Configuring Logging Policies

This chapter contains the following topics:

Logging on Cisco IOS Routers

Security Manager provides the following policies for configuring logging on a Cisco IOS router:

- Syslog Logging Setup—Enable the syslog-logging feature, and define basic logging parameters. For more information, see Defining Syslog Logging Setup Parameters, page 65-1.
- Syslog Servers—Define the remote servers to which syslog messages are sent. For more information, see Defining Syslog Servers, page 65-3.
- NetFlow—Enable NetFlow logging by providing parameters and interfaces. See Defining NetFlow Parameters, page 65-6 for more information.

Note We strongly recommend configuring a Network Time Protocol (NTP) policy on all routers on which logging is enabled. NTP synchronization provides accurate timestamps for syslog messages, which is essential for comparing logs on multiple devices.

Defining Syslog Logging Setup Parameters

This procedure describes enabling syslog logging on the router, and defining which messages are sent to a syslog server. In addition, you can optionally define:

- The source interface for all syslog messages sent from this device.
- The messages that are saved to a local buffer.
- An origin identifier added to each message.
- A rate limit on the number of messages that can be sent.

Note To send syslog messages from the router to a syslog server, you must also define the IP address of the syslog server. For more information, see Defining Syslog Servers, page 65-3.

Related Topics

- Defining Syslog Servers, page 65-3
- Understanding Log Message Severity Levels, page 65-4
- Logging on Cisco IOS Routers, page 65-1

Step 1 Do one of the following to access the router's Syslog Logging Setup page:

- (Device view) Select **Platform > Logging > Syslog Logging Setup** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > Syslog Logging Setup** from the Policy Type selector. Select an existing policy or create a new one.

The Syslog Logging Setup page is displayed. See Table 65-2 on page 65-8 for a description of the fields on this page.

Step 2 Select **Enable Logging** to turn on the syslog logging feature. If this option is not selected, no log messages are created.

Tip To use the device's default logging settings, or to restore the default settings, simply select Enable Logging, ensure all other fields are blank, then click **Save**. The default settings vary by device. See your router documentation for more details.

Step 3 (Optional) In the Source Interface field, enter the name of the interface or interface role whose address should be used as the source interface for all log messages sent to a syslog server; or click **Select** to select an interface role from a list or to create a new one. The source interface must have an IP address.

This option is useful when the syslog server cannot reach the address from which the connection originated (for example, due to a firewall). If you do not enter a value in this field, the address of the outgoing interface is used.

Step 4 (Optional) To send log messages to a syslog server:

a. Select **Enable Trap**. This option is selected by default.

b. Select a value from the Trap Level list. All messages of this severity or greater (that is, having the same or a lower severity-level number) are sent to the syslog server; messages of a lesser severity are ignored. For more information about severity levels, see Table 65-1 on page 65-4.

Step 5 (Optional) To save log messages locally to a buffer on the router:

a. Select **Enable Buffer**. This option is selected by default.

b. Enter the Buffer Size in bytes.

c. Select the lowest severity level for messages to be saved to the buffer. All messages of that severity level or greater are saved to the buffer.

d. Select **Use XML Format** to save messages in XML format. (You can configure both the regular buffer and the XML buffer in the same policy.) If you select this option, enter the size of the XML buffer in bytes.

Note Make sure not to make buffers so large that the router runs out of memory for other tasks. If this happens, deployment may fail.

Step 6 (Optional) Define a rate limit to prevent a flood of output messages:

a. Select **Enable Rate Limit**. This option is selected by default.

b. Enter the maximum number of messages that can be sent per second.

c. Select the severity levels to *exclude* from the rate limit. For example, if you select 2 (critical), all syslog messages of severity levels 0-2 are sent to the syslog server regardless of the defined rate limit.

d. Select **All Messages** to apply the rate limit to all syslog messages *except* console messages (and excepting those severity levels specifically excluded above).

e. Select **Console Messages** to apply the rate limit to console messages only.

Note If you enable rate limiting without specifying any options, the default settings (10 messages per second, applied to console messages only) are applied.

Step 7 (Optional) To add an origin identifier to the beginning of each syslog message:

a. Select the type of origin ID to send—the IP address of the router, its host name, or a text string that you provide.

b. If you select String, enter the desired text in the field provided. Spaces are permitted.

The origin identifier is useful for identifying the source of syslog messages in cases where you send output from multiple devices to a single syslog server.

Note The origin identifier is not added to messages sent to local destinations, such as the buffer, the console, and the monitor.

Defining Syslog Servers

This procedure describes how to define the servers to which the router should send syslog messages. When you define a syslog server, you can choose whether the logging messages it receives should be forwarded as plain text or in XML format.

If you define multiple syslog servers, logging messages are sent to all of them.

Before You Begin

- Enable syslog logging and define basic logging parameters on the Syslog Logging Setup page. For more information, see Defining Syslog Logging Setup Parameters, page 65-1.

Related Topics

- Defining Syslog Logging Setup Parameters, page 65-1
- Understanding Log Message Severity Levels, page 65-4
- Logging on Cisco IOS Routers, page 65-1

Step 1 Do one of the following to access the router's Syslog Servers page:

- (Device view) Select **Platform > Logging > Syslog Servers** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > Syslog Servers** from the Policy Type selector. Select an existing policy or create a new one.

The Syslog Servers page is displayed. See Table 65-3 on page 65-11 for a description of the fields on this page.

Step 2 To define a server to receive syslog messages from this router, click the **Add** button below the table to open the Syslog Server dialog box. See Table 65-4 on page 65-12 for more about this dialog box.

Step 3 In the IP Address field, enter the address of the desired syslog server, or click **Select** to select a network/host object from a list or to create a new one. For more information, see Specifying IP Addresses During Policy Definition, page 6-87.

Step 4 (Optional) Select **Forward Messages in XML Format** to forward received syslog messages in XML format instead of plain text.

Step 5 Click **OK** to save your definition and close the dialog box. The syslog server you defined is displayed in the table.

Note To edit a syslog server, select it from the table, then click **Edit**. To remove a syslog server, select it, then click **Delete**.

Understanding Log Message Severity Levels

Syslog messages on Cisco IOS routers are classified into eight severity levels. Each severity level is identified by a number and a corresponding name. The lower the number, the greater the severity, as shown in the following table.

Table 65-1 Syslog Message Severity Levels

Level Number	Level Name	Description
0	emergency	System unusable
1	alert	Immediate action needed
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages only
7	debugging	Debug messages

Related Topics

- Defining Syslog Logging Setup Parameters, page 65-1
- Defining Syslog Servers, page 65-3

NetFlow on Cisco IOS Routers

The ability to characterize IP traffic and understand how and where it flows is critical for network availability, performance and troubleshooting. Monitoring IP traffic flows facilitates accurate capacity planning, and ensures that network resources are used appropriately in support of organizational goals.

NetFlow is a logging feature available on IOS devices for recording, caching and transmitting IP traffic-flow information on a per-interface basis. The basic output of NetFlow is a flow record, where a "flow" is defined as a unidirectional stream of packets between a given source and destination—both defined by a network-layer IP address and transport-layer source and destination port numbers.

On the IOS device, NetFlow consists of two key components—a NetFlow cache which stores IP flow data, and the NetFlow export mechanism that transmits the NetFlow records to a collection server for data reporting. Thus, when enabled, NetFlow records and caches statistics for incoming and outgoing traffic flows, periodically transmitting these records from the device to a NetFlow collector, in the form of User Datagram Protocol (UDP) datagrams.

Several different formats for the export packet, or flow record, have evolved as NetFlow has matured, and these formats are commonly referred to as the NetFlow version. These versions are well documented, and include versions 1, 5, 7, and 9. The most commonly used format is NetFlow version 5, but version 9 is the latest format and has some advantages for extensibility, security, traffic analysis and multicasting.

Security Manager currently supports Traditional NetFlow on IOS devices. Traditional NetFlow provides a fixed flow record, even for version 9, meaning the device will use certain flags and predefined record combinations in generating the flow. The device configuration settings define export destinations, export interface, and certain version-specific transmission options.

More About Traffic Flows and NetFlow

Each packet that passes into or out of a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or "fingerprint," and they define whether the packet is unique, or related to other packets.

All packets with the same source/destination IP address, source/destination ports, protocol interface, and class of service are grouped into a flow and the packets and bytes are tallied. This method of flow determination (or "fingerprinting") is scalable because a large amount of network information can be condensed into a database of NetFlow information called the NetFlow cache.

In general, the NetFlow cache is constantly filling with flows, and software in the router or switch is searching the cache for flows that have terminated or expired, and these flows are exported to the NetFlow collector. (Unlike SNMP polling, NetFlow export periodically transmits information to the NetFlow collector.) The NetFlow collector has the job of assembling and organizing the exported flows to produce the real-time or historical reports used for traffic and security analysis.

NetFlow Summary

To summarize, the following steps outline NetFlow:

- NetFlow is configured on the router or switch to capture IP traffic flows
- Flow records are stored in the local NetFlow cache
- Periodically, approximately 30 to 50 flow records are bundled together and exported to a NetFlow collector server
- The collector software creates reports from the NetFlow data

Related Topics

- Logging on Cisco IOS Routers, page 65-1
- Defining NetFlow Parameters, page 65-6
- NetFlow Policy Page, page 65-12

Defining NetFlow Parameters

This procedure describes enabling NetFlow logging on the router.

Related Topics

- NetFlow on Cisco IOS Routers, page 65-5
- NetFlow Policy Page, page 65-12
- Logging on Cisco IOS Routers, page 65-1

Step 1 To access the router's NetFlow page, do one of the following:

- (Device view) Select **Platform > Logging > NetFlow** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > NetFlow** from the Policy Type selector. Select an existing policy or create a new one.

The router's NetFlow page is displayed. See NetFlow Policy Page, page 65-12 for complete descriptions of the fields on this page.

Step 2 On the **Setup** tab of the NetFlow page, specify global NetFlow parameters for the router:

- **Primary Destination** – Choose IP Address or Hostname from this list to enable NetFlow collection and to specify how the primary NetFlow collector will be defined. You can choose the blank entry to disable this option.
  - **IP Address** – Enter the IP address of the device hosting the primary NetFlow Collection Engine, and then enter the number of the **UDP Port** monitored by that flow collector (port numbers can range from 1 to 65535)
  - **Hostname** – Enter the fully qualified domain name of the device hosting the primary NetFlow Collection Engine, and then enter the number of the **UDP Port** monitored by that flow collector (port numbers can range from 1 to 65535)
- **Redundant Destination** – Choose IP Address or Hostname from this list to specify how the back-up NetFlow collector will be defined. You can choose the blank entry to disable this option.
  - **IP Address** – Enter the IP address of the device hosting the secondary NetFlow Collection Engine, and then enter the number of the **UDP Port** monitored by that flow collector (port numbers can range from 1 to 65535)
  - **Hostname** – Enter the fully qualified domain name of the device hosting the secondary NetFlow Collection Engine, and then enter the number of the **UDP Port** monitored by that flow collector (port numbers can range from 1 to 65535)

  Note If you define a Primary and a Redundant Destination, flow data is transmitted to both.

- **Source Interface** – Specify the router interface through which flow data will be transmitted to the collector destination(s).

- **Version** – Define the record format to be used for flow data by choosing the appropriate NetFlow version number from this drop-down list. You can choose the blank entry to disable this option.
  - **1** – The original record format. No additional parameters are required.
  - **5** – The most widely adopted format; includes Border Gateway Protocol (BGP) autonomous system (AS) information and flow sequence numbers.

    If BGP is configured on your network, you can include either origin or peer AS information in the NetFlow records. Choose **origin-as** or **peer-as** from the AS Type drop-down list. You can choose the blank entry to disable this option.

    Check **Enable BGP Nexthop** to include BGP next hop information in the flow caches. (Note that with version 5, this information is visible in the caches, but it is not exported.)
  - **9** – The most-recent, template-based version; not yet fully supported.

    If BGP is configured on your network, you can include either origin or peer AS information in the NetFlow records. Choose **origin-as** or **peer-as** from the AS Type drop-down list. You can choose the blank entry to disable this option.

    Check **Enable BGP Nexthop** to include BGP next hop information in the flow records.

Note AS information collection is resource intensive, especially for origin-as. If you are not interested in monitoring peering arrangements, disabling AS collection may improve performance.

Step 3 On the **Interfaces** tab, define the interfaces for which traffic flows are to be reported.

- To add an interface, click the Add Row button to open the Add NetFlow Interface Settings dialog box. This dialog box is described in Adding and Editing NetFlow Interface Settings, page 65-15.
- To edit an existing interface, select the appropriate entry in the Interfaces table and then click the Edit Row button to open the Edit NetFlow Interface Settings dialog box (described in Adding and Editing NetFlow Interface Settings, page 65-15).
- To delete an existing interface, select that entry in the Interfaces table and then click the Delete Row button, and then confirm the deletion.

Note You can disable NetFlow data collection on an interface without deleting it. Refer to Adding and Editing NetFlow Interface Settings, page 65-15 for more information.

Syslog Logging Setup Policy Page

Use the Syslog Logging Setup page to enable syslog logging and define basic logging parameters on the selected Cisco IOS router.

For more information, see Defining Syslog Logging Setup Parameters, page 65-1.

Note We strongly recommend that you define an NTP policy on all routers on which logging is enabled in order to create accurate timestamps for each log message. For more information, see NTP Policy Page, page 63-98.

Note If you unassign a logging setup policy, the default logging configuration is restored on the device upon deployment.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog Logging Setup** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > Syslog Logging Setup** from the Policy Type selector. Right-click **Syslog Logging Setup** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Logging on Cisco IOS Routers, page 65-1
- Syslog Servers Policy Page, page 65-10
- NTP on Cisco IOS Routers, page 63-96
- Understanding Interface Role Objects, page 6-73

Field Reference

Table 65-2 Syslog Logging Setup Page

Element	Description
Enable Logging	When selected, syslog logging is enabled on the device. When deselected, logging is disabled on the device. This is the default. **Tip** To use the device's default syslog logging settings, select the Enable Logging check box, then click **Save**, without entering additional values.
Source Interface	The source address for all outgoing log messages sent to a syslog server. This setting may be necessary when the syslog server cannot respond to the address from which the log message originated (for example, due to a firewall). If you do not define a value in this field, the address of the outgoing interface is used. Enter the name of an interface or interface role, or click **Select** to select an object from a list or to create a new one.
Trap	Defines which log messages are forwarded to a syslog server: • Enable Trap—When selected, log messages are sent to the syslog server. This is the default. When deselected, log messages are not sent. • Trap Level—The lowest severity level of messages that are logged and sent to the syslog server. All messages of this severity and greater are logged. Severity levels are identified by a name and a number. For more information, see Table 65-1 on page 65-4. **Tip** To restore the router's default trap settings, select **Enable Trap**, then select the blank setting from the Trap Level list.

Table 65-2 Syslog Logging Setup Page (continued)

Element	Description
Logging Buffer	Defines whether log messages are saved locally to a buffer on the device. • Enable Buffer—When selected, log messages are saved to a buffer on the device. This is the default. When deselected, a log buffer is not maintained on the device. • Buffer Size—The size of the buffer in bytes. Valid values range from 4096 to 4294967295 bytes (4 kilobytes to 4 gigabytes). The default size varies by platform. Make sure not to make the buffer so large that the router runs out of memory for other tasks; otherwise, deployment might fail. **Note** The maximum buffer size might be smaller on some devices. • Severity Level—The lowest severity level of messages that are saved in the buffer. All messages of this severity and greater are saved. On most Cisco IOS routers, the default severity level is 7 (debugging). Severity levels are identified by a name and a number. For more information, see Table 65-1 on page 65-4. • Use XML Format—When selected, log messages are saved to a buffer in XML format. (You can configure both the regular buffer and the XML buffer in the same policy.) When deselected, an XML buffer is not maintained on the device. • Buffer Size—The size of the XML buffer in bytes. Valid values range from 4096 to 4294967295 bytes (4 kilobytes to 4 gigabytes). **Note** The maximum buffer size might be smaller on some devices. **Tip** To restore the router's default buffer settings, select **Enable Trap**, erase the buffer size setting, then select the blank setting from the Severity Level list.

Table 65-2 Syslog Logging Setup Page (continued)

Element	Description
Rate Limit	Limits the rate of log messages sent to the syslog server. • Enable Rate Limit—When selected, the rate limit is enabled. When deselected, the rate limit is disabled. • Messages per Sec.—The maximum number of logging messages that can be sent per second. Valid values range from 1 to 10000. The default is 10 messages per second. • Exclude—The types of messages to *exclude* from the rate limit. This setting excludes the severity level you select as well as all messages with a lower severity level number (that is, more severe). The default is 3 (errors), which excludes all log messages with a severity level of 3, 2 (critical), 1 (alerts), or 0 (emergencies) from the rate limit. For more information about severity levels, see Table 65-1 on page 65-4. • All Messages—When selected, the rate limit applies to all messages except console messages. • Console Messages—When selected, the rate limit applies to console messages only. **Tip** To restore the router's default rate limit settings, select the **Enable Rate Limit** check box, then erase the rate limit value setting.
Origin ID	The origin identifier that is added to the beginning of all syslog messages sent from this device to the remote syslog server. The origin identifier is useful in cases where you send output from multiple devices to a single syslog server. • ID Type—The type of origin identifier added to the beginning of each syslog message. Options are: – IP Address—The IP address of the source device. – Hostname—The hostname of the source device. – String—User-defined text. • Value—Applies only when you select String as the ID type. Enter the text of the user-defined string. Spaces are permitted, except for the first character. **Note** The origin identifier is not added to messages sent to local destinations, such as the buffer, the console, and the monitor.

Syslog Servers Policy Page

Use the Syslog Servers page to create, edit, and delete servers that collect log messages from the router.

For more information, see Defining Syslog Servers, page 65-3.

Note To enable logging to the syslog servers defined on this page, you must enable logging and define basic parameters on the Syslog Logging Setup Policy Page, page 65-7.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog Servers** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > Syslog Servers** from the Policy Type selector. Right-click **Syslog Servers** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Logging on Cisco IOS Routers, page 65-1
- Syslog Server Dialog Box, page 65-11
- Table Columns and Column Heading Features, page 1-49
- Filtering Tables, page 1-48

Field Reference

Table 65-3 Syslog Servers Page

Element	Description
IP Address	The name of the syslog server, as represented by a network/host object, or its IP address.
XML	Indicates whether the syslog server receives log messages in XML format.
Add button	Opens the Syslog Server Dialog Box, page 65-11. From here you can define a syslog server.
Edit button	Opens the Syslog Server Dialog Box, page 65-11. From here you can edit the selected syslog server.
Delete button	Deletes the selected syslog server from the table.

Syslog Server Dialog Box

Use the Syslog Server dialog box to define the server that collects syslog messages from the router. You can also define whether the log messages it receives are in XML format or plain text.

Note To enable logging to the syslog servers defined on this page, you must enable logging and define basic parameters on the Syslog Logging Setup Policy Page, page 65-7.

Navigation Path

Go to the Syslog Servers Policy Page, page 65-10, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Syslog Servers, page 65-3
- Logging on Cisco IOS Routers, page 65-1

- Understanding Networks/Hosts Objects, page 6-80

Field Reference

Table 65-4 Syslog Server Dialog Box

Element	Description
IP Address	The IP address of the syslog server. Enter an IP address or the name of a network/host object, or click **Select** to select the object from a list or to create a new one.
Forward Messages in XML Format	When selected, log messages are sent to the syslog server in XML format. When deselected, log messages are sent to the syslog server as plain text.

NetFlow Policy Page

Use the NetFlow page to enable NetFlow recording and define its parameters on the selected Cisco IOS router.

The NetFlow page consists of two tabbed panels: Setup and Interfaces. The Setup tab provides global configuration parameters for NetFlow collection on the router. The Interfaces tab lists router interfaces for which NetFlow data collection is configured, and allows enabling and disabling ingress and egress accounting on a per-interface basis.

Note We strongly recommend that you define an NTP policy on all routers on which logging is enabled in order to create accurate timestamps for each log message. For more information, see NTP Policy Page, page 63-98.

Navigation Path

- (Device view) Select **Platform > Logging > NetFlow** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > NetFlow** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or right-click **NetFlow** to create a new policy.

Related Topics

- NetFlow on Cisco IOS Routers, page 65-5
- Defining NetFlow Parameters, page 65-6
- Adding and Editing NetFlow Interface Settings, page 65-15
- Logging on Cisco IOS Routers, page 65-1
- NTP on Cisco IOS Routers, page 63-96

Field Reference

Table 65-5 NetFlow Page

Element	Description
Setup tab	
Primary Destination Redundant Destination	The primary and secondary NetFlow collector. You must select a primary collector to enable NetFlow data collection on this device. To disable transmission of NetFlow data to either of these collectors, choose the blank entry from the drop-down list. Select whether to identify the NetFlow collector using its IP address or host name, then configure the required fields for each option: • **IP Address**—Enter the IP address of the device hosting the primary NetFlow Collection Engine. You can also specify a network/host object that specifies the IP address, or click **Select** to select the object from a list or to create a new one. In the **UDP Port** field, enter the port number monitored by the flow collector (port numbers can range from 1 to 65535). You can enter a number or the name of a port list object, or click **Select** to select an object from a list or to create a new one. • **Hostname**—Enter the fully qualified domain name of the device hosting the primary NetFlow Collection Engine. You also must specify the UDP port as you do when specifying the IP address.
Source Interface	The router interface through which flow data will be transmitted to the collector destinations. Enter an interface or interface role name, or click **Select** to select an object from a list or to create a new one.

Table 65-5 NetFlow Page (continued)

Element	Description
Version	The NetFlow version number, which defines the record format to be used for flow. You can choose the blank entry to disable this option. • **1**—The original record format. No additional parameters are required. • **5**—The most widely adopted format; includes Border Gateway Protocol (BGP) autonomous system (AS) information and flow sequence numbers. If BGP is configured on your network, you can include either origin or peer AS information in the NetFlow records. Choose **origin-as** or **peer-as** from the AS Type drop-down list. You can choose the blank entry to disable this option. Check **Enable BGP Nexthop** to include BGP next hop information in the flow caches. (Note that with version 5, this information is visible in the caches, but it is not exported.) • **9**—The most-recent, template-based version; not yet fully supported. If BGP is configured on your network, you can include either origin or peer AS information in the NetFlow records. Choose **origin-as** or **peer-as** from the AS Type drop-down list. You can choose the blank entry to disable this option. Check **Enable BGP Nexthop** to include BGP next hop information in the flow records. **Note** AS information collection is resource intensive, especially for origin-as. If you are not interested in monitoring peering arrangements, disabling AS collection might improve performance.
Interfaces tab	
Interface	The names of the interfaces on which NetFlow collection is configured.
Enable Ingress	"Enabled" indicates flow recording is enabled on this interface for incoming traffic; "Disabled" indicates incoming traffic is not recorded for this interface.
Enable Egress	"Enabled" indicates flow recording is enabled on this interface for outgoing traffic; "Disabled" indicates outgoing traffic is not recorded for this interface.
Add Row	Click this button to open the Add NetFlow Interface Settings dialog box. Adding a NetFlow interface is described in Adding and Editing NetFlow Interface Settings, page 65-15.
Edit Row	Click this button to open the Edit NetFlow Interface Settings dialog box for the selected interface. Editing NetFlow interfaces is described in Adding and Editing NetFlow Interface Settings, page 65-15.
Delete Row	Click this button to delete the selected interface. You will be asked to confirm the deletion.

Adding and Editing NetFlow Interface Settings

Use the Add NetFlow Interface Settings and Edit NetFlow Interface Settings dialog boxes to enable and disable NetFlow ingress and egress reporting for specific router interfaces.

Note Except for their titles, these two dialog boxes are identical. The following information applies to both.

Navigation Path

Go to the NetFlow Policy Page, page 65-12, then click the **Add Row** or **Edit Row** button beneath the table.

Related Topics

- Defining NetFlow Parameters, page 65-6
- Logging on Cisco IOS Routers, page 65-1

Field Reference

Table 65-6 Add/Edit NetFlow Interface Settings Dialog Box

Element	Description
Interface	The name of the interface or interface role. Enter a name or click **Select** to select an interface role from a list or to create a new one.
Enable Ingress Accounting	When this option is selected, NetFlow records are collected for traffic arriving on this interface. Deselect this option to halt data collection on this interface for incoming traffic.
Enable Egress Accounting	When this option is selected, NetFlow records are collected for traffic departing from this interface. Deselect this option to halt data collection on this interface for outgoing traffic.