CHAPTER 29

Configuring Security for the ML-MR-10 Card

This chapter describes the security features of the ML-MR-10 card and includes the following major sections:

Understanding Security

The ML-MR-10 card includes several security features. Some of these features operate independently from the ONS node where the ML-MR-10 card is installed. Others are configured using the Cisco Transport Controller (CTC) or Transaction Language One (TL1).

In software release 9.0 the ML-MR-10 card supports the following security features:

- Remote Authentication Dial-In User Service (RADIUS) stand alone
- RADIUS relay via shelf controller
- Disable or enable console access

The RADIUS stand alone feature operates independently from the ONS node where the ML-MR-10 card is installed and is configured with Cisco IOS.

The RADIUS relay feature and the disable or enable console access feature are configured using the CTC or TL1.

Disabling the Console Port on the ML-MR-10 Card

There are several ways to access the Cisco IOS running on the ML-MR-10 card, including a direct connection to the console port, which is the RJ-11 serial port on the front of the card. You 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-MR-10 card, click under the **IOS** tab, uncheck the **Enable Console Port Access** box and click **Apply.** You 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*.

RADIUS on the ML-MR-10 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-MR-10 card also supports RADIUS.

The ML-MR-10 card can operate either in RADIUS relay mode or in RADIUS stand alone mode (default). In either mode, the RADIUS messages from the ML-MR-10 card are passed to a RADIUS server that is on the data communications network (DCN) used to manage the ONS node.

Displaying the RADIUS Configuration

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

RADIUS Stand Alone Mode

In stand alone mode, RADIUS on the ML-MR-10 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-MR-10 card. RADIUS in stand alone mode is facilitated through AAA and enabled through AAA commands.

Understanding RADIUS

When a user attempts to log in and authenticate to an ML-MR-10 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, 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 ML-MR-10 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-MR-10 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. The ML-MR-10 card allows only the following AAA and RADIUS commands in the stand alone mode:

- AAA commands:
  - aaa authentication
  - aaa authorization
  - aaa accounting
  - aaa new-model
- RADIUS commands:
  - RADIUS-server host
  - RADIUS-server dead-criteria
  - RADIUS-server deadtime

  - ip RADIUS source-interface
  - ip RADIUS nas-ip-address

The sections to follow contains the following configuration information:

- Default RADIUS Configuration, page 29-4
- Identifying the RADIUS Server Host, page 29-4 (required)
- Configuring AAA Login Authentication, page 29-6 (required)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 29-8 (optional)
- Starting RADIUS Accounting, page 29-9 (optional)

Default RADIUS Configuration

RADIUS and AAA are disabled by default. When enabled, RADIUS can authenticate users accessing the ML-MR-10 card through the Cisco IOS CLI.

Identifying the RADIUS Server Host

The ML-MR-10 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-MR-10 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-MR-10 card. A RADIUS server, the ONS node, and the ML-MR-10 card use a shared secret text string to encrypt passwords and exchange responses. The system ensures that the ML-MR-10 cards' shared secret matches the shared secret in the NE.

Note Retransmission and timeout period values are configureable on the ML-MR-10 card in stand alone mode. These values are not configureable on the ML-MR-10 card in relay mode.

You can configure the ML-MR-10 card to use AAA server groups to group existing server hosts for authentication. For more information, see the "Configuring RADIUS Authorization for User Privileged Access and Network Services" section on page 29-8.

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 router 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:

```
Router(config)# RADIUS-server host 172.29.36.49 auth-port 1612 key rad1
Router(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:

```
Router(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 router and the key string to be shared by both the server and the router. 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*.

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 29-4. – **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.
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**, the command uses 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.

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-MR-10 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-MR-10 card using the **priv-lvl** command. A user authenticating with a RADIUS server will only access the ML-MR-10 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-MR-10 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-MR-10 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 default group RADIUS`	Configure the ML-MR-10 card for user RADIUS authorization for all network-related service requests.
Step 3	`Router (config)# aaa authorization exec default group RADIUS`	Configure the ML-MR-10 card for user RADIUS authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).

	Command	Purpose
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-MR-10 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 default/list-name start-stop group radius`	Enable RADIUS accounting for all network-related service requests.
Step 3	`Router (config)# aaa accounting exec default/list-name start-stop group 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.

RADIUS Relay Mode

In RADIUS relay mode, RADIUS on the ML-MR-10 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-MR-10 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-MR-10 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-MR-10 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-MR-10 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-MR-10 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-MR-10 card shows the true IP addresses of the RADIUS servers.

When in relay mode with multiple RADIUS server hosts, the ML-MR-10 card Cisco IOS CLI **show run** command 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-MR-10 card Cisco IOS CLI **show run** command output when the ML-MR-10 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.

The sections to follow contains the following configuration information:

- Configuring RADIUS Relay Mode, page 29-10
- Configure RADIUS Relay AAA Service for Console Port, page 29-11
- Configuring a nas-ip-address in the RADIUS Packet, page 29-11

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-MR-10 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-MR-10 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-MR-10 card is put back into stand alone mode.

Caution Do not use the Cisco IOS command **copy running-config startup-config** while the ML-MR-10 card is in relay mode. This command will save a Cisco IOS configuration file with RADIUS relay enabled. On a reboot, the ML-MR-10 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 uncheck the Enable RADIUS Relay box, and click Apply. Doing this will set the ML-MR-10 card in stand alone mode and clear RADIUS relay from the ML-MR-10 card configuration.

Configure RADIUS Relay AAA Service for Console Port

Enabling RADIUS Relay using CTC/TL1 configures the ML-MR-10 card accordingly. But this does not configure RADIUS Relay AAA service on the console port. In order to configure RADIUS Relay AAA service for the console port, manually configure it using IOS-CLI.

For information on configuring RADIUS relay AAA service on cosole port refer to the following sections:

- Configuring AAA Login Authentication, page 29-6
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 29-8
- Starting RADIUS Accounting, page 29-9

Configuring a nas-ip-address in the RADIUS Packet

The ML-MR-10 card, in both RADIUS relay mode and RADIUS stand alone mode, allows the user to configure a separate nas-ip-address for each ML-MR-10 card. This allows the RADIUS server to distinguish among individual cards in the same ONS node. Identifying the specific 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 and the ML-MR-10 card is in RADIUS stand alone mode, the nas-ip-address is filled in by the normal Cisco IOS mechanism using the value configured by the **ip RADIUS source-interface** 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-MR-10 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.