Administering the Router

This chapter describes how to perform one-time operations to administer the Cisco 910 Industrial Routers (*hereafter* referred to as the router). This chapter consists of these sections:

Managing the System Time and Date

You can manage the system time and date on your router using automatic configuration, such as the Network Time Protocol (NTP), or manual configuration methods.

These sections contain the following configuration information:

Understanding the System Clock

The heart of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- NTP
- Manual configuration

The system clock can provide time to these services:

- User **show** commands
- Logging and debugging messages

The system clock keeps track of time internally based on Universal Time Coordinated (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone so that the time appears correctly for the local time zone.

For configuration information, see the "Configuring Time and Date Manually" section on page -4.

Understanding Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Cisco's implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

If the network is isolated from the Internet, Cisco's implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

NTP Version 4

NTP version 4 is implemented on the router. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.
- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

Configuring NTP

These sections contain this configuration information:

Configuring NTP Server

This section describes how to configure the router to be synchronized by a time server.

Beginning in privileged EXEC mode, follow these steps to configure the NTP server:

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**ntp server** {[**ip** | **ipv6** | **address**] *hostname*} [**prefer**] [**key** *keyid*] [**maxpoll** number] [**minpoll** number] [**burst**] [**iburst**]	Defines the NTP server that provides the clocking source for the router. You can specify multiple server associations. ■ **key**– Configures a key to use while communicating with the NTP server. The range for the key-id argument is from 1 to 65534. **Note:** Only configure the key when you want the NTP server to provide authentication for the router. **maxpoll, minpoll**–Configures the maximum and minimum intervals in which to poll a server. The range for the max-poll and min-poll arguments is from 4 to 17 seconds, and the default values are 6 and 4, respectively. **prefer** -Assigns the NTP server as the preferred NTP server for the router. **Note:** When you configure a key for use in communicating with the NTP server, be sure that the key exists as a trusted key on the router. For more information on trusted keys, see the "Configuring NTP Authentication" section on page -3.
3.	**exit**	Return to privileged EXEC mode.
4.	**show ntp status**	(Optional) Show NTP status to verify the configuration.
5.	**show ntp associations**	(Optional) Show the NTP associations with upstream servers.
6.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the NTP service, use the **no ntp server** *hostname* global configuration command.

Configuring NTP Authentication

You can configure the router to authenticate the time sources to which the local clock synchronizes. When you enable NTP authentication, the router synchronizes to a time source only if the source carries one of the authentication keys specified by the ntp trusted-key command. The router drops any packets that fail the authentication check and prevents them from updating the local clock.

By default, NTP authentication is disabled on the router.

This section describes how to configure NTP server(s) with the authentication keys configured on the router.

Beginning in privileged EXEC mode, follow these steps to configure NTP authentication:

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**ntp authentication-key** *number* **md5** *key*	Defines the authentication key. This key must match the value on the NTP server along with the **ntp trusted-key** *number* value of the router in 3. below. The router does not synchronize to the NTP server clocking source unless the **ntp authentication-key** and the **ntp trusted-key** values on the server and the router match. The range for authentication keys is from 1 to 65534. For the MD5 string, you can enter up to 16 alphanumeric characters.
3.	**ntp trusted-key** *number*	Specifies one or more keys (defined in 2.) that a time source (NTP server) must provide in its NTP packets in order for the router to synchronize to it. The range for trusted keys is from 1 to 65534. This command provides protection against accidentally synchronizing the router to a time source (NTP server) that is not trusted.
4.	**exit**	Return to privileged EXEC mode.
5.	**show ntp status**	(Optional) Show NTP status to verify the configuration.
6.	**show ntp associations**	(Optional) Show the NTP associations with upstream servers.
7.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the authentication key for NTP, use the **no ntp authentication-key** *number* global configuration command.

To disable the authentication of the identity of the system, use the **ntp trusted-key** *number* global configuration command.

Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the router can synchronize, you do not need to manually set the system clock.

These sections contain this configuration information:

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Beginning in privileged EXEC mode, follow these steps to set the system clock:

	Command	Purpose
1.	**clock set** *hh*:*mm*:*ss month day year*	Manually set the system clock using one of these formats. ■ For *hh*:*mm*:*ss*, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. ■ For *day*, specify the day by date in the month. ■ For *month*, specify the month by name. ■ For *year*, specify the year (no abbreviation).

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001:

```
Router# clock set 13:32:00 July 23 2001
```

Displaying the Time and Date Configuration

To display the time and date configuration, use the **show clock** privileged EXEC command.

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- *—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

Configuring the Time Zone

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**clock timezone** *zone*	Set the time zone. The router keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set. ■ For *zone*, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC.
3.	**exit**	Return to privileged EXEC mode.
4.	**show running-config**	Verify your entries.
5.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To set the time to UTC, use the **no clock timezone** global configuration command.

Configuring a System Name and Prompt

You configure the system name on the router to identify it. By default, the system name and prompt are *Router*.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [>] is appexited. The prompt is updated whenever the system name changes.

These sections contain the following configuration information:

- Default System Name and Prompt Configuration, page 6
- Configuring a System Name, page 7
- Understanding DNS, page 7

Default System Name and Prompt Configuration

The default router system name and prompt is *Router*.

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**hostname** *name*	Manually configure a system name. The default setting is *router*. The name must follow the rules for ARPANET hostnames. They must start with a letter, exit with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.
3.	**exit**	Return to privileged EXEC mode.
4.	**show running-config**	Verify your entries.
5.	**copy running-config startup-confi**g	(Optional) Save your entries in the configuration file.

When you set the system name, it is also used as the system prompt.

To return to the default hostname, use the **no hostname** global configuration command.

Understanding DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your router, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, for example, the File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

These sections contain this configuration information:

- Default DNS Configuration, page 8
- Setting Up DNS, page 8
- Displaying the DNS Configuration, page 9

Default DNS Configuration

Table 1 shows the default DNS configuration.

Table 1 Default DNS Configuration

Feature	Default Setting
DNS enable state	Enabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up your router to use the DNS:

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**ip domain name** *name*	Define a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot-up time, no domain name is configured; however, if the router configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).
3.	**ip name-server** *dnsserver-address*	Defines up to three name servers. The address can be either an IPv4 address or an IPv6 address.
4.	**ip domain list** [*domain_name*]	(Optional) Define a list of default domain names to complete unqualified names.
5.	**ip domain lookup**	(Optional) Enable DNS-based hostname-to-address translation on your router. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
6.	**exit**	Return to privileged EXEC mode.
7.	**show running-config**	Verify your entries.
8.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

If you use the router IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appexited to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the hostname, the software looks up the IP address without appending any default domain name to the hostname.

To remove a domain name, use the **no ip domain name** *name* global configuration command. To remove a name server address, use the **no ip name-server** *server-address* global configuration command. To delete a name from a list, use the **no ip domain list** [*domain_name*] global configuration command. To disable DNS on the router, use the **no ip domain-lookup** global configuration command.

Displaying the DNS Configuration

To display the DNS configuration information, use the **show running-config** privileged EXEC command.

Managing the MAC Address Table

The MAC address table contains address information that the router uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address: a source MAC address that the router learns and then ages when it is not in use.
- Static address: a manually entered unicast address that does not age and that is not lost when the router resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

For complete syntax and usage information for the commands used in this section, see the command reference for this release.

These sections contain this configuration information:

- Building the Address Table, page 9
- Default MAC Address Table Configuration, page 9
- Changing the Address Aging Time, page 10
- Displaying Address Table Entries, page 10

Building the Address Table

With multiple MAC addresses supported on all ports, you can connect any port on the router to individual workstations, repeaters, routers, or other network devices. The router provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As stations are added or removed from the network, the router updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the router maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The router sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the router forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The router always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

Default MAC Address Table Configuration

Table 2 shows the default MAC address table configuration.

Table 2 Default MAC Address Table Configuration

Feature	Default Setting
Aging time	300 seconds
Dynamic addresses	Automatically learned
Static addresses	None configured

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the router learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the router receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned. Flooding results, which can impact router performance.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time:

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**mac address-table aging-time** [**0** | *10-1000000*]	Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table.
3.	**exit**	Return to privileged EXEC mode.
4.	**show mac address-table aging-time**	Verify your entries.
5.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Displaying Address Table Entries

You can display the MAC address table by using one or more of the privileged EXEC commands described in Table 3:

Table 3 Commands for Displaying the MAC Address Table

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.