Configuring Security for the ML-Series Card

This chapter describes the security features of the ML-Series card.

This chapter includes the following major sections:

Understanding Security

The ML-Series card includes several security features. Some of these features operate independently from the ONS node where the ML-Series card is installed. Others are configured using the Cisco Transport Controller (CTC) or Transaction Language One (TL1).

Security features configured with Cisco IOS include:

- Cisco IOS login enhancements
- Secure Shell (SSH) connection
- authentication, authorization, and accounting/Remote Authentication Dial-In User Service (AAA/RADIUS) stand alone mode
- Cisco IOS basic password (For information on basic Cisco IOS password configuration, see the "Passwords" section on page 3-8)

Security features configured with CTC or TL1 include:

- disabled console port
- AAA/RADIUS relay mode

Disabling the Console Port on the ML-Series Card

There are several ways to access the Cisco IOS running on the ML-Series card, including a direct connection to the console port, which is the RJ-11 serial port on the front of the card. Users can increase security by disabling this direct connection, which is enabled by default. This prevents console port input without preventing any console port output, such as Cisco IOS error messages.

You can disable console port access through CTC or TL1. To disable it with CTC, at the card-level view of the ML-Series card, click under the **IOS** tab and uncheck the **Enable Console Port Access** box and click **Apply.** The user must be logged in at the Superuser level to complete this task.

To disable it using TL1, refer to the *Cisco ONS SONET TL1 Command Guide*.

Secure Login on the ML-Series Card

The ML-Series card supports the Cisco IOS login enhancements integrated into Cisco IOS Release 12.2(25)S and introduced in Cisco IOS Release 12.3(4)T. The enhancements allow users to better secure the ML-Series card when creating a virtual connection, such as Telnet, SSH, or HTTP. The secure login feature records successful and failed login attempts for vty sessions (audit trail) on the ML-Series card. These features are configured using the Cisco IOS command-line interface (CLI.)

For more information, including step-by-step configuration examples, refer to the Cisco IOS Release 12.2(25)S feature guide module *Cisco IOS Login Enhancements* at http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guides_list.html.

Secure Shell on the ML-Series Card

This section describes how to configure the SSH feature.

These sections contain this information:

For other SSH configuration examples, see the "SSH Configuration Examples" section in the "Configuring Secure Shell" chapter of the *Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*, at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf.htm

Note For complete syntax and usage information for the commands used in this section, see the command reference for Cisco IOS Release 12.2 at the URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html.

Understanding SSH

The ML-Series card supports SSH, both version 1 (SSHv1) and version 2 (SSHv2). SSHv2 offers security improvements over SSHv1 and is the default choice on the ML-Series card.

SSH has two applications, an SSH server and SSH client. The ML-Series card only supports the SSH server and does not support the SSH client. The SSH server in Cisco IOS software works with publicly and commercially available SSH clients.

The SSH server enables a connection into the ML-Series card, similar to an inbound Telnet connection, but with stronger security. Before SSH, security was limited to the native security in Telnet. SSH improves on this by allowing the use of Cisco IOS software authentication.

The ONS node also supports SSH. When SSH is enabled on the ONS node, you use SSH to connect to the ML-Series card for Cisco IOS CLI sessions.

Note Telnet access to the ML-Series card is not automatically disabled when SSH is enabled. The user can disable Telnet access with the vty line configuration command **transport input ssh**.

Configuring SSH

This section has this configuration information:

- Configuration Guidelines, page 19-3
- Setting Up the ML-Series Card to Run SSH, page 19-3 (required)
- Configuring the SSH Server, page 19-4 (required)

Configuration Guidelines

Follow these guidelines when configuring the ML-Series card as an SSH server:

- The new model of AAA and a AAA login method must be enabled. If not previously enabled, complete the "Configuring AAA Login Authentication" section on page 19-11.
- A Rivest, Shamir, and Adelman (RSA) key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command. For more information, see the "Setting Up the ML-Series Card to Run SSH" section on page 19-3.
- When generating the RSA key pair, the message `No host name specified` might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.
- When generating the RSA key pair, the message `No domain specified` might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.

Setting Up the ML-Series Card to Run SSH

Follow these steps to set up your ML-Series card to run as an SSH server:

1. Configure a hostname and IP domain name for the ML-Series card.
2. Generate an RSA key pair for the ML-Series card, which automatically enables SSH.
3. Configure user authentication for local or remote access. This step is required.

Beginning in privileged EXEC mode, follow these steps to configure a hostname and an IP domain name and to generate an RSA key pair.

	Command	Purpose
Step 1	**Router #configure terminal**	Enter global configuration mode.
Step 2	**Router (config)# hostname** *hostname*	Configure a hostname for your ML-Series card.
Step 3	**Router (config)# ip domain-name** *domain_name*	Configure a host domain for your ML-Series card.
Step 4	**Router (config)# crypto key generate rsa**	Enable the SSH server for local and remote authentication on the ML-Series card and generate an RSA key pair. When you generate RSA keys, you are prompted to enter a modulus length. The default modulus length is 512 bits. A longer modulus length might be more secure, but it takes longer to generate and to use.
Step 5	**Router (config)# ip ssh timeout** *seconds*	Specify the timeout value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the ML-Series card uses the default timeout values of the CLI-based sessions. By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session timeout value returns to the default of 10 minutes.
Step 6	**Router (config)# ip ssh authentication-retries** *number*	Specify the number of times that a client can reauthenticate to the server. The default is 3; the range is 0 to 5.
Step 7	**Router (config)# end**	Return to privileged EXEC mode.
Step 8	**Router # show ip ssh** or **Router # show ssh**	Displays the version and configuration information for your SSH server. Displays the status of the SSH server on the ML-Series card.
Step 9	**Router #** show crypto key mypubkey rsa	Displays the generated RSA key pair associated with this ML-Series card.
Step 10	**Router # copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Configuring the SSH Server

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

	Command	Purpose
Step 1	`Router # configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# ip ssh version [1 | 2]`	(Optional) Configure the ML-Series card to run SSH Version 1 or SSH Version 2. • **1**—Configure the ML-Series card to run SSH Version 1. • **2**—Configure the ML-Series card to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.
Step 3	`Router (config)# ip ssh timeout` *seconds*	Specify the timeout value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the ML-Series card uses the default timeout values of the CLI-based sessions. By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session timeout value returns to the default of 10 minutes.
Step 4	`Router (config)# ip ssh authentication-retries` *number*	Specify the number of times that a client can reauthenticate to the server. The default is 3; the range is 0 to 5.
Step 5	`Router (config)# end`	Return to privileged EXEC mode.

Step 6	`Router # show ip ssh`
	or
	`Router # show ssh`
		Show the version and configuration information for your SSH server.
		Show the status of the SSH server connections on the ML-Series card.

Step 7	`Router # copy running-config startup-config`	(Optional) Save your entries in the configuration file.

To return to the default SSH control parameters, use the **no ip ssh** {**timeout** | **authentication-retries**} global configuration command.

Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in Table 19-1.

Table 19-1 Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
`show ip ssh`	Shows the version and configuration information for the SSH server.
`show ssh`	Shows the status of the SSH server.

For more information about these commands, see the "Secure Shell Commands" section in the "Other Security Features" chapter of the *Cisco IOS Security Command Reference, Cisco IOS Release 12.2,* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fothercr.htm.

RADIUS on the ML-Series Card

RADIUS is a distributed client/server system that secures networks against unauthorized access. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco or another software provider.

Many Cisco products offer RADIUS support, including the ONS 15454, ONS 15454 SDH, ONS 15327, ONS 15310-CL, and ONS 15600. The ML-Series card also supports RADIUS.

The ML-Series card can operate either in RADIUS relay mode or in RADIUS stand alone mode (default). In either mode, the RADIUS messages from the ML-Series card are passed to a RADIUS server that is on the data communications network (DCN) used to manage the ONS node.

RADIUS Relay Mode

In RADIUS relay mode, RADIUS on the ML-Series card is configured by CTC or TL1 and uses the AAA/RADIUS features of the ONS 15454 or ONS 15454 SDH node, which contains the ML-Series card. There is no interaction between RADIUS relay mode and RADIUS standalone mode. For information on ONS node security, refer to the "Security" chapter of the ONS node's reference manual.

An ML-Series card operating in RADIUS relay mode does need to be specified as a client in the RADIUS server entries. The RADIUS server uses the client entry for the ONS node as a proxy for the ML-Series card.

Enabling relay mode disables the Cisco IOS CLI commands used to configure AAA/RADIUS. The user can still use the Cisco IOS CLI commands not related to AAA/RADIUS.

In relay mode, the ML-Series card shows a RADIUS server host with an IP address that is really the internal IP address of the active timing, communications, and control card (TCC2/TCC2P). When the ML-Series card actually sends RADIUS packets to this internal address, the TCC2/TCC2P converts the RADIUS packet destination into the real IP address of the RADIUS server. In stand alone mode, the ML-Series card shows the true IP addresses of the RADIUS servers.

When in relay mode with multiple RADIUS server hosts, the ML-Series card IOS CLI **show run** output also shows the internal IP address of the active TCC2/TCCP card. But since the single IP address now represents multiple hosts, different port numbers are paired with the IP address to distinguish the individual hosts. These ports are from 1860 to 1869, one for each authentication server host configured, and from 1870 to 1879, one for each accounting server host configured.

The single IP address will not match the host IP addresses shown in CTC, which uses the true addresses of the RADIUS server hosts. These same true IP addresses appear in the ML-Series card IOS CLI **show run** output, when the ML-Series card is in stand alone mode.

Note A user can configure up to 10 servers for either authentication or accounting application, and one server host can perform both authentication and accounting applications.

Configuring RADIUS Relay Mode

This feature is turned on with CTC or TL1. To enable RADIUS Relay Mode through CTC, go to the card-level view of the ML-Series card, check the **Enable RADIUS Relay** box and click **Apply.** The user must be logged in at the Superuser level to complete this task.

To enable it using TL1, refer to the *Cisco ONS SONET TL1 Command Guide*.

Caution Switching the ML-Series card into RADIUS relay mode erases any configuration in the Cisco IOS configuration file related to AAA/RADIUS. The cleared AAA/RADIUS configuration is not restored to the Cisco IOS configuration file when the ML-Series card is put back into stand alone mode.

Caution Do not use the Cisco IOS command **copy running-config startup-config while the ML-Series card is in relay mode. This command will save a Cisco IOS configuration file with RADIUS relay enabled. On a reboot, the ML-Series card would come up in RADIUS relay mode, even when the** Enable RADIUS Relay box **on the CTC is not checked. If this situation arises, the user should** check the **Enable RADIUS Relay** box and click **Apply and then uncheck** the **Enable RADIUS Relay** box and click **Apply**. Doing this will set the ML-Series card in stand alone mode and clear RADIUS relay from the ML-Series card configuration.

RADIUS Stand Alone Mode

In stand alone mode, RADIUS on the ML-Series card is configured with the Cisco IOS CLI in the same general manner as RADIUS on a Cisco Catalyst switch.

This section describes how to enable and configure RADIUS in the stand alone mode on the ML-Series card. RADIUS in stand alone mode is facilitated through AAA and enabled through AAA commands.

Note For the remainder of the chapter, RADIUS refers to the Cisco IOS RADIUS available when the ML-Series card is in stand alone mode. It does not refer to RADIUS relay mode.

Note For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Security Command Reference, Release 12.2*.

These sections contain this configuration information:

Understanding RADIUS

When a user attempts to log in and authenticate to an ML-Series card with access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of these responses from the RADIUS server:
   a. ACCEPT—The user is authenticated.
   b. REJECT—The user is either not authenticated and is prompted to reenter the username and password, or access is denied.

The ACCEPT and REJECT responses are bundled with additional data that is used for privileged EXEC or network authorization. Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization if it is enabled. The additional data included with the ACCEPT and REJECT packets includes these items:

- Telnet, SSH, rlogin, or privileged EXEC services
- Connection parameters, including the host or client IP address, access list, and user timeouts

Configuring RADIUS

This section describes how to configure your ML-Series card to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You must also apply the method list to the interface on which you want authentication to occur. For the ML-Series card, this is the vty ports. You can optionally define method lists for RADIUS authorization and accounting.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your ML-Series card.

These sections contain this configuration information:

- Default RADIUS Configuration, page 19-9
- Identifying the RADIUS Server Host, page 19-9 (required)
- Configuring AAA Login Authentication, page 19-11 (required)
- Defining AAA Server Groups, page 19-13 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 19-15 (optional)
- Starting RADIUS Accounting, page 19-16 (optional)
- Configuring a nas-ip-address in the RADIUS Packet, page 19-16 (optional)
- Configuring Settings for All RADIUS Servers, page 19-17 (optional)
- Configuring the ML-Series Card to Use Vendor-Specific RADIUS Attributes, page 19-18 (optional)
- Configuring the ML-Series Card for Vendor-Proprietary RADIUS Server Communication, page 19-19 (optional)

Default RADIUS Configuration

RADIUS and AAA are disabled by default. To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the ML-Series card through the Cisco IOS CLI.

Identifying the RADIUS Server Host

ML-Series-card-to-RADIUS-server communication involves several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their hostname or IP address, their hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the ML-Series card tries the second host entry configured on the same device for accounting services.

To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the ML-Series card. A RADIUS server, the ONS node, and the ML-Series card use a shared secret text string to encrypt passwords and exchange responses. The system ensures that the ML-Series cards' shared secret matches the shared secret in the NE.

Note If you configure both global and per-server functions (timeout, retransmission, and key commands) on the switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these settings on all RADIUS servers, see the "Configuring Settings for All RADIUS Servers" section on page 19-17.

Note Retransmission and timeout period values are configureable on the ML-Series card in stand alone mode. These values are not configureable on the ML-Series card in relay mode.

You can configure the ML-Series card to use AAA server groups to group existing server hosts for authentication. For more information, see the "Defining AAA Server Groups" section on page 19-13.

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

	Command	Purpose
Step 1	`Router # configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# aaa new-model`	Enable AAA.
Step 3	**Router (config)# radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	`Router (config)# end`	Return to privileged EXEC mode.
Step 5	`Router# show running-config`	Verify your entries.
Step 6	`Router# copy running-config startup-config`	(Optional) Save your entries in the configuration file.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
Switch(config)# radius-server host host1
```

Note You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, see the RADIUS server documentation.

Configuring AAA Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list, which is named *default*. The default method list is automatically applied to all ports except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

For additional information on AAA login, refer to the "Authentication, Authorization, and Accounting (AAA)" chapter of the *Cisco IOS Security Configuration Guide, Release 12.2* at: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	`Router# configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# aaa new-model`	Enable AAA.

	Command	Purpose
Step 3	**Router (config)# aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: – **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the **enable** *password* global configuration command. – **group radius**—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see the "Identifying the RADIUS Server Host" section on page 19-9. – **line**—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the **password** *password* line configuration command. – **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *name* **password** global configuration command. – **local-case**—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the **username** *password* global configuration command. – **none**—Do not use any authentication for login.
Step 4	**Router (config)# line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.

	Command	Purpose
Step 5	`Router (config-line)# login authentication` {`default` | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	`Router (config)# end`	Return to privileged EXEC mode.
Step 7	`Router# show running-config`	Verify your entries.
Step 8	`Router# copy running-config startup-config`	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Defining AAA Server Groups

You can configure the ML-Series card to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service, such as accounting. If you configure two different host entries on the same RADIUS server for the same service, the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	`Router# configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# aaa new-model`	Enable AAA.

	Command	Purpose
Step 3	**Router (config)# radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or hostname of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	**Router (config)# aaa group server radius** *group-name*	Define the AAA server-group with a group name. This command puts the ML-Series card in a server group configuration mode.
Step 5	**Router (config-sg-radius)# server** *ip-address*	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	**Router (config-sg-radius)# end**	Return to privileged EXEC mode.
Step 7	**Router # show running-config**	Verify your entries.
Step 8	**Router # copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the "Configuring AAA Login Authentication" section on page 19-11.

To remove the specified RADIUS server, use the **no radius-server host** *hostname | ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the ML-Series card is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the ML-Series card uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

There is no support for setting the privilege level on the ML-Series card or using the **priv-lvl** command. A user authenticating with a RADIUS server will only access the ML-Series card with a privilege level of 1, which is the default login privilege level. Because of this, a priv-lvl configured on the RADIUS server should have the priv-lvl of 0 or 1. Once a user is authenticated and gains access to the ML-Series card, they can use the enable password to gain privileged EXEC authorization and become a super user with a privilege level of 15, which is the default privilege level of enable mode.

This example of an ML-Series card user record is from the output of the RADIUS server and shows the privilege level:

```
CISCO15 Auth-Type := Local, User-Password == "otbu+1"
Service-Type = Login,
Session-Timeout = 100000,
Cisco-AVPair = "shell:priv-lvl=1"
```

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	`Router# configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# aaa authorization network radius`	Configure the ML-Series card for user RADIUS authorization for all network-related service requests.
Step 3	`Router (config)# aaa authorization exec radius`	Configure the ML-Series card for user RADIUS authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	`Router (config)# end`	Return to privileged EXEC mode.
Step 5	`Router# show running-config`	Verify your entries.
Step 6	`Router# copy running-config startup-config`	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the ML-Series card reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

	Command	Purpose
Step 1	`Router# configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# aaa accounting network start-stop radius`	Enable RADIUS accounting for all network-related service requests.
Step 3	`Router (config)# aaa accounting exec start-stop radius`	Enable RADIUS accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 4	`Router (config)# end`	Return to privileged EXEC mode.
Step 5	`Router# show running-config`	Verify your entries.
Step 6	`Router# copy running-config startup-config`	(Optional) Save your entries in the configuration file.

To disable accounting, use the **no aaa accounting** {**network** | **exec**} **start-stop** *method1...* global configuration command.

Configuring a nas-ip-address in the RADIUS Packet

The ML-Series card in RADIUS relay mode allows the user to configure a separate nas-ip-address for each ML-Series card. In RADIUS standalone mode, this command is hidden in the Cisco IOS CLI. This allows the RADIUS server to distinguish among individual ML-Series card in the same ONS node.

Identifying the specific ML-Series card that sent the request to the server can be useful in debugging from the server. The nas-ip-address is primarily used for validation of the RADIUS authorization and accounting requests.

If this value is not configured, the nas-ip-address is filled in by the normal Cisco IOS mechanism using the value configured by the **ip radius-source** command. If no value is specified then the best IP address routable to the server is used. If no routable address is available, the IP address of the server is used.

Beginning in privileged EXEC mode, follow these steps to configure the nas-ip-address:

	Command	Purpose
Step 1	**Router# configure terminal**	Enter global configuration mode.
Step 2	**Router (config)# [no] ip radius nas-ip-address** {*hostname* | *ip-address*}	Specify the IP address or hostname of the attribute 4 (nas-ip-address) in the radius packet. If there is only one ML-Series card in the ONS node, this command does not provide any advantage. The public IP address of the ONS node serves as the nas-ip-address in the RADIUS packet sent to the server.
Step 3	**Router (config)# end**	Return to privileged EXEC mode.
Step 4	**Router# show running-config**	Verify your settings.
Step 5	**Router# copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the ML-Series card and all RADIUS servers:

	Command	Purpose
Step 1	**Router# configure terminal**	Enter global configuration mode.
Step 2	**Router (config)# radius-server key** *string*	Specify the shared secret text string used between the ML-Series card and all RADIUS servers. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 3	**Router (config)# radius-server retransmit** *retries*	Specify the number of times the ML-Series card sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.
Step 4	**Router (config)# radius-server timeout** *seconds*	Specify the number of seconds a ML-Series card waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.

	Command	Purpose
Step 5	**Router (config)# radius-server deadtime** *minutes*	Specify the number of minutes to mark as "dead" any RADIUS servers that fail to respond to authentication requests. A RADIUS server marked as "dead" is skipped by additional authentication requests for the specified number of *minutes*. This allows trying the next configured server without having to wait for the request to time out before. If all RADIUS servers are marked as "dead," the skipping will not take place. The default is 0; the range is 1 to 1440 minutes.
Step 6	**Router (config)# end**	Return to privileged EXEC mode.
Step 7	**Router# show running-config**	Verify your settings.
Step 8	**Router# copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default setting for the retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the ML-Series Card to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the ML-Series card and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco Terminal Access Controller Access Control System Plus (TACACS+) specification, and *sep* is the character = for mandatory attributes and the character * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, this AV pair activates Cisco's *multiple named ip address pools* feature during IP authorization (during point-to-point protocol [PPP] internet protocol control protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

This example shows how to specify an authorized VLAN in the RADIUS server database:

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

This example shows how to apply an input access control list (ACL) in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

This example shows how to apply an output ACL in ASCII format to an interface for the duration of this connection:

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

Beginning in privileged EXEC mode, follow these steps to configure the ML-Series card to recognize and use VSAs:

	Command	Purpose
Step 1	`Router# configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# radius-server vsa send [accounting | authentication]`	Enable the ML-Series card to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used. The AAA server includes the authorization level in the VSA response message for the ML-Series card.
Step 3	`Router (config)# end`	Return to privileged EXEC mode.
Step 4	`Router# show running-config`	Verify your settings.
Step 5	`Router# copy running-config startup-config`	(Optional) Save your entries in the configuration file.

For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, see the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide, Release 12.2*.

Configuring the ML-Series Card for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the ML-Series card and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the ML-Series card. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

	Command	Purpose
Step 1	`Router# configure terminal`	Enter global configuration mode.
Step 2	`Router (config)# radius-server host {`*`hostname`*` | `*`ip-address`*`} non-standard`	Specify the IP address or hostname of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.

	Command	Purpose
Step 3	**Router (config)# radius-server key** *string*	Specify the shared secret text string used between the ML-Series card and the vendor-proprietary RADIUS server. The ML-Series card and the RADIUS server use this text string to encrypt passwords and exchange responses. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 4	**Router (config)# end**	Return to privileged EXEC mode.
Step 5	**Router# show running-config**	Verify your settings.
Step 6	**Router# copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the vendor-proprietary RADIUS host, use the **no radius-server host** {*hostname* | *ip-address*} **non-standard** global configuration command. To disable the key, use the **no radius-server key** global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the ML-Series card and the server:

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

Displaying the RADIUS Configuration

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