CHAPTER 28

Router Properties

Router properties let you define the overall attributes of the router, such as the router name, domain name, password, Simple Network Management Protocol (SNMP) status, Domain Name System (DNS) server address, user accounts, router log attributes, virtual type terminal (vty) settings, SSH settings, and other router access security settings.

Device Properties

The Properties—Device screen contains host, domain, and password information for your router.

Device Tab

The Device tab contains the following fields.

Host

Enter the name you want to give the router in this field.

Domain

Enter the domain name for your organization. If you do not know the domain name, obtain it from your network administrator.

Enter the Text for Banner

Enter text for the router banner. The router text banner is displayed whenever anyone logs in to the router. We recommend that the text banner include a message indicating that unauthorized access is prohibited.

Password Tab

The Password tab contains the following fields.

Enable Secret Password

Cisco Router and Security Device Manager (Cisco SDM) supports the enable secret password. The enable secret password allows you to control who is able to enter configuration commands on this router. We strongly recommend that you set an enable secret password. The password will not be readable in the Cisco SDM Device Properties window, and it will appear in encrypted form in the router configuration file. Therefore, you should record this password in case you forget it.

The Cisco IOS release that the router is running may also support the enable password. The enable password functions like the enable secret password, but was encrypted in the configuration file. If an enable password is configured using the command-line interface (CLI), it is ignored if an enable secret password is configured.

Current Password

If a password has already been set, this area contains asterisks (*).

Enter New Password

Enter the new enable password in this field.

Reenter New Password

Reenter the password exactly as you entered it in the New Password field.

Date and Time: Clock Properties

Use this window to view and edit the date and time settings on the router.

Date/Time

You can see the router date and time settings on the right side of the Cisco SDM status bar. The time and date settings in this part of the Clock Properties window are not updated.

Router Time Source

This field can contain the following values:

- NTP – The router receives time information from an NTP server.
- User Configuration – The time and date values are set manually, using Cisco SDM or the CLI.
- No time source – The router is not configured with time or date settings.

Change Settings

Click to change the date and time settings on the router.

Date and Time Properties

Use this window to set the router date and time. You can have Cisco SDM synchronize the settings with the PC, or you can set them manually.

Synchronize with my local PC clock

Check to set up Cisco SDM to synchronize router date and time settings with the date and time settings on the PC.

Synchronize

Click to have Cisco SDM synchronize time settings. Cisco SDM adjusts date and time settings in this way only when you click **Synchronize**. Cisco SDM does not automatically resynchronize them with the PC during subsequent sessions. This button is disabled if you have not checked **Synchronize with my local PC clock**.

Note You must make the Time Zone and Daylight Savings settings on the PC before starting Cisco SDM so that Cisco SDM will receive the correct settings when you click **Synchronize**.

Edit Date and Time

Use this area to set the date and time manually. You can choose the month and the year from the drop-down lists, and choose the day of the month in the calendar. The fields in the Time area require values in 24-hour format. You can choose your time zone based on Greenwich mean time (GMT), or you can browse the list for major cities in your time zone.

If you want the router to adjust time settings for daylight saving time and standard time, check **Automatically adjust clock for daylight savings changes**.

Apply

Click to apply the date and time settings you have made in the Date, Time, and Time Zone fields.

NTP

Network Time Protocol (NTP) allows routers on your network to synchronize their time settings with an NTP server. A group of NTP clients that obtains time and date information from a single source will have more consistent time settings. This window allows you to view the NTP server information that has been configured, add new information, or edit or delete existing information.

Note If your router does not support NTP commands, this branch will not appear in the Router Properties tree.

IP Address

The IP address of an NTP server.

If your organization does not have an NTP server, you may want to use a publicly available server, such as the server described at the following URL:

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

Interface

The interface over which the router will communicate with the NTP server.

Prefer

This column contains **Yes** if this NTP server has been designated as a preferred NTP server. Preferred NTP servers will be contacted before nonpreferred servers. There can be more than one preferred NTP server.

Add

Click to add NTP server information.

Edit

Click to edit a specified NTP server configuration.

Delete

Click to delete a specified NTP server configuration.

Add or Edit NTP Server Details

Add or edit NTP server information in this window.

IP Address

Enter or edit the IP address of an NTP server.

Prefer

Click this box if this is to be the preferred NTP server.

Interface

Choose the router interface that will provide access to the NTP server. You can use the **show IP routes** CLI command to determine which interface has a route to this NTP server.

Note An extended access rule will be created for port 123 traffic and applied to the interface that you choose in this window. If an access rule is already in place for this interface, Cisco SDM will add statements to permit port 123 traffic on this interface. If the existing rule is a standard access rule, Cisco SDM changes it to an extended rule in order to be able to specify traffic type and destination.

Authentication Key

Check this box if the NTP server uses an authentication key, and enter the information required in the fields. The information in these fields must match the key information on the NTP server.

Key Number

Enter the number for the authentication key. The key number range is 0 to 4294967295.

Key Value

Enter the key used by the NTP server. The key value can use any of the letters A to Z, uppercase or lowercase, and can be no more than 32 characters.

Confirm Key Value

Reenter the key value to confirm accuracy.

SNTP

This window is displayed on Cisco 830 routers. The Simple Network Time Protocol (SNTP) is a less complex version of Network Time Protocol (NTP). NTP allows routers on your network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single

source will have more consistent time settings. This window allows you to view the NTP server information that has been configured, to add new information, or to edit or delete existing information.

Note If your router does not support NTP commands, this branch will not appear in the Router Properties tree.

Property

The system-defined name for this NTP server.

Value

The IP address for this NTP server.

Add

Click to add NTP server information.

Edit

Click to edit a specified NTP server configuration.

Delete

Click to delete a specified NTP server configuration.

Add an NTP Server

Enter the IP address of an NTP server in this window.

Note An extended access rule will be created for port 123 traffic and applied to the interface that you choose in this window. If an access rule was already in place for this interface, Cisco SDM will add statements to permit port 123 traffic on this interface. If the existing rule was a standard access rule, Cisco SDM changes it to an extended rule in order to be able to specify traffic type and destination.

IP Address

Enter the IP address of the NTP server in dotted-decimal format. For more information, see IP Addresses and Subnet Masks.

Logging

Use this window to enable logging of system messages, and to specify logging hosts where logs can be kept. You can specify the level of logging messages that you want to send and to collect, and enter the hostname or IP address of multiple logging hosts.

IP Address/Hostname

Click **Add**, and enter the IP address or hostname of a network host to which you want the router to send logging messages for storage. The **Edit** and **Delete** buttons enable you to modify information that you entered and to delete entries.

Specify the types of messages that are sent to logging hosts by choosing the logging level from the **Logging Level** drop-down list. See Logging Level for more information.

Logging Level

The following logging levels are available in **Logging Level** drop-down lists:

- emergencies (0)
- alerts (1)
- critical (2)
- errors (3)
- warnings (4)
- notifications (5)
- informational (6)
- debugging (7)

The log collects all messages of the level you choose plus all messages of lower levels, or the router sends all messages of the level you choose plus all messages of lower levels to the logging hosts. For example, if you choose notifications (5),

the log collects or sends messages of levels 0 through 5. Firewall logging messages require a logging level of debugging(7), and Application Security logging messages require a level of informational(6).

Logging to Buffer

If you want system messages to be logged to the router buffer, check the **Logging Buffer** check box in the dialog that Cisco SDM displays when you click **Edit**, then enter the buffer size in the Buffer Size field. The larger the buffer, the more entries can be stored before the oldest ones are deleted to make room for new entries. However, you should balance logging needs against router performance.

Specify the types of messages that are collected in the log by choosing the logging level from the **Logging Level** drop-down list. See Logging Level for more information.

SNMP

This window lets you enable SNMP, set SNMP community strings, and enter SNMP trap manager information.

Enable SNMP

Check this check box to enable SNMP support. Uncheck to disable SNMP support. SNMP is enabled by default.

Community String

SNMP community strings are embedded passwords to Management Information Bases (MIBs). MIBs store data about router operation and are meant to be available to authenticated remote users. The two types of community strings are “public” community strings, which provide read-only access to all objects in the MIB except community strings, and “private” community strings, which provide read-and-write access to all objects in the MIB except community strings.

The community string table lists all of the configured community strings and their types. Use the **Add** button to display the Add a Community String dialog box and create new community strings. Click the **Edit** or **Delete** buttons to edit or delete the community string you chose in the table.

Trap Receiver

Enter the IP addresses and community strings of the trap receivers—that is, the addresses where the trap information should be sent. These are normally the IP addresses of the SNMP management stations monitoring your domain. Check with your site administrator to determine the address if you are unsure of it.

Click the **Add**, **Edit**, or **Delete** buttons to administer trap receiver information.

SNMP Server Location

Text field you can use to enter the SNMP server location. It is not a configuration parameter that will affect the operation of the router.

SNMP Server Contact

Text field you can use to enter contact information for a person managing the SNMP server. It is not a configuration parameter that will affect the operation of the router.

Netflow

This window shows how your router is configured to monitor Netflow top talkers on interfaces that have Netflow configured. For more information on the items shown, see Netflow Talkers.

You can monitor Netflow parameters on your router and view top-talker statistics in **Monitor > Inteface Status** and **Monitor > Traffic Status > Top N Traffic Flows**. If you do *not* enable Netflow top talkers, then the top ten talkers are monitored.

Netflow Talkers

In this window you can Netflow top talkers.

Enable Top Talkers

Check the **Enable Top Talkers** check box to enable monitoring of the top talkers on the interfaces that have Netflow configured.

Top Talkers

Set the number of top talkers in the **Top Talkers** number box. Choose a number in the range 1–200. Cisco SDM will track and record data on up to the number of top talkers that you set.

Cache Timeout

Set the timeout, in milliseconds, for the top-talkers cache in the **Cache timeout** number box. Choose a number in the range 1–3600000. The top-talkers cache will refresh when the timeout is reached.

Sort By

Choose how to sort the top talkers by choosing bytes or packets from the **Sort by** drop-down list.

Router Access

This window explains which features are included in router access.

User Accounts: Configure User Accounts for Router Access

This window allows you to define accounts and passwords that will enable users to authenticate themselves when logging in to the router using HTTP, Telnet, PPP, or some other means.

Username

User account name.

Password

User account password, displayed as asterisks (*).

Note The user password is not the same as the enable secret password configured in the Device Properties—Password tab. The user password enables the specified user to log in to the router and enter a limited set of commands.

Privilege Level

Privilege level for the user.

View Name

If a CLI view has been associated with the user account, the view name appears in this column. Views define the user's access to Cisco SDM based on the user's role. Click Associate a View with the user for more information.

Note If Cisco SDM is launched with a user-defined view, or with an altered Cisco SDM-defined view, Cisco SDM operates in Monitor mode, and the user has read-only privileges. The Cisco SDM features available to be monitored depend on the commands present in the view. Not all features may be available for monitoring by the user.

What Do You Want To Do?

To:	Do This:
Add a new user account.	Click **Add**. Then add the account in the Add a Username window.
Edit a user account.	Choose the user account and click **Edit**. Then edit the account in the Edit a Username window.
Delete a user account.	Choose the user account and click **Delete**. Then, confirm the deletion in the displayed warning box.

Add or Edit a Username

Add or edit a user account in the fields provided in this window.

Username

Enter or edit the username in this field.

Password

Enter or edit the password in this field.

Confirm Password

Reenter the password in this field. If the password and the confirm password do not match, an error message window appears when you click **OK**.

When you click **OK**, the new or edited account information appears in the Configure User Accounts for Telnet window.

Encrypt password using MD5 hash algorithm Check Box

Check if you want the password to be encrypted using the one-way Message Digest 5 (MD5) algorithm, which provides strong encryption protection.

Note Protocols that require the retrieval of clear text passwords, such as CHAP, cannot be used with MD5-encrypted passwords. MD5 encryption is not reversible. To restore the password to clear text, you must delete the user account and re-create it without checking the **Encrypt password** option.

Privilege Level

Enter the privilege level for the user. When applied to a CLI command, that command can only be executed by users with a privilege level equal to or higher than the level set for the command.

Associate a View with the user

This field is displayed when you are setting up user accounts for router access. It may not be visible if you are working in a different area of Cisco SDM.

Check the **Associate a View with the user** option if you want to restrict user access to a specific view. If you associate a view with any user for the first time, you are prompted to enter the view password. This option is only available in the Router Access node of the Additional Tasks tree.

View Name:

Choose the view you want to associate with this user from the following:

- SDM_Administrator—A user associated with the view type SDM_Administrator has complete access to Cisco SDM and can perform all operations supported by Cisco SDM.
- SDM_Monitor—A user associated with the view type SDM_Monitor can monitor all features supported by Cisco SDM. The user is not able to deliver configurations using Cisco SDM. The user is able to navigate the various areas of Cisco SDM, such as Interfaces and Connections, Firewall, and VPN. However, the user interface components in these areas are disabled.
- SDM_Firewall—A user associated with the view type SDM_Firewall can use the Cisco SDM Firewall and Monitor features. The user can configure firewalls and ACLs using the Firewall wizard, Firewall Policy View, and ACL Editor. User interface components in other areas are disabled for this user.
- SDM_EasyVPN_Remote—A user associated with the view type SDM_EasyVPN_Remote can use the Cisco SDM Easy VPN Remote features. The user is able to create Easy VPN Remote connections and edit them. User interface components in other areas are disabled for this user.

Details

The **Associate a View for this user** area displays details of the specified view. Click the **Details** button for a more detailed information about the specified view.

View Password

When you associate a view with any user for the first time, you are prompted to enter the view password for Cisco SDM-defined views. Use this password to switch between other views.

Enter the View Password

Enter the view password in the View Password field.

vty Settings

This window displays the virtual terminal (vty) settings on your router. The Property column contains configured line ranges and configurable properties for each range. The settings for these properties are contained in the Value column.

This table shows your router vty settings and contains the following columns:

- Line Range—Displays the range of vty connections to which the rest of the settings in the row apply.
- Input Protocols Allowed—Shows the protocols configured for input. Can be Telnet, SSH, or both Telnet and SSH.
- Output Protocols Allowed—Shows the protocols configured for output. Can be Telnet, SSH, or both Telnet and SSH.
- EXEC Timeout—Number of seconds of inactivity after which a session is terminated.
- Inbound Access-class—Name or number of the access rule applied to the inbound direction of the line range.
- Outbound Access-class—Name or number of the access rule applied to the outbound direction of the line range.
- ACL—If configured, shows the ACL associated with the vty connections.
- Authentication Policy—The AAA authentication policy associated with this vty line. This field is visible if AAA is configured on the router.
- Authorization Policy—The AAA authorization policy associated with this vty line. This field is visible if AAA is configured on the router.

Note To use SSH as an input or output protocol, you must enable it by clicking **SSH** in the Additional Tasks tree and generating an RSA key.

Edit vty Lines

This window lets you edit virtual terminal (vty) settings on your router.

Line Range

Enter the range of vty lines to which the settings made in this window will apply.

Time Out

Enter the number of seconds of inactivity allowed to pass before an inactive connection will be terminated.

Input Protocol

Choose the input protocols by clicking the appropriate check boxes.

Telnet Check Box

Check to enableTelnet access to your router.

SSH Check Box

Check to enable SSH clients to log in to the router.

Output Protocol

Choose the output protocols by clicking the appropriate check boxes.

Telnet Check Box

Check to enable Telnet access to your router.

SSH Check Box

Check to enable the router to communicate with SSH clients.

Access Rule

You can associate access rules to filter inbound and outbound traffic on the vty lines in the range.

Inbound

Enter the name or number of the access rule you want to filter inbound traffic, or click the button and browse for the access rule.

Outbound

Enter the name or number of the access rule you want to filter outbound traffic, or click the button and browse for the access rule.

Authentication/Authorization

These fields are visible when AAA is enabled on the router. AAA can be enabled by clicking **Additional Tasks** > **AAA** > **Enable**.

Authentication Policy

Choose the authentication policy that you want to use for this vty line.

Authorization Policy

Choose the authorization policy that you want to use for this vty line.

Configure Management Access Policies

Use this window to review existing management access policies and to choose policies for editing. Management access policies specify which networks and hosts will be able to access the router command-line interface. In the policy, you can specify which protocols the host or network in the policy can use, and which router interface will carry the management traffic.

Host/Network

A network address or host IP address. If a network address is given, the policy applies to all hosts on that network. If a host address is given, the policy applies to that host.

A network address is shown in the format network number/network bits, as in the following example:

```
172.23.44.0/24
```

For more information on this format, and on how IP addresses and subnet masks are used, see IP Addresses and Subnet Masks.

Management Interface

The router interface over which management traffic will flow.

Permitted Protocols

This column lists the protocols that the specified hosts can use when communicating with the router. The following protocols can be configured:

- Cisco SDM—Specified hosts can use Cisco SDM.
- Telnet—Specified hosts can use Telnet to access the router CLI.
- SSH—Specified hosts can use Secure Shell to access the router CLI.
- HTTP—Specified hosts can use Hypertext Transfer Protocol to access the router. If Cisco SDM is specified, either HTTP or HTTPS must also be specified.
- HTTPS—Specified hosts can use Hypertext Transfer Protocol Secure to access the router.
- RCP—Specified hosts can use Remote Copy Protocol to manage files on the router.
- SNMP—Specified hosts can use Simple Network Management Protocol to manage the router.

Add Button

Click to add a management policy, and specify the policy in the Add a Management Policy window.

Edit Button

Click to edit a management policy, and specify the policy in the Edit a Management Policy window.

Delete Button

Click to delete a specified management policy.

Apply Button

Click to apply changes you made in the Add or Edit a Management Policy window to the router configuration.

Discard Changes Button

Click to discard changes you made in the Add or Edit a Management Policy window to the router configuration. The changes you made are discarded and removed from the Configure Management Access Policies window.

Add or Edit a Management Policy

Use this window to add or edit a management policy.

Type

Specify whether the address you provide is the address of a host or a network.

IP Address/Subnet Mask

If you specified **Network** in the Type field, enter the IP address of a host, or the network address and subnet mask. For more information, see IP Addresses and Subnet Masks.

Interface

Choose the interface through which you want to allow management traffic. The interface should be the most direct route from the host or network to the local router.

Management Protocols

Specify the management protocols allowed for the host or network.

Allow SDM

Check to allow the specified host or network to access Cisco SDM. When you check this box, the following protocols are automatically checked: Telnet, SSH, HTTP, HTTPS, and RCP. Checking this option does not prevent you from allowing additional protocols.

If you want to make users employ secure protocols when logging in to Cisco SDM, check **Allow secure protocols only**. When you check this box, the following protocols are automatically checked: SSH, HTTPS, RCP. If you then check a nonsecure protocol such as Telnet, Cisco SDM unchecks **Allow secure protocols only**.

You Can Specify Management Protocols Individually

If you want to specify individual protocols that the host or network can use, you can check any of the boxes: Telnet, SSH, HTTP, RCP, or SNMP.

If Telnet and SSH are not enabled (checked) in the VTYs window, and SNMP is not enabled in the SNMP Properties window, Cisco SDM will advise you to enable those protocols when they are specified in this window.

Note The options **Allow secure protocols only** and **HTTPS** are disabled if the Cisco IOS release on the router does not support HTTPS.

Management Access Error Messages

The following error messages may be generated by the Management Access feature.

Error Message

```
SDM Warning: ANY Not Allowed
```

Explanation A management policy is read-only if any of its source or destination rule entries contain the “any” keyword. Such policies cannot be edited in the Management Access window. A policy containing the “any” keyword can create a security risk for the following reasons:

– If “any” is associated with source, it allows traffic from any network to enter the router.

– If “any” is associated with destination, it allows access to any node on the network supported by the router.

Recommended Action You can remove the access entry that caused this message to appear by choosing the rule in the Rules window and clicking **Edit**. Alternatively, in the Interfaces and Connections window, you can disassociate the rule from the interface it is applied to.

Error Message

```
SDM Warning: Unsupported Access Control Entry
```

Explanation A management policy will be read only if unsupported access control entries (ACEs) are associated with the interface or vty line to which you applied the management policy. You can use the CLI to remove the unsupported ACEs. Unsupported ACEs are those that contain keywords or syntax that Cisco SDM does not support.

Error Message

```
SDM Warning: SDM Not Allowed
```

Explanation This message is displayed if you still have not configured a management access policy to allow a host or network to access Cisco SDM on this router.

Recommended Action You must provide such a policy in order to make Cisco SDM on this router accessible. You cannot navigate to other features or deliver commands to the router until you configure a management access policy to allow access to Cisco SDM for a host or network.

Error Message

```
SDM Warning: Current Host Not Allowed
```

Explanation This message is displayed if you have not configured a management access policy to allow the current host or network to access Cisco SDM on this router.

Recommended Action You should create such a policy in order to make Cisco SDM on this router accessible from the current host or network. If you do not, you will lose the connection to the router when you deliver the configuration to the router. Click **Yes** to add to a management access policy now for the current host or network. Click **No** to proceed without adding a policy for the current host or network. You will lose contact with the router during command delivery, and you will have to log in to Cisco SDM using a different host or network.

SSH

This router implements Secure Shell (SSH) Server, a feature that enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality similar to that of an inbound Telnet connection, but which provides strong encryption to be used with Cisco IOS software authentication. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients. This feature is disabled if the router is not using an IPsec DES or 3DES Cisco IOS release, and if the SSH branch of the Additional Tasks tree does not appear.

SSH uses an RSA cryptographic key to encrypt data traveling between the router and the SSH client. Generating the RSA key in this window enables SSH communication between the router and the SSH clients.

Status Messages

Crypto key is not set on this device

Appears if there is no cryptographic key configured for the device. If there is no key configured, you can enter a modulus size and generate a key.

RSA key is set on this router

Appears if a cryptographic key was generated. SSH is enabled on this router.

Key modulus size Button

Visible if no cryptographic key has been generated. Click this button and enter the modulus size you want to give the key. If you want a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

Generate RSA Key Button

Click to generate a cryptographic key for the router using the modulus size you entered. If the cryptographic key was generated, this button is disabled.

DHCP Configuration

This window explains how you can manage DHCP configurations on your router.

DHCP Pools

This window displays the DHCP pools configured on the router.

Pool Name

The name of the DHCP pool.

Interface

The interface on which the DHCP pool is configured. Clients attached to this interface will receive IP addresses from this DHCP pool.

Details of DHCP Pool *name*

This area provides the following details about the pool identified in *name*:

- **DHCP Pool Range**—Range of IP addresses that can be granted to clients.
- **Default Router IP Address**—If the router has an IP address in the same subnet as the DHCP pool, it is shown here.

- **DNS Servers**—IP addresses of the DNS servers that the router will provide to DHCP clients.
- **WINS Servers**—IP addresses of the WINS servers that the router will provide to DHCP clients.
- **Domain Name**—Domain name configured on the router.
- **Lease Time**—Amount of time that the router will lease an IP address to a client.
- **Import All**—Whether the router imports DHCP option parameters to the DHCP server database and also sends this information to DHCP clients on the LAN when they request IP addresses.

Add

Choose this option to create a new DHCP pool. The user must specify the DHCP pool name, DHCP pool network, DHCP pool IP address range, and lease time. Optionally, DNS servers, WINS server, the domain name, and the default router can also be configured in the DHCP pool.

Edit

Choose this option to edit an existing DHCP pool.

Delete

Choose this option to delete a DHCP pool.

DHCP Pool Status

Click this button to see the IP addresses leased by the specified pool. If a DHCP pool contains any parameters other than pool network, IP address range, lease time, DNS servers, WINS servers, domain name, and default router, Cisco SDM shows this pool as read-only. If a pool contains a discontinuous range of IP addresses, it also is shown as read-only.

Add or Edit DHCP Pool

Add or edit a DHCP pool in this window. You cannot edit Cisco SDM-default pools.

DHCP Pool Name

Provide a name for the DHCP pool in this field.

DHCP Pool Network

Enter the network from which the IP addresses in the pool will be taken, for example, 192.168.233.0. This cannot be the IP address of an individual host.

Subnet Mask

Enter the subnet mask. The subnet mask of 255.255.255.0 provides 255 IP addresses.

DHCP Pool

Enter the starting and ending IP addresses in the range. For example, if the network is 192.168.233.0 and the subnet mask is 255.255.255.0, the starting address is 192.168.233.1 and the ending address is 192.168.233.254.

Lease Length

Enter the amount of time that addresses are to be leased to clients. You can specify that leased addresses never expire, or you can specify the lease time in days, hours, and minutes. Do not exceed 365 days, 23 hours, or 59 minutes.

DHCP Options

Enter information for the DNS servers, WINS servers, the domain name, and the default router in the DHCP options fields. These values are sent to DHCP clients when they request an IP address.

Import all DHCP Options into the DHCP server database

Click this option if you want to import DHCP option parameters into the DHCP server database and also send this information to DHCP clients on the LAN when they request IP addresses.

DHCP Bindings

This window shows existing manual DHCP bindings. A manual DHCP binding allows you to allocate the same IP address to a specific client each time the client requests an IP address from the available DHCP pools.

You can also add new bindings, edit existing bindings, or delete existing bindings.

Binding Name

Name assigned to the DHCP binding.

Host/IP Mask

IP address and mask bound to the client.

MAC Address

MAC address of the client.

Type

Type of MAC address is one of the following:

- Ethernet

  Client has a hardware address.
- IEEE802

  Client has a hardware address.
- <None>

  Client has a client identifier.

Client Name

Optional name assigned to the client.

Add Button

Click to add a new manual DHCP binding.

Edit Button

Click to edit the specified manual DHCP binding.

Delete Button

Click to delete the specified manual DHCP binding.

Add or Edit DHCP Binding

This window allows you to add or edit existing manual DHCP bindings.

Name

Enter the name you want for the DHCP binding. If you are editing the DHCP binding, the name field is read-only.

Host IP

Enter the IP address you want to bind to the client. The address should be from the DHCP pool available to the client. Do not enter an address in use by another DHCP binding.

Mask

Enter the mask used for the host IP address.

Identifier

From the drop-down menu, choose a method for identifying the client with a MAC address.

MAC Address

Enter the MAC address of the client. Do not enter an address in use by another DHCP binding.

Type

If you chose **Hardware Address** from the Identifier drop-down menu, choose **Ethernet** or **IEEE802** to set the MAC address type of the client.

Client Name (Optional)

Enter a name to identify the client. The name should be a hostname only, not a domain-style name. For example, *router* is an acceptable name, but *router.cisco.com* is not.

DNS Properties

The Domain Name System (DNS) is a database of Internet hostnames with their corresponding IP addresses distributed over designated DNS servers. It enables network users to refer to hosts by name, rather than by IP addresses, which are harder to remember. Use this window to enable the use of DNS servers for hostname-to-address translation.

Enable DNS-based hostname to address translation Check Box

Check to enable the router to use DNS. Uncheck if you do not want to use DNS.

DNS IP Address

Enter the IP addresses of the DNS servers that you want the router to send DNS requests to.

Click the **Add**, **Edit**, or **Delete** buttons to administer DNS IP address information.

Dynamic DNS Methods

This window shows a list of dynamic DNS methods.

Each dynamic DNS method shown will send with its update the hostname and domain name configured in **Configure > Additional Tasks > Router Properties**. However, if you create a dynamic DNS method when configuring a WAN interface, you can override the hostname and domain name configured in **Configure > Additional Tasks > Router Properties**. The new hostname and domain name will apply only to that dynamic DNS method.

Some dynamic DNS methods are read-only. These were configured in the Cisco IOS software through the CLI, and cannot be edited or deleted. To make these read-only methods editable, use the CLI to change the internal cache or host group options to HTTP or IETF.

Add Button

Click the **Add** button to create a new dynamic DNS method.

Edit Button

To edit a dynamic DNS method, choose it from the list of existing dynamic DNS methods and then click **Edit**.

Delete Button

To edit a dynamic DNS method, choose it from the list of existing dynamic DNS methods and then click **Delete**.

Note A warning appears if you attempt to delete a dynamic DNS method that is associated with one or more interfaces.

Add or Edit Dynamic DNS Method

This window allows you to add or edit a dynamic DNS method. Set the type of method by choosing **HTTP** or **IETF**.

HTTP

HTTP is a dynamic DNS method type that updates a DNS service provider with changes to the associated interface's IP address.

Server

If using HTTP, choose the domain address of the DNS service provider from the drop-down menu.

Username

If using HTTP, enter a username for accessing the DNS service provider.

Password

If using HTTP, enter a password for accessing the DNS service provider.

IETF

IETF is a dynamic DNS method type that updates a DNS server with changes to the associated interface's IP address.

If using IETF, configure a DNS server for the router in **Configure > Additional Tasks > DNS**.