Configuring Network Management Features

This chapter provides information about configuring the network management features for the Cisco 800M Series ISR and contains the following sections:

Cisco Configuration Professional

Cisco Configuration Professional is a GUI based device management tool for Cisco access routers. This tool simplifies routing, firewall, IPS, VPN, unified communications, and WAN, and LAN configurations through GUI-based wizards. Cisco CP is a valuable productivity enhancing tool for network administrators and channel partners for deploying routers with increased confidence and ease. It offers a one-click router lock-down and an innovative voice and security auditing capability to check and recommend changes to router configurations. Cisco CP also monitors router status and troubleshoots WAN and VPN connectivity issues.

For more information about configuring Cisco 800M series ISR using Cisco Configuration Professional, see the following web link:

http://www.cisco.com/c/dam/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_5/olh/ccp.pdf

Cisco Configuration Professional Express

Cisco Configuration Professional Express (Cisco CP Express), a lightweight version of Cisco Configuration Professional, is an embedded, device-management tool that provides the ability to bootstrap and provision a Cisco Integrated Services Router (ISR). The Cisco CP Express helps you set up a network with complete WAN and LAN configuration, along with security features.

For more information about configuring Cisco 800M series ISR using Cisco CP Express, see the following web link:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_configuration_professional_express/v3_1/guides/featureguide/ccp_express_Feature_Guide.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure is a network management tool that supports life cycle management of your entire network infrastructure from one graphical interface. Prime Infrastructure provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

For more information on configuring Cisco 800M Series ISR using Cisco Prime Infrastructure, see the the following web link:

http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-1/user/guide/pi_ug.html

Embedded Event Manager

Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

For more information on configuring Embedded Event Manager, see the following web link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-mt/eem-15-mt-book.html

Configuring IP SLAs

IP Service Level Agreements (IP SLAs) allows Cisco customers to analyze IP service levels for IP applications and services, to increase productivity, to lower operational costs, and to reduce the frequency of network outages. IP SLAs uses active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. Using IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance. IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist administrators with network troubleshooting. IP SLAs can be

accessed using the Cisco software commands or Simple Network Management Protocol (SNMP) through the Cisco Round-Trip Time Monitor (RTTMON) and syslog Management Information Bases (MIBs).

For more information on configuring IP SLAs, see the following web link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-class-plc.html

Configuring Radius

The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

For more information about configuring Radius, see the following web link

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/15-mt/sec-usr-rad-15-mt-book/sec-cfg-radius.html

Configuring TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a device or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service--authentication, authorization, and accounting--independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service.

For more information about configuring TACACS+, see the following web link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/15-mt/sec-usr-tacacs-15-mt-book/sec-cfg-tacacs.html

Configuring SSH

Secure Shell (SSH) runs on top of a reliable transport layer and provides strong authentication and encryption capabilities.SSH provides a means to securely access and securely execute commands on another computer over a network.

For more information about configuring SSH see the following web link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-usr-ssh-15-mt-book/sec-usr-ssh-sec-shell.html

Configuring SNMP

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that is used for monitoring and managing devices in a network.

For more information about configuring SNMP, see the following web link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-mt/snmp-15-mt-book/nm-snmp-cfg-snmp-support.html

Configuring NetFlow

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the routing devices in the network. It is emerging as a primary network accounting and security technology.

NetFlow identifies packet flows for both ingress and egress IP packets. It does not involve any connection-setup protocol, either between routers or to any other networking device or end station. NetFlow does not require any change externally--either to the packets themselves or to any networking device. NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow capture and export are performed independently on each internetworking device; NetFlow need not be operational on each router in the network.

For more information about configuring NetFlow, see the following web link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book.html

Configuring Flexible NetFlow

Flexible NetFlow is a Cisco IOS technology that provides statistics on packets flowing through the router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting.

Flexible NetFlow improves on original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

For more information about configuring NetFlow, see the following web link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book.html

MIB Support

The Cisco 800M series ISR supports the MIBs supported by Cisco 800 series ISRs. The following MIBs are modified for Cisco 800M series ISR:

- CISCO-PRODUCTS-MIB
- OLD-CISCO-CHASSIS-MIB
- ENTITY-MIB
- IF-MIB

- CISCO-IF-EXTENSION-MIB
- CISCO-LICENSE-MGMT-MIB
- CISCO-WAN-3G-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB