Chapter 27

Network Time Protocol (NTP)

Introduction

This chapter describes the Network Time Protocol (NTP) service provided by the router, and how to configure and monitor NTP on the router.

The Network Time Protocol (NTP) is a protocol for synchronising the time clocks on a collection of network devices using a distributed client/server mechanism. NTP uses UDP (User Datagram Protocol) as the transport mechanism. NTP evolved from the Time Protocol (RFC 868) and the ICMP Timestamp message (RFC 792).

NTP provides protocol mechanisms to specify the precision and estimated error of the local clock and the characteristics of the reference clock to which it may be synchronized.

Overview of the Network Time Protocol

NTP uses a subnetwork with primary reference clocks, gateways, secondary reference clocks, and local hosts. These are organised into a hierarchy with the more accurate clocks near the top and less accurate ones near the bottom (Figure 27-1 on page 27-3).

A number of primary reference clocks, synchronised to national standards, are connected to widely accessible resources (such as backbone gateways or routers) operating as primary time servers. The primary time servers use NTP between them to crosscheck clocks, to mitigate errors due to equipment or propagation failures, and to distribute time information to local secondary time servers. The secondary time servers redistribute the time information to the remaining local hosts.

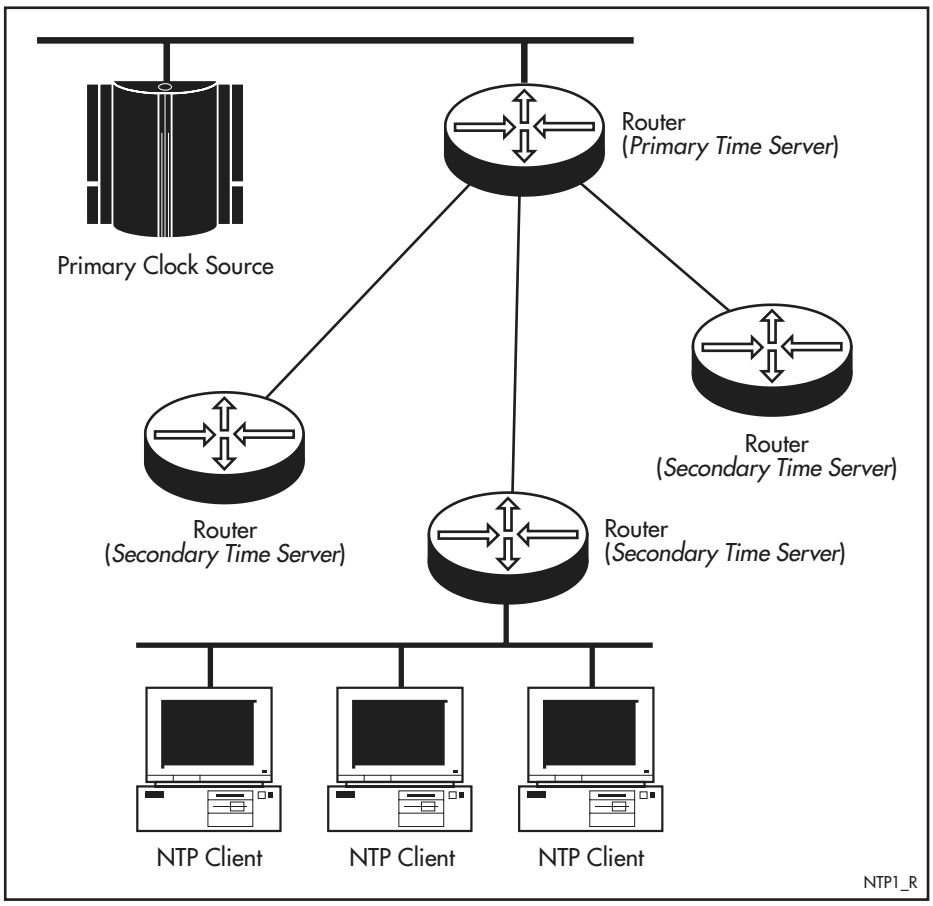
The hierarchical organisation and distribution of time information reduces the protocol overhead, and allows selected hosts to be equipped with cheaper but less accurate clocks. NTP provides information organizes this hierarchy on the basis of precision or estimated error.

An NTP entity may be in one of the following operating modes; however, the router's implementation of NTP supports two modes: client and server.

- An NTP entity operating in a *client* mode sends periodic messages to its peers, requesting synchronisation by its peers.
- An NTP entity enters the s*erver* mode temporarily when it receives a client request message from one of its peers, and remains in server mode until the reply to the request has been transmitted.
- An NTP entity operating in *symmetric active* mode sends messages announcing its willingness to synchronise and be synchronised by its peers.
- An NTP entity enters *symmetric passive* mode in response to a message from a peer operating in Symmetric Active mode. An NTP entity operating in this mode announces its willingness to synchronise and be synchronised by its peers.
- An NTP entity operating in *broadcast* mode periodically sends messages announcing its willingness to synchronise all of its peers but not to be synchronised by any of them.

NTP messages are generally sent regardless of the reachability state or stratum (rank) of the peers.

Figure 27-1: Network Model for the Network Time Protocol



The same message format is used for both requests and replies. When a request is received, the server interchanges addresses and ports, fills in or overwrites certain fields in the message, recalculates the checksum, and returns it immediately. The information included in the NTP message allows each client/server peer to determine the timekeeping characteristics of its peers, including the expected accuracies of their clocks. Each peer uses this information and selects the best time from possibly several other clocks, updates the local clock, and estimates its accuracy.

There is no provision in NTP for peer discovery, acquisition, or authentication. Data integrity is provided by the IP and UDP checksums. No reachability, circuit-management, duplicate-detection, or retransmission facilities are provided or necessary.

By its very nature clock synchronization requires long periods of time (hours or days) and multiple comparisons in order to maintain accurate timekeeping. The more comparisons performed, the greater the accuracy of the timekeeping.

NTP on the Router

Our router implementation of NTP is based on RFC 958, "*Network Time Protocol (NTP)*", RFC 1305, "*Network Time Protocol (Version 3), Specification, Implementation and Analysis*", and RFC 1510, "*The Kerberos Network Authentication Service (V5)*".

Two modes of operation are supported: client and server. The router is in client mode most of the time where it polls the configured peer at least once every preconfigured minimum poll time period.

The preconfigured minimum time period is approximately one minute. In an ISDN network this may cause ISDN calls to be activated every minute, resulting in high ISDN call charges.

The peer that the router refers to must be a more accurate clock source than the router itself or another router directly connected to a more accurate clock source. The router operates as a secondary time server. It cannot operate as a primary time server unless the primary clock source is operating in server mode. A primary clock source usually operates in broadcast mode, which is not supported by the router's implementation of NTP. There is no support for clock selection or filtering. When the router receives a valid reply from the peer, it synchronises its own internal clock according to the information from the reply.

If the router receives a synchronisation request from an NTP client, it temporarily switches to server mode. It replies to the request with the current time from the router's internal clock along with other information useful for synchronisation. The router's internal clock is accurate to ±0.005 seconds.

Configuration Example

NTP requires the IP module to be enabled and configured correctly. See Chapter 14, Internet Protocol (IP) for detailed descriptions of the commands required to enable and configure IP.

The router's implementation of NTP supports two modes: client and server mode. When a synchronisation request is received from a client (e.g. a PC on a LAN), the router enters server mode and responds with time information derived from the router's own internal clock. Periodically the router enters client mode, sending synchronisation requests to a predefined peer to synchronise its own internal clock. The peer is assumed to be a primary clock source or another router connected directly to a primary clock source.

This example illustrates how to configure two routers, one at a Head Office and one at a Regional Office, to provide a network time service (Figure 27-2 on page 27-5, Table 27-1 on page 27-5). The Head Office router is connected to a primary time server and provides the most accurate time information. The router at the Regional Office uses the Head Office router as its peer to avoid the cost of an additional WAN connection but provides slightly less accurate time information.

To configure NTP on the router, the NTP module must be enabled and an NTP peer must be defined. The offset of local time from UTC time must also be set.

Figure 27-2: Example network configuration for a network time service

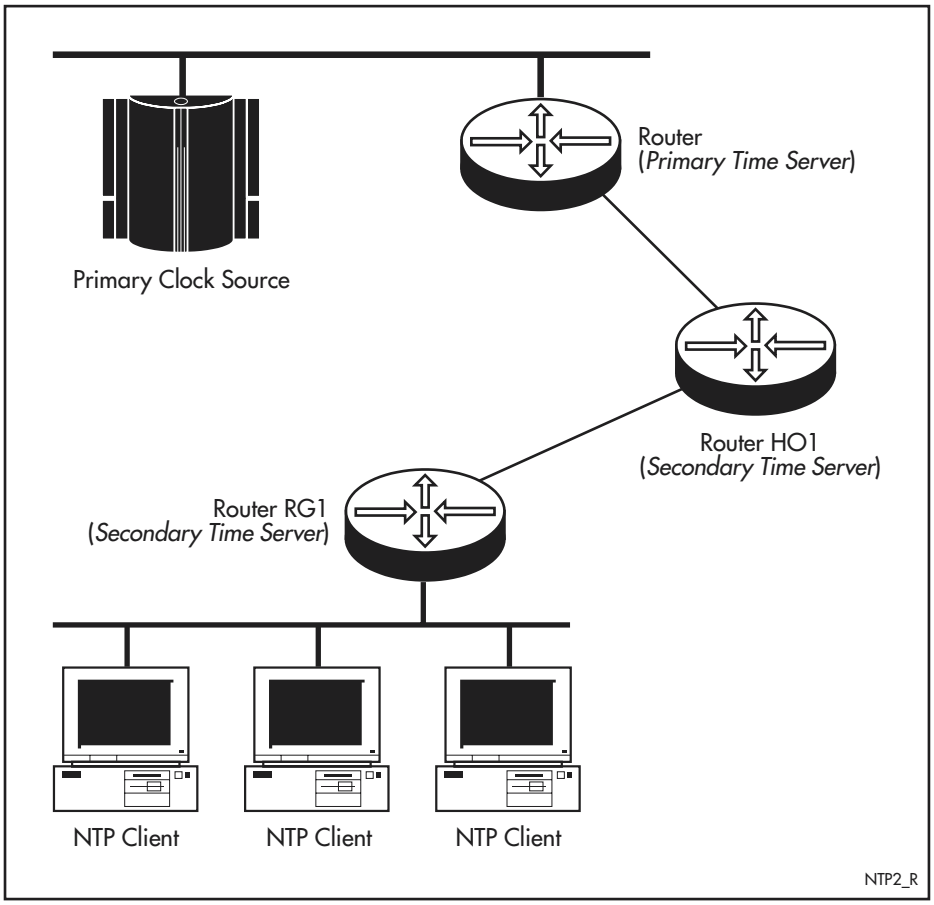
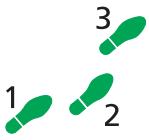


Table 27-1: Example configuration parameters for a network time service

Site	Regional Office	Head Office
Router Name	RG1	HO1
IP Address of Router	192.168.35.114	192.168.35.113
IP Address of Peer	192.168.35.113	192.168.13.3



To configure NTP

1. Enable NTP and define the NTP peer.

The NTP module must be enabled on all routers that are to provide a network time service. Each router must have a peer defined where the router synchronises its own internal clock. Enable NTP on the Head Office router and specify a primary time server as the peer by using the commands:

```
enable ntp
add ntp peer=192.168.13.3
```

Enable NTP on the Regional Office router and specify the Head Office router as the peer by using the commands:

```
enable ntp
add ntp peer=192.168.35.113
```

2. **Configure the NTP parameters.**

   On each router, the offset of local time from UTC time must be specified. In this example, both routers are in the same time zone, which is 13 hours ahead of UTC time. Use the following commands on both routers:

   ```
   set ntp utcoffset=+13:00:00
   reset ntp
   ```

3. **Check the NTP configuration.**

   Check the NTP configuration on each router by using the command:

   ```
   show ntp
   ```

   This produces a display (on the Head Office router) like Figure 27-3 on page 27-6.

Figure 27-3: Example output from the **show ntp** commands for the Head Office router in an example network time service

```
NTP Module Configurations
-------------------------
Status          : ENABLED
Host Address    : 192.168.35.113
UTC offset      : +13:00:00
Last Updated    : 15:21:37 on 14-Feb-95
Last Delta      : +00.28

Configured Peer
---------------
192.168.13.3

Counters
---------
Packets Sent           : 0000000011
Packets Received       : 0000000010
Packets w/ head error  : 0000000000
Packets w/ data error  : 0000000006
```

Command Reference

This section describes the commands available on the router to configure and manage the Network Time Protocol (NTP) on the router.

NTP requires the IP module to be enabled and configured correctly. See Chapter 14, Internet Protocol (IP) for detailed descriptions of the commands required to enable and configure IP.

The shortest valid command is denoted by capital letters in the Syntax section. See "Conventions" on page xcv of Preface in the front of this manual for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of messages and their meanings.

add ntp peer

Syntax `ADD NTP PEer=`*`ipadd`*

where *ipadd* is the IP address of the NTP peer, in dotted decimal notation

Description This command specifies the NTP peer for this router. Only one peer may be defined and must not already be defined.

Examples To add the router with IP address 172.16.8.1 as a peer, use the command:

```
add ntp pe=172.16.8.1
```

Related Commands **delete ntp peer**

delete ntp peer

Syntax `DELete NTP PEer=`*`ipadd`*

where *ipadd* is the IP address of the NTP peer, in dotted decimal notation

Description This command deletes the specified NTP peer for this router. The peer must already be defined.

Examples To remove the router with IP address 172.16.8.1 as a peer, use the command:

```
del ntp pe=172.16.8.1
```

Related Commands **add ntp peer**

disable ntp

Syntax `DISable NTP`

Description This command disables the NTP module. The NTP module must not already be disabled.

Examples To disable the NTP module, use the command:

```
dis ntp
```

Related Commands **enable ntp**
purge ntp
reset ntp

enable ntp

Syntax `ENAble NTP`

Description This command enables the NTP module. The NTP module must not already be enabled.

Examples To enable the NTP module, use the command:

```
ena ntp
```

Related Commands **disable ntp**
purge ntp
reset ntp

purge ntp

Syntax `PURge NTP`

Description This command purges all NTP configurations and returns the NTP module to its initialised state.

Examples To purge the current configuration of the NTP module, use the command:

```
pur ntp
```

Related Commands **disable ntp**
enable ntp
reset ntp

reset ntp

Syntax `RESET NTP`

Description This command resets the NTP module. All dynamic configuration information is cleared and then reloaded from non-volatile storage, and requests are transmitted.

Examples To restart the NTP module, use the command:

```
reset ntp
```

Related Commands **disable ntp**
enable ntp
purge ntp

set ntp utcoffset

Syntax `SET NTP UTCoffset=-24:00:00..+24:00:00`

Description This command sets the offset of local time from UTC time. All time information managed by NTP is in UTC time.

NTP and the Logging Facility share a common (system-wide) UTC offset. Changing the UTC offset by using the **set ntp utcoff** command also changes the value of the UTC offset used by the Logging Facility.

Examples To set the UTC offset to +4:00 hours, use the command:

```
set ntp utc=4:00
```

Related Commands **show ntp**

show ntp

Syntax `SHow NTP`

Description This command displays configuration information for the NTP module (Figure 27-4, Table 27-2 on page 27-10).

Figure 27-4: Example output from the **show ntp** command

```
NTP Module Configurations
-------------------------
Status          : ENABLED
Host Address    : 192.168.35.149
UTC offset      : +13:00:00
Last Updated    : 15:21:37 on 14-Feb-1995
Last Delta      : +00.28

Configured Peer
---------------
192.168.46.33

Counters
---------
Packets Sent           : 0000000011
Packets Received       : 0000000010
Packets w/ head error  : 0000000000
Packets w/ data error  : 0000000006
```

Table 27-2: Parameters in the output of the **show ntp** command

Parameter	Meaning
Status	Whether the NTP module is enabled.
Host Address	IP address of this NTP module.
UTC offset	Offset of local time from UTC time.
Last Updated	Time and date that NTP last updated the router's clock.
Last Delta	Change in the router's clock at the last update.
Configured Peer	IP address of the NTP peer.
Packets Sent	Number of NTP protocol packets this router has transmitted.
Packets Received	Number of NTP protocol packets this router has received.
Packets w/ head error	Number of NTP protocol packets with errors in the header that this router received.
Packets w/ data error	Number of NTP protocol packets with errors in the data portion that this router received.

Examples To display the current NTP configuration, use the command:

```
sh ntp
```

Related Commands **add ntp peer**
set ntp utcoffset