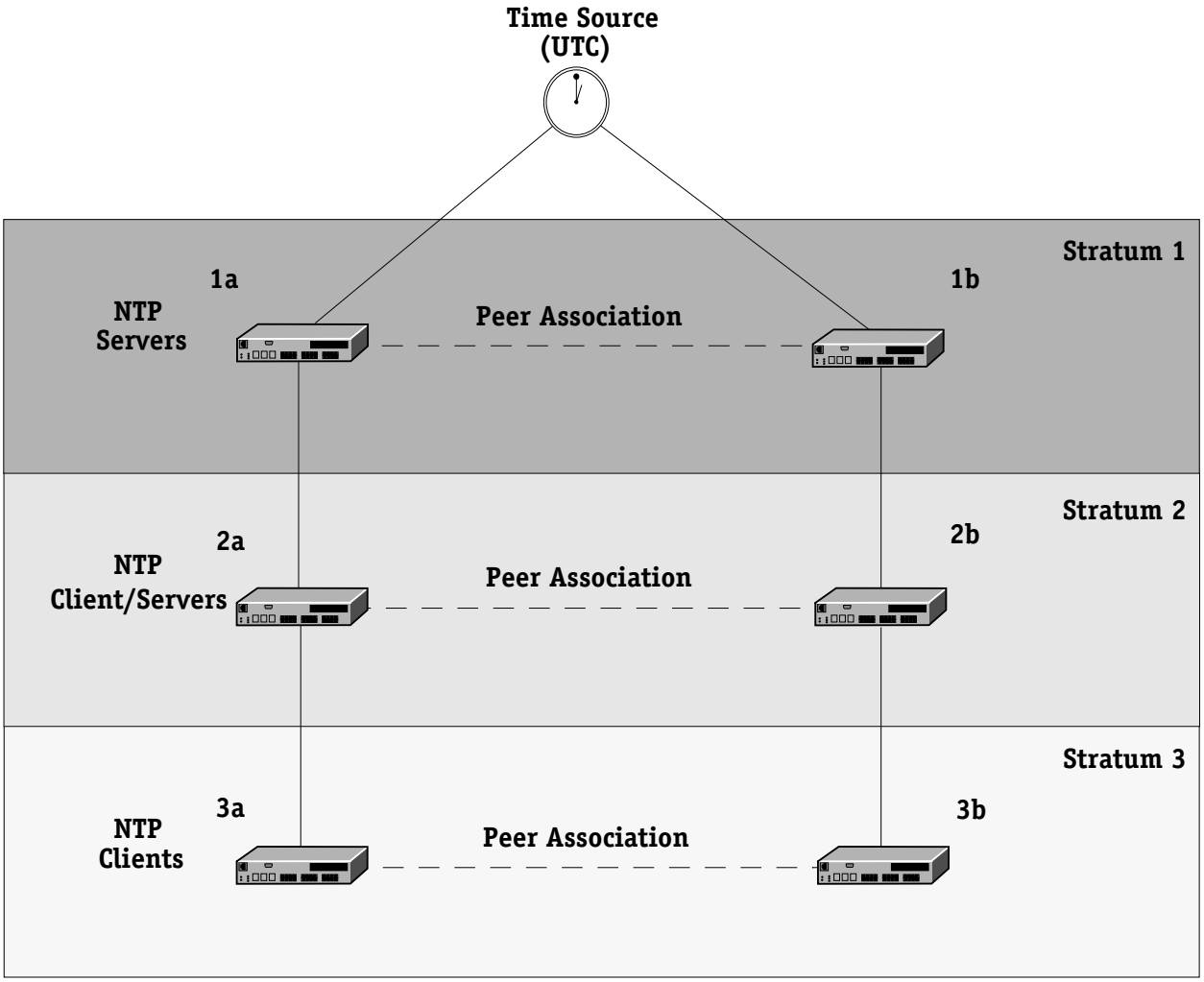
NTP operates on the premise that there is one true standard time (defined by UTC), and that if several servers claiming synchronization to the standard time are in disagreement, then one or more of them must be out of synchronization or not functioning correctly.

The stratum gradiation is used to qualify the accuracy of a time source along with other factors such as advertised precision and the length of the network path between connections. NTP operates with a basic distrust of time information sent from other network entities, and is most effective when multiple NTP time sources are integrated together for checks and cross-checks.

To achieve this end, there are several modes of operation that an NTP entity can use when synchronizing time in a network. These modes help predict how the entity behaves when requesting or sending time information, listed below:

- A switch can be a client of an NTP server (usually of a lower stratum), receiving time information from the server but not passing it on to other switches.
- A switch can be a client of an NTP server, and in turn be a server to another switch or switches.
- A switch (regardless of its status as either a client or server) must be *peered* with another switch. Peering allows NTP entities in the network of the same stratum to regard each other as reliable sources of time and exchange time information.

Examples of these are shown in the simple network diagram below:



Servers 1a and 1b receive time information from, or synchronize with, a UTC time source such as a radio clock. (In most cases, these servers would not be connected to the same UTC source, though it is shown this way for simplicity.) Servers 1a and 1b become stratum 1 NTP servers and are peered with each other, allowing them to check UTC time information against each other. These machines support machines 2a and 2b as clients, and these clients are synchronized to the higher stratum servers 1a and 1b.

Clients 2a and 2b are also peered with each other for time checks, and become stratum 2 NTP servers for more clients (3a and 3b, which are also peered).

In this hierarchy, the stratum 1 servers synchronize to the most accurate time source available, then check the time information with peers at the same stratum. The stratum 2 machines synchronize to the stratum 1 servers, but do not send time information to the stratum 1 machines. Machines 2a and 2b in turn provide time information to the stratum 3 machines.

It is important to consider the issue of robustness when selecting sources for time synchronization. It is suggested that at least three sources should be available, and at least one should be “close” to you in terms of network topology. It is also suggested that each NTP client is peered with at least three other same stratum clients, so that time information crosschecking will be performed.

When planning your network, it is helpful to use the following general rules:

- It is usually not a good idea to synchronize a local time server with a peer (in other words, a server at the same stratum), unless the latter is receiving time updates from a source that has a lower stratum then from where the former is receiving time updates. This minimizes common points of failure.
- Peer associations should only be configured between servers at the same stratum level. Higher Strata should configure lower Strata, not the reverse.
- It is inadvisable to configure time servers in a domain to a single time source. Doing so invites common points of failure.

NTP and Authentication

NTP is designed to use either DES or MD5 encryption authentication to prevent outside influence upon NTP timestamp information. This is done by using a key file. The key file is loaded into the switch memory, and consists of a text file that lists key identifiers that correspond to particular NTP entities.

If authentication is enabled on an NTP switch, any NTP message sent to the switch must contain the correct key ID in the message packet to use in decryption. Likewise, any message sent from the authentication enabled switch will not be readable unless the receiving NTP entity possesses the correct key ID.

Key files are created by a system administrator independent of the NTP protocol, and then placed in the switch memory. An example of a key file is show below:

```
1     N     29233e0461ecd6ae     # des key in NTP format
2     M     RIrop8KPPvQvYotM     # md5 key as an ASCII random string
14    M     sundial              # md5 key as an ASCII string
15    A     sundial              # des key as an ASCII string
```

In a key file, the first token is the key number ID, the second is the key format, and the third is the key itself. (The text following a "#" is not counted as part of the key, and is used merely for description.) There are 4 key formats:

N	Indicates a DES key written as a hex number, in NTP standard format with the high order bit of each octet being the odd parity bit.
M	Indicates an MD5 key written as a 1 to 31 character ASCII string with each character standing for a key octet.
A	Indicates a DES key written as a 1 to 8 character string in 7-bit ASCII format, where each character stands for a key octet string.
S	Indicates a DES key written as a hex number in the DES standard format, with the low order bit of each octet being the odd parity bit.

For information on activating authentication, specifying the location of a key file, and configuring key IDs for switches, see the following sections:

- *Configuring an NTP Client* on page 9-6
- *Configuring a New Peer Association* on page 9-12
- *Configuring a New Server* on page 9-13
- *Configuring a Broadcast Time Service* on page 9-13

Network Time Protocol Management Menu

To access the NTP management menu, connect to a switch via a console or telnet session and enter **NTP** at the system prompt. If you are in verbose mode, or enter a question mark (?) at the prompt, the following screen is displayed:

```
Command          NTP Management Menu
---------------  ------------------------------------------------------------
Ntconfig         Enter the NTP configuration menu
Ntinfo           Enter the NTP information menu
Ntstats          Enter the NTP statistics menu
Ntadmin          Enter the NTP administration menu
Ntaccess         Enter the NTP access control menu

   Main      File      Summary    VLAN      Networking
   Interface Security  System     Services  Help
```

Ntconfig. This command accesses the NTP configuration menu, which allows you to configure this NTP device, add or remove peer associations, add an NTP server, configure this NTP device's broadcast time, and set or change this NTP device's fudge factor. See *NTP Configuration Menu* on page 9-6 for more information on the NTP configuration menu.

Ntinfo. This command accesses the NTP information menu, which allows you to view a list of all peers for this NTP device, display a list of peers with summary information (in two different formats), display detailed information for one or more peers, and display local server information. See *NTP Information Menu* on page 9-15 for more information.

Ntstats. This command accesses the NTP statistics menu, which allows you to view the statistics for the loop filter, peer memory usage, I/O subsystem, local server, event time subsystem, packet counts, leap second state, clock status, monitoring routines data. See *NTP Statistics Menu* on page 9-23 for more information.

Ntadmin. This command accesses the NTP administration menu, which allows you to set the receive timeout, set an encryption delay, specify a remote NTP server, set a password and key ID for this NTP device, set and clear a system flag, and restart the NTP software. See *NTP Administration Menu* on page 9-33 for more information.

Ntaccess. This command accesses the NTP access control menu, which allows you to change the authentication key ID for request and control messages, reinitalize the key ID list, add a key ID to or remove a key ID from the trusted list, display the state of the authentication code, create or remove restrict and add flags to an entry, view a servers restriction list, remove a restriction entry from this NTP device, and configure, remove or view traps set in the server. See *NTP Access Control Menu* on page 9-36 for more information.

NTP Configuration Menu

To view the NTP configuration menu, enter the **ntconfig** command at the system prompt. If you are in verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (**?**) at the prompt to display this menu:

```
Command          NTP Configuration Menu
--------------   ------------------------------------------------------------
ntpiconfig       Initial NTP configuration
ntpaddpeer       configure a new peer association
ntpaddserv       configure a new server
ntpbcast         configure broadcasting time service
ntpunconfig      unconfigure existing peer assocations
ntpprec          set the server's advertised precision
ntpfudge         set/change one of a clock's fudge factors

   Related Menus:
   Ntconfig   Ntinfo   Ntstats   Ntadmin   Ntaccess
```

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

A switch can be configured to act as an NTP client, or an NTP client/server. An NTP client receives updates from an NTP server without passing on time information to other clients, while and NTP client/server receives time information from a server, and acts as a server for other clients in a higher stratum.

Configuring an NTP Client

To set up the NTP client, use the **ntpiconfig** command as follows:

1. Enter the command as shown, at the system prompt:

   ```
   ntpiconfig
   ```

   The following menu appears:

   ```
                        NTP Startup Configuration


   1) Response timeout                    : 0
   2) Authentication delay                : No
   3) Authentication key file name        : UNSET
   4) NTP client mode                     : Ucast
   5) Enable monitor                      : No
   6) Enable NTP server                   : No
   ```

2. Adjust the configurable variables for this NTP client as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

   ```
   <lineNumber>=<value>
   ```

   For example, to change the **Response timeout** to 10, you would enter **1** (the line number for **Response timeout**), an equal sign (**=**), and the number **10** (the new value), as shown:

   ```
   1=10
   ```

After enabling NTP for this switch, you need to configure at least one peer association, unless you will be supplying time synchronization. In that case, you need to configure a reference clock.

For information on adding a peer association, see *Configuring a New Peer Association* on page 9-12.

Field Descriptions

The following section describes the fields displayed using the **ntpconfig** command.

1) Response timeout

This field sets the timeout period for responses to server queries. Server queries come from the server responsible for providing this client with NTP time information. The default is 8000 milliseconds.

2) Authentication delay

This field sets a specified time interval that is added to timestamps included in requests to the server that required authentication. Typically this delay is needed in cases of long delay paths, or of servers whose clocks are unsynchronized.

3) Authentication key file name

The key file is a file that holds the NTP authentication keys used during remote access or configuration of the server responsible for this client. This fields allows you to specify the name of the key file. The key file should be kept in the **/flash** directory of the switch.

Specifying a key file expands the NTP Startup Configuration menu. For more information on configuring authentication, see *Configuring Client/Server Authentication* on page 9-9.

4) NTP client mode

This field allows you to set how the client mode of this device sends its server queries. The options are **U** (for unicast), **B** (for broadcast), or **M** (for multicast).

Setting the NTP client mode to broadcast or multicast expands the NTP Startup Configuration menu. A suboption for the NTP client mode appears, allowing you to specify the broadcast or multicast address, as shown:

```
41) NTP multicast address                    :
```

Enter the broadcast of multicast address at the prompt by typing line number **41**, and equal sign (**=**), and the IP address. For example, to specify a multicast address of 204.0.1.1, you would enter the following:

```
41=204.0.1.1
```

5) Enable monitor

This field turns NTP monitoring on or off. Entering **yes** activates NTP monitoring, while entering **no** deactivates this function. The statistics for monitoring can be viewed using the **ntpmon** command in the statistics menu. See *NTP Statistics Menu* on page 9-23 for more information.

6) Enable NTP server

This field allows you to enable the server portion of the NTP software for this NTP device. When set to **yes**, this device can act as an NTP server for other clients. When set to **no**, this device is only a client of another NTP server.

Configuring an NTP Client/Server

A switch can be configured to act both as a client and a server. If you want to run both the client and server portions of the NTP software, follow the steps below:

1. Enter the command as shown, at the system prompt:

   ntpiconfig

   The following menu appears:

```
                    NTP Startup Configuration


1) Response timeout                          : 0
2) Authentication delay                      : No
3) Authentication key file name              : UNSET
4) NTP client mode                           : Ucast
5) Enable monitor                            : No
6) Enable NTP server                         : No
```

2. Adjust the configurable variables for this NTP client as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

   <lineNumber>=<value>

   For example, to change the **Response timeout** to 10, you would enter **1** (the line number for **Response timeout**), an equal sign (**=**), and the number **10** (the new value), as shown:

   1=10

3. Enable the NTP server by entering a **6**, an equal sign (**=**), and **yes** at the prompt, as shown:

   6=yes

   The NTP Startup Configuration menu expands to display new options. The menu now appears similar to the following:

```
                    NTP Startup Configuration


1) Response timeout                          : 0
2) Authentication delay                      : No
3) Authentication key file name              : UNSET
4) NTP client mode                           : Ucast
5) Enable monitor                            : No
6) Enable NTP server                         : No
  61) Client limit                               : 3
  62) Client limit period                        : 3600
  63) Enable server authentication               : No
  64) Advertised precision                       : -7
  65) Broadcast delay                            : 0
```

4. Adjust the configurable variables for this NTP server as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

   <lineNumber>=<value>

   For example, to change the **Client limit** to 10, you would enter **61** (the line number for **Client limit**), an equal sign (**=**), and the number **10** (the new value), as shown:

   61=10

Field Descriptions

The following section describes the expanded menu options.

61) Client limit

This field allows you to set a specific number of clients that are allowed to make requests of the server during a specified time period. Setting this field to **0** allows an unlimited number of clients to connect to the server.

62) Client limit period

This field allows you to set the client limit time period (in seconds). This along with the **client limit** field above determine how many clients are allowed to make requests of this server.

63) Enable server authentication

This field enables the authentication of unsynchronized peers. If set to **yes**, NTP only synchronizes with peers that has been authenticated with the correct key ID.

64) Advertised precision

Sets the precision which the server advertises to the specified value. This should be a negative integer in the range -4 through -20.

65) Broadcast delay

This fields allows you to set a specified network delay time. Normally, NTP automatically compensates for the network delay between the broadcast/multicast server and the client. If this calibration fails, the delay set here is used instead.

Configuring Client/Server Authentication

In order to use authentication, you must specify a key file. A key file contains the keys necessary for NTP to decode encrypted NTP messages. To specify a key file, follow the steps below:

1. Enter the command as shown, at the system prompt:

   ntpiconfig

   The following menu appears:

NTP Startup Configuration

1) Response timeout : 0
2) Authentication delay : No
3) Authentication key file name : UNSET
4) NTP client mode : Ucast
5) Enable monitor : No
6) Enable NTP server : No

2. Adjust the configurable variables for this NTP client as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

   <lineNumber>=<value>

   For example, to change the **Response timeout** to 10, you would enter **1** (the line number for **Response timeout**), an equal sign (**=**), and the number **10** (the new value), as shown:

   1=10

3. Enable authentication by entering a **3**, and equal sign (=), and a key file name at the prompt, as shown:

   3=ntp.keys

   The NTP Startup Configuration menu expands to display new options. The menu now appears similar to the following:

NTP Startup Configuration

```
1) Response timeout                          : 0
2) Authentication delay                      : No
3) Authentication key file name              : ntp.keys
  31) Configuration info authentication key    :
  32) Control request authentication key       :
  33) Configuration change authentication key  :
4) NTP client mode                           : Ucast
5) Enable monitor                            : No
6) Enable NTP server                         : No
```

4. Adjust the configurable variables for authentication as needed by entering the line number, and equal sign, and a new value at the system prompt, as shown:

   <lineNumber>=<value>

   For example, to change the **Configuration info authentication key** to 10, you would enter **1** (the line number for **Configuration info authentication key**), an equal sign (**=**), and the number **10** (the new value), as shown:

   1=10

Field Descriptions

The following section describes the expanded menu options.

31) Configuration info authentication key

The number of the key in the key file used to authenticate configuration information. Configuration information sets configuration parameters. For more information on the key file, see *NTP and Authentication* on page 9-4.

32) Control request authentication key

The number of the key in the key file used authenticate control requests. Control requests come from other NTP clients and servers. For more information on the key file, see *NTP and Authentication* on page 9-4.

33) Configuration change authentication key

The number of the key in the key file used authenticate configuration change requests. Configuration change requests come from other NTP clients and servers. For more information on the key file, see *NTP and Authentication* on page 9-4.

Configuring a New Peer Association

When you have configured the NTP client and/or server, you will need to set at least one peer association for the switch. An NTP peer is a machine of the same stratum that will compare and check time information sent from the switch, and in turn send time information to the switch.

To configure a new peer, enter the **ntpaddpeer** command in the following manner:

ntpaddpeer <address> [<keyId> <version> <minpol>] [prefer]

where **<address>** is the either the domain name or IP address of the peer machine. The optional configuration items are described below:

<keyId>. An unsigned 32-bit integer key identifier for encryption authentication. The default is for no key ID.

<version>. The version of NTP being used. The options are versions 1, 2, or 3. If no number is entered, it is assumed that version 3 is being used.

<minpol>. The minimum poll interval for time checks to this peer. The number entered is seconds raised to the power of 2.

prefer. An identifier that marks this peer as a preferred source of time information. In a situation where multiple peers could provide time information to this client, the preferred peer is the one that is used.

For example, to add a peer with an address of 1.1.1.1, a key identifier of 5, using version 3 of NTP, minimum poll of 16 seconds, and marked as a preferred server, you would enter the following:

ntpaddpeer 1.1.1.1 5 3 4 prefer

When you have finished press **<return>**. A brief message appears confirming the addition of a new peer.

Configuring a New Server

For the switch to synchronize its time, you must specify a server, or servers, from which the switch receives time information. This is done with the **ntpaddserv** command.

To add a synchronization server to a switch, use the command that follows:

ntpaddserv <address> [<keyId><version><minpol>] [prefer]

where **<address>** is the either the domain name or IP address of the server. The optional configuration items are described below:

<keyId>. An unsigned 32-bit integer key identifier for encryption authentication. The default is no key ID.

<version>. The version of NTP being used. The options are versions 1, 2, or 3. If no number is entered, it is assumed that version 3 is being used.

<minpol>. The minimum poll interval for time checks to this server. The number entered is seconds raised to the power of 2.

prefer. An identifier that marks this peer as a preferred source of time information. In a situation where multiple peers could provide time information to this client, the preferred peer is the one that is used.

For example, to add a peer with an address of 1.1.1.1, a key identifier of 5, using version 3 of NTP, with a poll time of 16, and marked as a preferred server, you would enter the following:

ntpaddpeer 1.1.1.1 5 3 4 prefer

When you have finished press **<return>**. A brief message appears confirming the addition of a new server.

Configuring a Broadcast Time Service

The NTP server can be configured to operate in broadcast mode, where the server sends periodic broadcast messages to a client population by using the broadcast or multicast address specified. To configure the server to use a broadcast or multicast address, enter the **ntpbcast** command as shown:

ntpbcast <address> [<keyId>] [<version>] [<minpol>]

where **<address>** is the either the domain name or the broadcast or multicast address.

♦ Important Note ♦

A multicast address of 224.0.1.1 has been assigned to NTP. Presently, this is the only address that should be used for multicast messages.

The optional configuration items are described below:

<keyId>. An unsigned 32-bit integer key identifier for encryption authentication. The default is no key ID.

<version>. The version of NTP being used. The options are versions 1, 2, or 3. If no number is entered, it is assumed that version 3 is being used.

<minpol>. The minimum poll interval for time checks to this server. The number entered is in seconds raised to the power of 2.

For example, to add broadcast address 1.1.1.1 with a key identifier of 5, using version 3 of NTP, and a minimum poll time of 16 seconds, you would enter the following:

```
ntpbcast 1.1.1.1 5 3 4
```

When you have finished press **<return>**. A brief message appears confirming the addition of a new server.

Unconfigure Existing Peer Associations

You can remove server, peer, or reference clock associations for this switch using the **ntpunconfig** command. This will remove a selected address from this switch's list of configured addresses. To do this, enter the **ntpunconfig** command as follows:

```
ntpunconfig <address>
```

where **<address>** is the either the domain name or IP address of the association. For example, to remove a peer association with address 1.1.1.1, enter the following:

```
ntpunconfig 1.1.1.1
```

When you have finished press **<return>**. A brief message appears confirming the addition of a new server.

You can remove multiple addresses at one time by adding additional addresses to the command. For example, to remove a peer association with address 1.1.1.1 and a reference clock association with address 1.1.1.2, enter:

```
ntpunconfig 1.1.1.1 1.1.1.2
```

When you have finished press **<return>**. A brief message appears confirming the removal of the association.

Set the Server's Advertised Precision

If necessary, you can adjust the server's advertised precision. The precision of a server is a signed integer indicating the precision of the clocks in seconds to the nearest power of 2. It determines how accurate the clock is under normal circumstances, and allows NTP to determine which is the best time source for synchronization. To set the servers advertised precision, enter the **ntpprec** command as shown:

```
ntpprec <interval>
```

where **<interval>** is the signed integer in seconds. This number must be between -4 and -20. For example, to set the server's advertised precision to -5, you would enter the following:

```
ntpprec -5
```

When you have finished press **<return>**. A brief message appears confirming the change of the advertised precision.

♦ Note ♦

The determination of a server's advertised precision in based largely on the clock type used as the ultimate time source (stratum 1).

NTP Information Menu

To view the NTP configuration menu, enter the **ntinfo** command at the system prompt. If you are using verbose mode, the NTP configuration menu is displayed. Otherwise, enter a question mark (**?**) at the prompt to display this menu:

```
Command          NTP Information Menu
---------------  ------------------------------------------------------------
ntplpeers        display list of peers the server knows about
ntppeers         display peer summary information
ntpdmpeers       display peer summary info the way Dave Mills likes it
ntpshowpeer      display detailed information for one or more peers
ntpvers          print version number
ntpinfo          display local server information

   Related Menus:
   Ntconfig   Ntinfo   Ntstats   Ntadmin   Ntaccess
```

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Display List of Peers the Server Knows About

The **ntplpeers** command is used to display a brief list of all NTP associations related to this switch (servers, peers, etc.).

To display a list of NTP associations, enter the **ntplpeers** command at the system prompt. A display similar to the following is shown:

```
client 1.1.1.1
client 1.1.1.2
sym_active 1.1.1.3
```

The list shows the mode this switch is using in relation to the association, and the address of the remote association. The address is either a domain name or an IP address. The available modes are as follows:

Symmetric Active (1) — A host in this mode sends periodic messages regardless of the reachability state of stratum of its peer. By operating in this mode the host announces its willingness to synchronize and be synchronized by the peer.

Symmetric Passive (2) — This type of association is ordinarily created upon the arrival of a message from a peer operating in the symmetric active mode and persists only as long as the peer is reachable and operating at a stratum level less than or equal to the host; otherwise the association is dissolved. The association will always persist until at least one message has been sent in reply. By operating in this mode the host announces its willingness to synchronize and be synchronized by the peer.

Client (3) — A host operating in this mode sends periodic messages regardless of the reachability state of stratum of its peer. By operating in this mode the host, usually a LAN workstation, announces its willingness to be synchronized, but not to synchronize the peer.

Server (4) This type of association is ordinarily created upon arrival of a client request message and exists only in order to reply to that request, after which the association is dissolved. By operating in this mode the host, usually a LAN time server, announces its willingness to synchronize, but not be synchronized by the peer.

Broadcast (5) A host operating in this mode sends periodic messages regardless of the reachability state or stratum of the peers. By operating in this mode, the host, usually a LAN time server operating on a a high-speed broadcast medium, announces its willingness to synchronize all peers, but not be synchronized by any of them.

♦ Note ♦

The mode of the switch in relation to the remote association is determined when you create the association. See *NTP Configuration Menu* on page 9-6 for more information on creating NTP associations.

Display Peer Summary Information

The **ntppeers** command displays a more detailed version of the **ntplpeers** command. To display a list of peers that includes summary information, enter the **ntppeers** command at the system prompt. A screen similar to the following appears:

	remote	local	st	poll	reach	delay	offset	disp
=	1.1.1.1	0.0.0.5	16	64	0	0.00000	0.00000	16.0000
+	1.1.1.2	0.0.0.5	1	64	0	0.00000	0.00000	16.0000
=	1.1.1.3	0.0.0.5	2	64	0	0.00000	0.00000	16.0000

The symbols at the very left of this table note the relationship (mode) of the switch to the remote association. The section below is a key for interpreting these symbols:

+ The switch is in symmetric active mode.

- The switch is in symmetric passive mode.

= The switch is in client mode.

^ The switch is broadcasting to this address.

~ The switch is receiving broadcasts from this address.

***** The switch is currently synchronizing with this address.

Field Descriptions

The following sections describe the fields displayed using the **ntppeers** command

Remote. The IP address of the remote association.

Local. The local interface address assigned by NTP to the remote association. If this address is **0.0.0.0**, then the local address has yet to be determined.

St. The stratum level of the remote peer. If this number is **16**, the remote peer has not been synchronized.

Poll. The polling interval, in seconds.

Reach. The reachability register of the remote association, in octal format. This number is determined by the NTP algorithm.

Delay. The currently estimated delay of this remote association, in seconds. This time is determined by the NTP algorithm.

Offset. The currently estimated offset of this remote association, in seconds. This time is determined by the NTP algorithm.

Disp. The currently estimated dispersion of this remote association, in seconds. This time is determined by the NTP algorithm.

Display Alternate Peer Summary Information

The **ntpdmpeers** command displays a more detailed version of the **ntpshowpeer** command with a slightly different output than the **ntppeers** command. To display a list of peers that includes summary information, enter the **ntpdmpeers** command at the system prompt. A screen similar to the following appears:

	remote	local	st	poll	reach	delay	offset	disp
+	1.1.1.1	0.0.0.5	16	64	0	0.00000	0.00000	16.0000
+	1.1.1.2	0.0.0.5	1	64	0	0.00000	0.00000	16.0000
*	1.1.1.3	0.0.0.5	2	64	0	0.00000	0.00000	16.0000

This table is identical to the **ntppeers** command except for the symbols displayed on the far left side. A key for the symbols is provided below:

- **.** Indicates that the remote association was cast aside during the false ticker detection.
- **+** Indicates that the remote association was accepted and not discarded by the false ticker detection.
- ***** Indicates the remote association the switch is currently synchronizing with.

Display Detailed Information for One or More Peers

The **ntpshowpeer** command allows you to view detailed NTP information about any remote associations of this switch. To view detailed NTP information about a remote association enter the **ntpshowpeer** command in the following manner:

```
ntpshowpeer <address>
```

where **<address>** is the either the domain name or IP address of the remote association. For example, to show information for a peer with IP address 1.1.1.4, enter:

```
ntpshowpeer 1.1.1.4
```

A screen similar to the following is displayed:

```
remote 1.1.1.4, local 0.0.0.6
hmode sym_active, pmode server, stratum 16, precision -7
leap 11, refid [0.0.0.0], rootdistance 0.00000, rootdispersion 0.00000
ppoll 6, hpoll 6, keyid 0, version 3, association 41807
valid 0, reach 000, unreach 0, flash 000, boffset 0.00391, ttl/mode 0
timer 32s, flags config, bclient
reference time:          00000000.00000000 Thu, Feb 7 1936 6:28:16.000
originate timestamp:     00000000.00000000 Thu, Feb 7 1936 6:28:16.000
receive timestamp:       00000000.00000000 Thu, Feb 7 1936 6:28:16.000
transmit timestamp:      00000000.00000000 Thu, Feb 7 1936 6:28:16.000
filter delay:      0.00000 0.00000 0.00000 0.00000
                   0.00000 0.00000 0.00000 0.00000
filter offset:     0.000000 0.000000 0.000000 0.000000
                   0.000000 0.000000 0.000000 0.000000
filter order:      7     6     5     4
                   3     2     1     0
offset 0.000000, delay 0.00000, dispersion 16.00000, selectdisp 0.00000
```

It is possible to display information from more than one remote association by adding more addresses when entering the **ntpshowpeer** command. For example, to display information on a peer with IP address 1.1.1.4 and a peer with IP address 1.1.1.5, enter:

```
ntpshowpeer 1.1.1.4 1.1.1.5
```

Field Descriptions

The following section describes the fields displayed using the **ntpshowpeer** command.

Remote. The IP address of the remote association.

Local. The local interface address assigned by NTP to the remote association. If this address is **0.0.0.0**, then the local address has yet to be determined.

Hmode. The host mode of this remote association. There are five possible modes: symmetric active, symmetric passive, client, server, and broadcast. The displayed mode is assumed if this association becomes the switch's host NTP server. For a description of the modes, see *Display List of Peers the Server Knows About* on page 9-15. For a description of how to set a switch host NTP server, see *Specify the Host Whose NTP Server We Talk To* on page 9-34.

Pmode. The peer mode of this remote association. There are five possible modes: symmetric active, symmetric passive, client, server, and broadcast. The displayed mode is assumed if this association becomes the switch's host NTP server. For a description of the modes, see *Display List of Peers the Server Knows About* on page 9-15. For a description of how to configure a peer, see *Configuring a New Peer Association* on page 9-12

Stratum. The stratum level of the remote peer. If this number is **16**, the remote peer has not been synchronized.

Precision. The advertised precision of this association, which is a number from -4 to -20. For information on setting the advertised precision, see *Configuring an NTP Client* on page 9-6 and *Set the Server's Advertised Precision* on page 9-14.

Leap. The status of leap second insertion for this association. Leap seconds are seconds that are added to the timestamp of an NTP entity to correct accumulated time errors. The possible values are:

00	No warning.
01	Last minute has 61 seconds.
10	Last minute has 59 seconds.
11	Alarm condition (clock not synchronized).

Refid. This is a 32-bit code identifying the particular reference clock. In the case of stratum 0 (unspecified) or stratum 1 (primary reference source), this is a four-octet, left-justified, zero-padded ASCII string. In the case of stratum 2 and greater (secondary reference) this is the four-octet Internet address of the peer selected for synchronization.

Rootdistance. This is a signed fixed-point number indicating the total roundtrip delay to the primary reference source at the root of the synchronization subnet, in seconds. Note that this variable can take on both positive and negative values, depending on clock precision and skew.

Rootdispersion. This is a signed fixed-point number indicating the maximum error relative to the primary reference source at the root of the synchronization subnet, in seconds. Only positive values are possible.

Ppoll. The poll time for this association when it is a peer. This number is the minimum interval between transmitted messages, in seconds as a power of two. For instance, a value of six indicates a minimum interval of 64 seconds.

Hpoll. The poll time for this association when it is a host. This number is the minimum interval between transmitted messages, in seconds as a power of two. For instance, a value of six indicates a minimum interval of 64 seconds.

KeyID. This is an integer identifying the cryptographic key used to generate the message authentication code.

Version. The version of NTP this association is using; the options are **1**, **2**, or **3**.

Association. The number of seconds since this NTP entity was associated with the switch.

Valid. This is an integer counter indicating the valid samples remaining in the filter register. It is used to determine the reachability state of an association, and when the poll interval should be increased or decreased.

Reach. This is a shift register used to determine the reachability status of this peer. The NTP algorithm uses this when determining timestamp information.

Unreach. The number of times this NTP entity was unreachable.

Flash. This field displays the number of error bits from the packet procedure.

Boffset. This field displays the default broadcast delay in seconds.

TTL/mode. This fields displays the Time-to-Live (TTL) time in seconds and the mode (unicast, multicast, or broadcast) of NTP messages sent to a broadcast address. For information on configuring an NTP broadcast address, see *Configuring a Broadcast Time Service* on page 9-13.

Timer. Shows the number of seconds until the next NTP message is sent to an association.

Flags Config. This counter lists what flags have been configured for this NTP entity. For more information about setting flags, see *Set a System Flag (Auth, Bclient, Monitor, Stats)* on page 9-35.

Reference Time. This is the local time, in timestamp format, when the local clock was last updated. If the local clock has never been synchronized, the value is zero.

Originate Timestamp. This is the local time, in timestamp format, of the peer when its last NTP message was sent. If the peer becomes unreachable the value is set to zero.

Receive Timestamp. This is the local time, in timestamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable the value is set to zero.

Transmit Timestamp. This is the local time, in timestamp format, when the last NTP message was sent from this association.

Filter delay. NTP comes with various filter routines as part of the algorithm that determines timestamp information. This field shows the delay in seconds the NTP algorithm uses to correct for delays caused by messages traversing through the NTP filters.

Filter offset. NTP comes with various filter routines as part of the algorithm that determines timestamp information. This counter indicates the offset of the peer clock relative to the local clock due to filters.

Filter order. The order in which NTP messages pass through filters.

Delay. The currently estimated delay of this remote association, in seconds. This number indicates the roundtrip delay of the peer clock relative to the local clock over the network path between them, in seconds. Note that this variable can take on both positive and negative values, depending on clock precision and skew-error accumulation. This time is determined by the NTP algorithm.

Offset. The currently estimated offset of this remote association, in seconds. This counter indicates the offset of the peer clock relative to the local clock. This time is determined by the NTP algorithm.

Disp. The currently estimated dispersion of this remote association, in seconds. This counter indicates the maximum error of the peer clock relative to the local clock over the network path between them, in seconds. Only positive values greater than zero are possible. This time is determined by the NTP algorithm.

Print Version Number

The **ntpvers** is used to show the version number of the xntp file. To display the version number, enter the **ntpvers** command at the system prompt. A message similar to the following is shown:

```
xntp Fri Apr 9 22:52:46 PDT 1999 (1)
```

Display Local Server Information

The **ntpinfo** command is used to display information about the local switch's implementation of NTP. To view local switch NTP information, enter the **ntpinfo** command at the system prompt. A screen similar to the following is shown:

```
system peer:          0.0.0.0
system peer mode:     unspec
leap indicator:       11
stratum:              16
precision:            -7
root distance:        0.00000 s
root dispersion:      0.00000 s
reference ID:         [0.0.0.0]
reference time:       00000000.00000000 Thu, Feb 7 1936 6:28:16.000
system flags:         monitor stats
frequency:            0.000 ppm
stability:            0.000 ppm
broadcastdelay:       0.003906 s
authdelay:            0.000122 s
```

Field Descriptions

The following section explains the fields shown using the **ntpinfo** command.

System peer. The IP address of the switch.

System peer mode. The peer mode of this remote association. There are five possible modes: symmetric active, symmetric passive, client, server, and broadcast. The displayed mode is assumed if this association becomes the switch's host NTP server. For a description of the modes, see *Display List of Peers the Server Knows About* on page 9-15. For a description of how to configure a peer, see *Configuring a New Peer Association* on page 9-12

Leap indicator. The status of leap second insertion for this association. Leap seconds are seconds that are added to the timestamp of an NTP entity to correct accumulated time errors. The possible values are:

00	No warning.
01	Last minute has 61 seconds.
10	Last minute has 59 seconds.
11	Alarm condition (clock not synchronized)

Stratum. The stratum level of the remote peer. If this number is **16**, the remote peer has not been synchronized.

Precision. The advertised precision of the switch. It will be a number between -4 and -20.

Root distance. This is a signed fixed-point number indicating the total roundtrip delay to the primary reference source at the root of the synchronization subnet, in seconds. Note that this variable can take on both positive and negative values, depending on clock precision and skew.

Rootdispersion. This is a signed fixed-point number indicating the maximum error relative to the primary reference source at the root of the synchronization subnet, in seconds. Only positive values are possible.

Reference ID. This is a 32-bit code identifying the particular reference clock. In the case of stratum 0 (unspecified) or stratum 1 (primary reference source), this is a four-octet, left-justified, zero-padded ASCII string. In the case of stratum 2 and greater (secondary reference) this is the four-octet Internet address of the peer selected for synchronization.

Reference time. This is the local time at which the local clock was last set or corrected.

System Flags. This counter lists what flags have been configured for this NTP entity. For more information about setting flags, see *Set a System Flag (Auth, Bclient, Monitor, Stats)* on page 9-35.

Frequency. A number indicating the local clock's frequency in relation to a reference clock's Pulse per Second (PPS). If the clock is running in perfect synchronization, this number should be 1. Otherwise, it will be slightly lower or higher in order to compensate for the time difference.

Stability. The residual frequency error (in seconds) remaining after the system frequency correction is applied.

Broadcastdelay. The broadcast delay, in seconds, of this association. For information on how to set the broadcast delay, see *Configuring a Broadcast Time Service* on page 9-13.

Authdelay. The authentication delay, in seconds, of this association. For information on how to set the authentication delay, see *Set the Delay Added to Encryption Time Stamps* on page 9-33.

NTP Statistics Menu

To view the NTP Statistics Menu, enter the **ntstats** command at the system prompt. If you are in verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (**?**) at the prompt to display this menu:

```
Command         NTP Statistics Menu
--------------  ------------------------------------------------------------
ntpstat         display local server statistics
ntppstat        display server statistics associated with particular peer(s)
ntploopinfo     display loop filter information
ntpmem          display peer memory usage statistics
ntpio           display I/O subsystem statistics
ntptimer        display event timer subsystem statistics
ntpreset        reset various subsystem statistics counters
ntppreset       reset stat counters associated with particular peer(s)
ntpctlstat      display packet count statistics from the control module
ntpleap         display the current leap second state
ntpmon          turn the server's monitoring facility on or off
ntpmlist        display data the server's monitor routines have collected

   Related Menus:
   Ntconfig   Ntinfo   Ntstats   Ntadmin   Ntaccess
```

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Display Local Server Statistics

The **ntpstat** command allow you to view statistics for the local NTP entity (switch). To view statistics, enter the **ntpstat** command at the system prompt. A display similar to the following is displayed:

```
system uptime:                  0
time since reset:               0
bad stratum in packet:          0
old version packets:            0
new version packets:            16
unknown version number:         0
bad packet length:              0
packets processed:              0
bad authentication:             0
limitation rejects:             0
```

Field Descriptions

The following section describes the fields displayed using the **ntpstat** command.

system uptime. The number of seconds the local NTP server has been associated with the switch.

time since reset. The number of seconds since the last time the local NTP server was restarted.

bad stratum in packet. The number of NTP packets received that had a corrupted stratum bit in the data of the packet.

old version packets. The number of NTP packets received that were of an older version of NTP (either version 1 or 2).

new version packets. The number of NTP packets received that were version 3 of NTP.

unknown version number. The number of NTP packets received for which the version was unknown (most likely due to packet corruption).

bad packet length. The number of NTP packets received that did not fit the NTP packet structure (most likely due to packet corruption).

packets processed. The total number of NTP packets processed.

bad authentication. The number of NTP packets rejected because they did not meet authentication standards.

limitation rejects. The number of NTP packets rejected because there were restrictions set on their point of origin. For information on setting restrictions, see *Create Restrict Entry/Add Flags to Entry* on page 9-39.

Display Server Statistics Associated with Particular Peer(s)

The **ntppstat** command allows you to view statistics for a specific NTP peer. To view statistics for a peer, enter the **ntppstat** command as shown:

```
ntppstat <ipAddress>
```

where **<ipAddress>** is the address of the peer for which you want to view statistics. For example, to view statistics for a peer with IP address 131.218.18.4, enter the following:

```
ntppstat 131.216.18.4
```

A screen similar to the following displays:

```
remote host              : 131.216.18.4
local interface          : 0.0.0.0
time last received       : 9s
time until next send     : 6s
reachability change      : 2973s
packets sent             : 184
packets received         : 181
bad authentication       : 2
bogus origin             : 2
duplicate                : 6
bad dispersion           : 69
bad reference time       : 1
candidate order          : 1
```

Field Descriptions

The following section describes the fields displayed using the **ntppstat** command.

remote host. The IP address of the host whose statistics you are viewing.

local interface. The local interface address assigned by NTP to the remote association. If this address is **0.0.0.0**, then the local address has yet to be determined.

time last received. The number of seconds since the last NTP message packet was received from another NTP entity in the network.

time until next send. The number of seconds until this NTP peer sends out an NTP message packet.

reachability change. This field displays the number of times this client/server's reachability has changed.

packets sent. The number of NTP message packets this peer has sent out.

packets received. The number of NTP message packets this peer has received.

bad authentication. The number NTP message packets this peer has rejected due to failed authentication.

bogus origin. The number of times a response packet from another NTP entity doesn't match the request packet sent out by this client/server.

duplicate. The number of identical NTP message packets this peer has received.

bad dispersion. The number of packets that were discarded due to overly large error dispersions.

bad reference time. The number of packets that were discarded because the contained reference time didn't match the local peer expectation.

candidate order. A number that represents this client/server's synchronization order. A lower number represents a reliable synchronization source.

Display Loop Filter Information

The loop filter is used to control and correct the phase of timestamps as processed by the local clock. The loop filter examines timestamps sent to and from the local clock and can adjust them to account for natural wander and jitter.

To view the statistics of the loop filter, enter the **ntploop** command at the system prompt. A screen similar to the following is shown:

```
offset:           0.000000 s
frequency:        0.000 ppm
poll adjust:      0
watchdog timer:   0 s
```

All of these field variables are determined by the NTP algorithm

Field Descriptions

The following section describes the fields displayed using the **ntploop** command.

offset. The currently estimated offset of this remote association, in seconds. This counter indicates the offset of the peer clock relative to the local clock.

frequency. A number indicating the local clock's frequency in relation to a reference clock's Pulse per Second (PPS). If the clock is running in perfect synchronization, this number should be 1. Otherwise, it will be slightly lower or higher in order to compensate for the time discrepancy between the reference clock and the local clock.

poll adjust. The number of times the poll time has been adjusted to conform to the network.

watchdog timer. The number of seconds since the local clock for this client/server was last adjusted.

Display Peer Memory Usage Statistics

The memory usage for the NTP information on the switch can be displayed using the ntpmem command. To view memory information, enter the **ntpmem** command at the system prompt. A screen similar to the following is shown:

```
time since reset:     0
total peer memory:    15
free peer memory:     11
calls to findpeer:    0
new peer allocations: 0
peer demobilizations: 0
hash table counts:    1  0  1  0  0  1  0  0
                      0  0  0  0  0  0  0  0
                      0  0  0  0  0  0  0  0
                      0  0  0  0  0  0  1  0
```

Field Descriptions

The following section describes the fields displayed using the **ntpmem** command.

time since reset. The number of seconds since the last reset of NTP (usually a reboot of the switch).

total peer memory. The total number of NTP associations possible for this switch.

free peer memory. The number of available spots on this switch for NTP associations.

calls to findpeer. The number of times the switch sent an NTP packet of any kind to a configured NTP association.

new peer allocations. The number of new NTP associations created since the last restart.

peer demobilizations. The number NTP associations lost since the last restart.

hash table counts. The number of peer tables hashed to the index.

Display I/O Subsystem Statistics

The **ntpio** command allows you to view general statistics on received and transmitted NTP packets for this switch. To view the I/O statistics, enter the **ntpio** command at the system prompt. A screen similar to the following is displayed:

```
time since reset:          0
receive buffers:           10
free receive buffers:      9
used receive buffers:      0
low water refills:         0
dropped packets:           0
ignored packets:           0
received packets:          18
packets sent:              17
packets not sent:          0
interrupts handled:        18
received by int:           18
```

Field Descriptions

The following section describes the fields displayed using the **ntpio** command.

time since reset. The number of seconds since the last restart of NTP.

receive buffers. The number of switch receive buffers currently allocated by this NTP entity.

free receive buffers. The number of free receive buffers.

used receive buffers. The number of receive buffers being used.

low water refills. The number of times memory has been added.

dropped packets. The number of packets discarded due to lack of resources (i.e., memory).

ignored packets. The number of packets ignored by this client/server.

received packets. The total number of NTP packets received by the switch.

packets sent. The total number of NTP packets sent by the switch.

packets not sent. The number of NTP packets generated but not sent due to restrictions. For information on NTP restrictions, see *Create Restrict Entry/Add Flags to Entry* on page 9-39.

interrupts handled. The number of times NTP information was interrupted in the process of transmitting or receiving.

received by int. The number of packets received by interrupts.

Display Event Timer Subsystem Statistics

The **ntptimer** command allows you to view significant NTP events that have occurred on this switch. To view significant NTP events, enter the **ntptimer** command at the system prompt. A screen similar to the following is displayed:

```
time since reset:       0
alarms handled:         0
alarm overruns:         0
calls to transmit:      0
```

Field Descriptions

The following section describes the fields displayed using the **ntptimer** command.

time since reset. The number of seconds since the last reset of NTP.

alarms handled. The number of NTP alarms generated by this switch. NTP alarms occur when the NTP algorithm determines that an NTP entity is out of synchronization.

alarm overruns. The number of times the NTP alarm routine was backed up.

calls to transmit. The number of requests from other NTP entities for information, either configuration, statistical, or timestamp.

Reset Various Subsystem Statistics Counters

To reset the counters displayed for the commands used in the NTP Statistics Menu (**ntpstat**, **ntploopinfo**, **ntpio**, and **ntptimer**), use the **ntpreset** command. To reset the statistics, enter the **ntpreset** command at the system prompt followed by one or more of the following flags:

- **io**
- **sys**
- **mem**
- **timer**
- **auth**
- **allpeers**

A brief message is displayed confirming the command.

Reset Stat Counters Associated With Particular Peer(s)

It is possible to remotely reset statistics for other NTP associations from the switch. To reset statistics for an NTP association, enter the ntppreset command as follows:

```
ntppreset <address>
```

where **<address>** is the either the domain name or IP address of the remote association. For example, to reset statistics for a peer with IP address 1.1.1.4, enter:

```
ntppreset 1.1.1.4
```

It is possible to reset the statistics for more than one NTP association at a time by adding more than one address to the command. For example, to reset statistics for a peer with IP address 1.1.1.4 and a peer with IP address 1.1.1.5, you would enter:

```
ntppreset 1.1.1.4 1.1.1.5
```

A brief message is displayed confirming the command.

Display Packet Count Statistics from the Control Module

In a comprehensive network-management environment, facilities should exist to perform routine NTP control and monitoring functions. The control module of NTP is responsible for sending and receiving control messages. To display the statistics for the control module, enter the **ntpctlstat** command at the system prompt. A screen similar to the following is shown:

```
time since reset:          0
requests received:         0
responses sent:            0
fragments sent:            0
async messages sent:       0
error msgs sent:           0
total bad pkts:            0
packet too short:          0
response on input:         0
fragment on input:         0
error set on input:        0
bad offset on input:       0
bad version packets:       0
data in pkt too short:     0
unknown op codes:          0
```

Field Descriptions

The following section describes the fields displayed using the **ntpctlstat** command.

time since reset. The number of seconds since the last reset of NTP (usually a switch reboot).

requests received. The number of NTP requests received from any NTP association.

responses sent. The number of NTP messages sent from this switch in response to NTP association requests.

fragments sent. The number of NTP messages sent from this switch that did not contain all appropriate NTP data. This can occur if timestamp information from other NTP entities is judged by this switch to be incorrect.

async messages sent. The number of async trap packets sent.

error msgs sent. The number of error messages sent from the switch to other NTP entities because the switch was not able to respond to the NTP entity's request.

total bad pkts. The total number of packets received that NTP was not able to read.

packet too short. The number of packets received that NTP rejected because the packet was the incorrect length.

response on input. The number of packets received that required the switch to respond to the sender with an NTP message.

fragment on input. The number of packets received that the switch that did not contain complete NTP data.

error set on input. The number of input control packets received with the error bit set.

bad offset on input. The number of NTP timestamps received that the switch disallowed because the added time offset parameter appeared to be incorrect. This can occur if an NTP entity becomes unsynchronized and generates false timestamp information.

bad version packets. The number of packets received where the version number of NTP was undefinable. This is usually caused by packet corruption.

data in pkt too short. The number of packets received that NTP rejected because the packet information was incomplete.

unknown op codes. The number of NTP packets received that contained an unreadable request or information. This is usually caused by packet corruption.

Display the Current Leap Second State

If necessary, NTP adds or subtracts a second from the timestamps sent out on the network to correct for errors in time information. These modifications are called leap seconds. To display leap second information for the switch, enter the **ntpleap** command at the system prompt. A screen similar to the following is displayed:

```
sys.leap:                    11 (clock out of sync)
leap.indicator:              00 (leap controlled by lower stratum)
leap.warning:                00 (leap controlled by lower stratum)
leap.bits:                   00 (no leap second scheduled)
time to next leap interrupt: 1 s
date of next leap interrupt: Tue, Jul 6 1999 12:38:45
calls to leap process:       0
leap more than month away:   0
leap less than month away:   0
leap less than day away:     0
leap in less than 2 hours:   0
leap happened:               0
```

Field Descriptions

The following section describes the fields displayed using the **ntpleap** command.

sys.leap. The current status of the leap second monitor. There are four possible codes:

00	No warning.
01	Last minute has 61 seconds.
10	Last minute has 59 seconds.
11	Alarm condition (clock not synchronized)

leap.indicator. The number of leap seconds that occurred during the current day.

leap.warning. The number of leap seconds that will occur in the current month.

leap.bits. The number of leap bits set within the last hour.

time to next leap interrupt. A leap interrupt occurs when the NTP algorithm examines the topology of the network and determines if a leap second is needed (it may or may not be necessary at the time of the interrupt). This counter displays seconds until the next interrupt.

date of next leap interrupt. The time, in standard date notation, of the next leap interrupt after the most current leap interrupt is finished.

calls to leap process. The number of times a leap second has been added or subtracted.

leap more than month away. A scheduled leap second insertion more than a month away.

leap less than month away. A scheduled leap second insertion less than a month away.

leap less than day away. A scheduled leap second insertion less than a day away.

leap in less than 2 hours. A scheduled leap second insertion less than two hours away.

leap happened. The date of the last leap second insertion.

Turn the Server's Monitoring Facility On or Off

The Server Monitoring Facility keeps track of all NTP association for this switch. When it is On, it is possible to display a list of all NTP associations. For more information on displaying the Monitoring Facility list of NTP associations, see *Display Data The Server's Monitor Routines Have Collected* on page 9-31.

To turn the Monitoring Facility on or off, enter the **ntpmon** command as shown:

```
ntpmon <on:off>
```

where **<on:off>** is the status of the monitoring facility. For example, to turn the facility on, enter:

```
ntpmon on
```

Display Data The Server's Monitor Routines Have Collected

If the NTP monitoring facility is turned on, you can display a list of all known NTP associations with general information using the **ntpmlist** command.

To display a list of collected monitoring statistics, enter the **ntpmlist** command at the system prompt. A screen similar to the following is displayed:

remote address	port	local address	count	m	ver	drop	last	first
127.0.0.1	1025	127.0.0.1	1	7	3	0	0	0

This table is useful in establishing which entity is associated with the switch, and if entities have formed associations independent of administrator configuration (for example, if a user sets up an association with NTP without notifying the network administrator).

Field Descriptions

The following section describes the fields displayed using the **ntpmlist** command.

remote address. The IP address of the remote association.

port. The port the association was learned on and on which the association communicates with the switch.

♦ Note ♦

This is the TCP and UDP definition of a port, not a switch interface port.

local address. The local interface address for this association as created by the NTP configuration on the switch.

count. The number of NTP packets received from this association.

m. The mode the NTP associations uses in relation to the switch.

ver. The version of NTP the association is using (1,2, or 3)

drop. The number of NTP packets received from this association that were dropped (due to restrictions, bad packet data, etc.).

last. The number of seconds since the last NTP message was received from this association.

first. The number of seconds since the first NTP message was received from this association.

NTP Administration Menu

To view the NTP Administration Menu, enter the **ntadmin** command at the system prompt. If you are using verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (**?**) at the prompt to display this menu:

```
Command         NTP Administration Menu
--------------  ------------------------------------------------------------
ntptimeo        set the primary receive time out
ntpdelay        set the delay added to encryption time stamps
ntphost         specify the host whose NTP server we talk to
ntppasswd       specify a password to use for authenticated requests
ntpkeyid        set keyid to use for authenticated requests
ntpkeytype      set key type to use for authenticated requests (des|md5)
ntpdisable      clear a system flag (auth, bclient, monitor, stats)
ntpenable       set a system flag (auth, bclient, monitor, stats)

    Related Menus:
    Ntconfig   Ntinfo   Ntstats   Ntadmin   Ntaccess
```

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Set the Primary Receive Timeout

The **ntptimeo** command allows you to specify the number of milliseconds the server waits for a response to queries before the operation times out. The default is 8000 milliseconds. To change the timeout, enter the ntptimeo command as shown:

```
ntptimeo <value>
```

where **<value>** is the number of milliseconds of the new timeout length. For example, to set the timeout value to 3000 milliseconds, enter the following:

```
ntptimeo 3000
```

To view the current timeout setting with out changing it, enter the **ntptimeo** command with no value. A message similar to the following is shown:

```
primary timeout is 6000 ms
```

Set the Delay Added to Encryption Time Stamps

The **ntpdelay** command specifies a set time interval to add to timestamps included in server requests that require authentication. This can be used to enable server configuration over long delay network paths or between machines whose clocks are not synchronized.

To set the delay time, enter the ntpdelay command as shown:

```
ntpdelay <value>
```

where **<value>** is the number of milliseconds of the new delay time length. For example, to set the delay value to 30 milliseconds, enter the following:

```
ntpdelay 30
```

To view the current delay setting with out changing it, enter the **ntpdelay** command with no value. A message similar to the following is shown:

```
delay 30 ms
```

Specify the Host Whose NTP Server We Talk To

The **ntphost** command specifies the name of the NTP server to which server queries are sent. This can be a domain name or an IP address. The default is localhost (the local server).

To change the NTP server for the switch, enter the **ntphost** command as shown:

```
ntphost <address>
```

where **<address>** is the either the domain name or IP address of the NTP server. For example, to configure the switch to use an NTP server with an IP address of 1.1.1.4, enter:

```
ntphost 1.1.1.4
```

To view the current NTP server used by the switch, enter the **ntphost** command at the prompt with no address. A message similar to the following is shown:

```
current host is 1.1.1.4
```

Specify a Password to Use for Authenticated Requests

The **ntppasswd** command allows you to specify a password that must be entered when making configuration requests. The password must correspond to the key configured for use by the NTP server.

To specify a password:

1. Enter the **ntppasswd** command at the system prompt. A prompt displays asking for the Key ID number for the server, as shown:

   ```
   Keyid:
   ```

   Enter the key ID number for the server (as specified in the key file) and press **<return>**.

2. The following prompt appears requesting a password, as shown:

   ```
   Password:
   ```

   Enter the new password. This password is now required before making a configuration request of the server.

Set Key ID to Use for Authenticated Requests

The **ntpkeyid** command allows you to specify a key number to be used to authenticate configuration requests. This must correspond to the key number the server has been configured to use in the key file.

To set a new key ID, enter the **ntpkeyid** command as shown:

```
ntpkeyid <value>
```

where **<value>** is the new key ID number. For example, to set the key ID to 2, you would enter the following:

```
ntpkeyid 2
```

To view the currently configured key ID, enter the **ntpkeyid** command at the prompt and press **<return>**. A message similar to the following is shown:

```
keyid is 2
```

Set Key Type to Use for Authenticated Requests (DES|MD5)

NTP supports two types of encryption: DES or MD5. If you decide to use encryption to authenticate NTP information and configuration requests, you must specify which type of encryption to use.

To specify an encryption type enter the **ntpkeytype** command as shown:

```
ntpkeytype <value>
```

where **<value>** is either DES or MD5. For example, to set the key type to MD5, you would enter:

```
ntpkeytype MD5
```

To view the currently specified key type, enter the **ntpkeytype** command at the system prompt, and press **<return>**. A message similar to the following is displayed:

```
keytype is MD5
```

Set a System Flag (Auth, Bclient, Monitor, Stats)

The **ntpenable** command provides a way to enable various server options by creating flags added to NTP messages sent to the server.

To set a system flag, enter the **ntpenable** command as shown:

```
ntpenable <flag>
```

where **<flag>** is the type of flag the server will receive. There are six flag types that can be set:

auth	This flag causes the server to synchronize with unconfigured peers only if the peer has been correctly authenticated using a trusted key and key identifier. The default for this flag is disabled (off).
bclient	This flag causes the server to listen for a message from a broadcast or multicast server, following which an association is automatically instantiated for that server. The default for this flag is disabled (off).
monitor	This flag enables the monitoring facility. The default for this flag is disabled (off).
stats	This flag enables the statistics facility file generator. The default for this flag is enable (on).

When you have finished specifying a flag, press **<enter>.** A brief message appears to confirm the operation.

Clear a System Flag (Auth, Bclient, Monitor, Stats)

The **ntpdisable** command allows you to remove previously set flags from NTP messages sent to the server.

To disable a flag, enter the **ntpdisable** command as follows:

```
ntpdisable <flag>
```

where **<flag>** is the type of flag the server will receive. There are six flag types that can be set and removed. The flags are described in the section *Set a System Flag (Auth, Bclient, Monitor, Stats)* on page 9-35.

NTP Access Control Menu

To view the NTP Access Control Menu, enter the **ntaccess** command at the system prompt. If you are using verbose mode the NTP configuration menu is displayed. Otherwise, enter a question mark (**?**) at the prompt to display this menu:

```
Command         NTP Access Control Menu
--------------   ------------------------------------------------------------
ntpreqk         change the request message authentication keyid
ntpctlk         change the control message authentication keyid
ntpckey         add one or more key ID's to the trusted list
ntpvkey         display the trusted key ID list
ntpdkey         remove one or more key ID's from the trusted list
ntpauth         display the state of the authentication code
ntpcres         create restrict entry/add flags to entry
ntpvres         view the server's restrict list
ntpmres         remove flags from a restrict entry
ntpdres         delete a restrict entry
ntpctrap        configure a trap in the server
ntpvtrap        display the traps set in the server
ntpdtrap        remove a trap (configured or otherwise) from the server

   Related Menus:
   Ntconfig   Ntinfo   Ntstats   Ntadmin   Ntaccess
```

The main menu options are shown in the **Related Menus** list for quick access if you need to change menus.

Change the Request Message Authentication Key ID

There are two types of messages an NTP entity can send to another NTP entity: request and control. Request messages ask for information from the NTP entity such as timestamp information, statistics, etc. It is possible to change the authentication key identifier for request messages sent from the switch to another NTP entity.

To change the authentication key ID, enter the **ntpreqk** command as shown:

```
ntpreqk <value>
```

where **<value>** is the new key ID. Press **<return>**, and a brief message is displayed confirming the operation.

♦ Note ♦

The authentication key ID must match in both the switch sending the message and the switch receiving the message.

Change the Control Message Authentication Key ID

There are two types of messages an NTP entity can send to another NTP entity: request and control. Control messages attempt to change the configuration of the NTP entity in some fashion. It is possible to change the authentication key identifier for control messages sent from the switch to another NTP entity.

To change the authentication key ID, enter the **ntpctlk** command as shown:

```
ntpctlk <value>
```

where **<value>** is the new key ID. Press **<return>**, and a brief message is displayed confirming the operation.

♦ Note ♦

The authentication key ID must match in both the switch sending the message, and the switch receiving the message.

Add One or More Key ID's to the Trusted List

The trusted list in the key file is a list of all keys that are considered authentic and uncompromised. Messages from an NTP entity using one of these keys are accepted and acted upon. It is possible to add a key to the trusted list.

To add a key ID to the trust list in the key file, enter the **ntpckey** command as shown:

```
ntpckey <value>
```

where **<value>** is the new key ID to be added to the trusted list. For example, to add key ID 5 to the trusted list, enter the following:

```
ntpckey 5
```

A brief message is displayed confirming the operation.

♦ Note ♦

Adding a key ID using the **ntpckey** command adds the key to the working version of the key file in the switch's RAM. If you reset the switch or re-initialize NTP, the added key is lost.

Display the Trusted Key ID List

The trusted list in the key file is a list of all keys that are considered authentic and uncompromised. Messages from an NTP entity using one of these keys are accepted and acted upon.

To display a list of the trusted keys for this NTP client or server, enter the **ntpvkey** command at the system prompt. A list of the key numbers accepted by this client or server is displayed. For more information on authentication, see *NTP and Authentication* on page 9-4.

Remove One or More Key ID's from the Trusted List

The trusted list in the key file is a list of all keys that are considered authentic and uncompromised. Messages from an NTP entity using one of these keys are accepted and acted upon. It is possible to remove a key from the trusted list.

To remove a key ID from the trusted list, enter the ntpdkey command as shown:

```
ntpdkey <value>
```

where **<value>** is the new key ID to be remove from the trusted list. For example, to remove key ID 5 from the trusted list, enter the following:

```
ntpdkey 5
```

A brief message is displayed confirming the operation.

♦ Note ♦

Removing a key ID using the **ntpdkey** command removes the key from the working version of the key file in the switch's RAM. If you reset the switch or re-initialize NTP, the removed key is reinstated.

Display the State of the Authentication Code

The **ntpauth** command allows you to look at the statistics of the authentication routine. These statistics consist of counters for various functions of the authentication code.

To view the statistics of the authentication code, enter the **ntpauth** command at the system prompt. A screen similar to the following is shown:

```
time since reset:       0
key lookups:            0
keys not found:         0
uncached keys:          0
encryptions:            0
decryptions:            0
```

Field Descriptions

The following sections explains the fields displayed using the **ntpauth** command.

time since reset. The number of seconds since the last restart of the switch.

key lookups. The number of times the switch has examined the key file to find a key.

keys not found. The number of times the switch failed to find a key in its key file.

uncached keys. The number of keys added to the key file using the **ntpckey** command.

encryptions. The number of times the switch sent NTP messages or information out in encrypted form.

decryptions. The number of times the switch received NTP messages of information that was encrypted, and successfully decrypted the information.

Create Restrict Entry/Add Flags to Entry

It is possible to place restriction flags on specific NTP entities in relation to the switch. Restriction flags prevent messages or information coming from the NTP entity from affecting the switch.

To create a restriction flag, enter the **ntpcres** commands as shown:

```
ntpcres <address> <mask> <restriction>
```

where **<address>** is the IP address of the NTP entity, **<mask>** is the entity's subnet mask, and **<restriction>** is the specific flag you want to place on the entity. For example to put an **ignore** restriction on an entity with address 1.1.1.1 and a subnet mask of 255.255.0.0, enter the following:

```
ntpcres 1.1.1.1 255.255.0.0 ignore
```

The following is a list of possible restriction flags that can be used:

ignore	Ignore all packets from hosts which match this entry. If this flag is specified neither queries nor time server polls will be responded to**.**
noquery	Ignore all NTP information queries and configuration requests from the source. Time service is not affected.
nomodify	Ignore all NTP information queries and configuration requests that attempt to modify the state of the server (i.e., run time reconfiguration). Queries which return information are permitted.
notrap	Decline to provide control message trap service to matching hosts. The trap service is a subsystem of the control message protocol which is intended for use by remote event logging programs.
lowpriotrap	Declare traps set by matching hosts to be low priority. The number of traps a server can maintain is limited (the current limit is 3). Traps are usually assigned on a first come, first serve basis, with later trap requestors being denied service. This flag modifies the assignment algorithm by allowing low priority traps to be overridden by later requests for normal priority traps. For more information on setting traps see *Configure a Trap in the Server* on page 9-41
noserve	Ignore NTP packets other than information queries and configuration requests. In effect, time service is denied, though queries may still be permitted.
nopeer	Provide stateless time service to polling hosts, but do not allocate peer memory resources to these hosts even if they otherwise might be considered useful as future synchronization partners.
notrust	Treat these hosts normally in other respects, but never use them as synchronization sources.

limited — These hosts are subject to a limitation of the number of clients from the same net. Net in this context refers to the IP notion of net (class A, class B, class C, etc.). Only the first client limit hosts that have shown up at the server and that have been active during the last client limit period (in seconds) are accepted. Requests from other clients from the same net are rejected. Only time request packets are taken into account. Query packets sent by the ntpq and xntpdc programs are not subject to these limits. A history of clients is kept using the monitoring capability of xntpd. Thus, monitoring is always active as long as there is a restriction entry with the limited flag. For more information on enabling monitoring, see *Turn the Server's Monitoring Facility On or Off* on page 9-31.

ntpport — This is actually a match algorithm modifier, rather than a restriction flag. Its presence causes the restriction entry to be matched only if the source port in the packet is the standard NTP UDP port (123). Both **ntpport** and **non-ntpport** may be specified. The **ntpport** is considered more specific and is sorted later in the list.

View the Server's Restrict List

The **ntpvres** command allows you to view a list of all the configured restrictions for the switch. To view a list of configured restriction, enter the **ntpvres** command at the system prompt. A screen similar to the following appears:

address	mask	count	flags
0.0.0.0	0.0.0.0	12	none
127.0.0.1	255.255.255.255	0	ntpport, ignore

Field Descriptions

The following section describes the fields displayed with the **ntpvres** command.

address. The IP address of the NTP entity for which flags have been configured.

mask. The subnet mask of the NTP entity for which flags have been configured.

count. The number of NTP messages from the NTP entity that have been affected by the configured flags.

flags. The flags configured for this NTP entity. For a description of all possible flags, see *Create Restrict Entry/Add Flags to Entry* on page 9-39.

Remove Flags from a Restrict Entry

It is possible to place restriction flags on specific NTP entities in relation to the switch. Restriction flags prevent messages or information coming from the NTP entity from affecting the switch.

To remove a restriction flag from an NTP entity, enter the **ntpmres** commands as shown:

```
ntpmres <address> <mask> <restriction>
```

where **<address>** is the IP address of the NTP entity, **<mask>** is the entity's subnet mask, and **<restriction>** is the specific flag you want to remove from the entity. For example, to remove an **ignore** restriction from an entity with address 1.1.1.1 and a subnet mask of 255.255.0.0, enter the following:

```
ntpmres 1.1.1.1 255.255.0.0 ignore
```

Delete a Restrict Entry

To remove an entry completely from the restriction list, enter the **ntpdres** command in the following manner:

```
ntpdres <address> <mask>
```

where **<address>** is the IP address of the NTP entity, and **<mask>** is the entity's subnet mask. For example to remove an entity with address 1.1.1.1 and a subnet mask of 255.255.0.0, enter the following:

```
ntpdres 1.1.1.1 255.255.0.0
```

This entity will no longer be listed in the restriction list and has no restriction flags placed on messages it sends to the switch.

Configure a Trap in the Server

The **ntpctrap** command allows you to set a trap receiver for the given address and port number. The trap receiver will log event messages and other information for the server in a log file.

To create a trap receiver, enter the **ntpctrap** command in the following manner:

```
ntpctrap <address> [<port>] [<interface>]
```

where address is the IP address of the switch. There are two optional items you can specify:

port — The port on the switch used for sending NTP messages. If no port is specified, a default port of 18447 is used.

♦ Note ♦

This is the TCP and UDP definition of a port, not a switch interface port.

interface — The local interface address for this NTP entity. If no interface is specified, the interface for the local NTP entity is used. For more information on interface addresses, see *Display Peer Summary Information* on page 9-16.

Display the Traps Set in the Server

The **ntpvtrap** command allows you to view a list of trap receivers set for the server. To view the trap list, enter the **ntpvtrap** command at the system prompt. A display similar to the following is shown:

```
address 127.0.0.1, port 18447
interface: 0.0.0.5, configured
set for 0 seconds, last set 0 seconds ago
sequence 1, number of resets 1
```

Field Descriptions

The following section describes the fields shown with the **ntpvtrap** command.

address. The address of the server where the trap was set.

port. The port on which the server is listening for NTP messages.

♦ Note ♦

This is the TCP and UDP definition of a port, not a switch interface port.

interface. The local interface address of the NTP server.

set for n seconds. The time the trap was initially set.

last set. The time in seconds from when the last trap was set for this server.

sequence. The number of times the trap was set.

number of resets. The number of times the trap has been reset.

Remove a Trap (Configured or Otherwise) from the Server

The **ntpdtrap** command allows you to remove a trap receiver for the given address. The trap receiver will log event messages an other information for the server in a log file.

To delete a trap receiver, enter the **ntpdtrap** command in the following manner:

```
ntpctrap <address> [<port>] [<interface>]
```

where address is the IP address of the switch. There are two optional items you can specify:

port The port on the switch used for sending NTP messages.

♦ Note ♦

This is the TCP/IP and UDP definition of a port, not a switch interface port.

interface The local interface address for this NTP entity. For more information on interface addresses, see *Display Peer Summary Information* on page 9-16.