Nortel Secure Router 2330/4134

Configuration — Network Management

Release: 10.2
Document Revision: 03.01

www.nortel.com

NN47263-602

Nortel Secure Router 2330/4134
Release: 10.2
Publication: NN47263-602
Document release date: 7 September 2009

Contents

New in this release

The following section details what is new in *Nortel Secure Router 2330/4134 Configuration — Network Management* (NN47263-602).

Features

See the following sections for information about feature changes.

SR2330 hardware

This document is updated to show support for the Secure Router 2330 chassis.

DHCPv4 over VLAN

With Release 10.2, you can configure DHCP server and DHCP Relay on VLAN interfaces. For more information, see "DHCPv4 over VLAN" (page 23).

DHCPv4 Relay over VLAN

With Release 10.2, you can also configure DHCPv4 Relay over VLAN. For more information, see "DHCPv4 Relay over VLAN" (page 71).

Enabling all traps

With Release 10.2, you can now enable all traps on the router using the **`enable-all`** option under **`snmp-server enable traps`**. For more information, see "Enabling traps" (page 35).

Clearing the event log

With Release 10.2, you can now clear the event log, using the **`clear event_log`** command. For more information, see "Clearing the event log" (page 47).

Introduction

This document contains procedural and conceptual information to help you to configure and manage the Nortel Secure Router 4134.

Navigation

Network management fundamentals

This section contains conceptual information to support the administration of the Nortel Secure Router 4134for performing network management tasks. Read and understand this information before you configure or maintain network management interfaces on the Nortel Secure Router 4134.

Prerequisites

- You need an understanding of basic network security concepts.
- Familiarity with SNMPv1 as per RFC 1157 and SNMPv2c as per RFC 1903.
- Familiarity with the structure of management information (SMI) v1 as per RFC 1155 and SMIv2 as per RFC 1902.

Navigation

Simple network management protocol

This section contains conceptual information about the Simple Network Management Protocol (SNMP) service on the Secure Router. SNMP is an application layer protocol that facilitates the exchange of management information between network devices.

SNMP is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. Use SNMP to manage network performance, find and solve network problems, and plan for network growth. You must have a good understanding of SNMP before you configure the SNMP service to access the Secure Router remotely from an SNMP-based network management system.

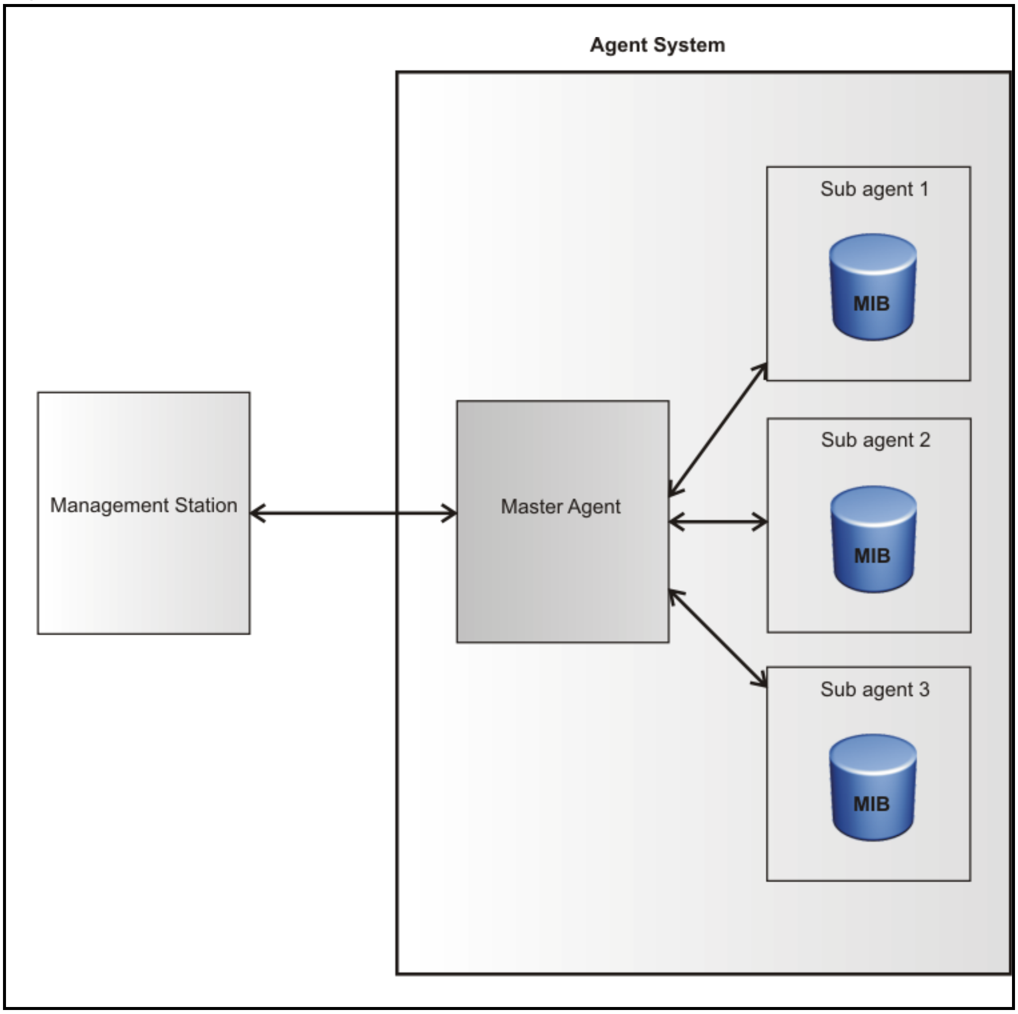
Within the SNMP framework, a managed node can be any hardware device connected to the network, for example, a router, computer, or terminal server. A managed node contains a processing entity called an agent. The agent accesses the management information. The agent contains the two following agent types:

- master agent—sends and receives SNMP protocol messages with the management station
- sub-agent(s)—receives the requests processed by the master agent and sends the response back to the master agent. Sub-agents directly access the management information database.

An external management station uses the SNMP protocol to communicate with and send SNMP requests to the master agent. The master agent processes the requests and sends a second request to the appropriate sub-agent to retrieve the information. The sub-agent processes the request and responds to the master agent that then forwards the response to the management station. The master and sub-agent do not use the SNMP protocol to communicate with one another; they use the AgentX protocol.

In the case of SNMP traps, the sub-agent sends a notification message to the master agent. The master agent reformats the message and forwards the notification to the destined management station. For an illustration of the SNMP process, see Figure 1 "AgentX Architecture" (page 13).

Figure 1
AgentX Architecture



You can use any configured and operational interface on the Secure Router to perform SNMP requests. If the management station is in a different network, you must configure the proper routes on both the management station and the Secure Router

Supported SNMP protocols and commands

The Secure Router supports SNMPv1 (RFC 1157) and SNMPv2c (RFC 1903) protocols. More specifically, the Secure Router supports:

- get and get-next requests from SNMPv1 and SNMPv2c
- get-bulk requests from SNMPv2c
- SNMP traps as per SNMPv1
- SNMPv2c notifications
- SMIv2 enterprise MIBs

- SMIv1 standard MIBs
- SNMP set requests are supported for the following MIB objects:
  - sysContact
  - sysName
  - sysLocation

SNMP requests use the User Datagram Protocol (UDP) port 161 to reach the agent. The agent sends traps using UDP port 162.

SNMP communities

SNMP communities are configured to define access control for SNMP clients requesting access to managed objects. A community is defined by specifying the name of the community in a text string.

When an SNMP manager uses a community string to request access to the Secure Router MIB collection, the community string is used to authenticate the SNMP manager. When an SNMP manager is successfully authenticated, access to the MIB collection is granted. The level of access authorized is based on the access privileges associated with the community string. The access privileges available are read-only and read-write. When the Secure Router does not recognize an SNMP manager as a valid client, authentication fails. SNMP authentication failure traps are sent to SNMP targets as specified by the trap target configuration.

You can configure a maximum of ten SNMP communities on the Secure Router. By default, all SNMP communities have read-only access.

Community clients

You can add SNMP clients to a community by specifying the IP address of the client. When you assign SNMP clients to an SNMP community, you restrict the set of SNMP clients that may access the MIB using the associated community name.

When clients are defined within a community, only those clients are granted access to the managed objects using that community string.

If no clients are defined within a community, any SNMP manager that requests access using that community name is granted access to the entire MIB collection on the Secure Router.

The level of access granted to community clients is determined by the configured access privileges associated with a community.

SNMP traps

A trap is an unsolicited notification sent to an SNMP management station by an agent. The Secure Router supports a maximum of ten trap-hosts.

The SNMPV1 and SNMPV2c traps in the Secure Router 2330/4134 supports T1/E1 and T3/E3 (SR4134 only) interfaces for the list of alarms as follows:

- RAIS alarm
- RRAI alarm
- RLOS alarm
- RLOF alarm
- TAIS alarm
- TRAI alarm

Trap source IP address

SNMPv1 and SNMPv2c trap Protocol Data Units (PDU) include the trap source IP address field. By default, the trap source IP address is 0.0.0.0. However, the IP address of configured interface is accepted as trap source IP address with the limitation of IPv4 address.

SNMP MIB support

The Secure Router supports various SNMP standards defined by the RFC documents published by the Internet Engineering Task Force (IETF). For a list of supported SNMP standards, see "Supported SNMP standards and standard MIBs" (page 15).

You can download supported standard MIBs (RFC documents) from the Internet Engineering Task Force web site at www.ietf.org.

The Secure Router also supports a set of enterprise-defined MIBs. For a list of the supported Nortel enterprise-specific MIBs , see "Supported enterprise-specific MIBs" (page 19).

Supported SNMP standards and standard MIBs

This section provides a list of SNMP standards and the standard MIBs supported on the Secure Router. The following list identifies the tables and groups supported for each MIB. For more information about each MIB, see the RFC.

- RFC 1155—*Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1157—*A Simple Network Management Protocol (SNMP)*

- RFC 1213—*Management Information Base for Network Management of TCP/IP-based internets: MIB-II*
- RFC 1215—*Convention for defining Traps for use with the SNMP*
- RFC 1315—*Management Information Base for Frame Relay DTEs*
- RFC 1406—*Definitions of Managed Objects for the DS1 and E1 Interface Types*
- RFC 1407—*Definitions of Managed Objects for the DS3/E3 Interface Type*
- RFC 1471—*The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol*
- RFC 1473—*The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol*
- RFC 1493—*Definitions of Managed Objects for Bridges*
- RFC 1657—*Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*
- RFC 1724—*RIP Version 2 MIB Extension*
- RFC 1757—*Remote Network Monitoring Management Information Base*
    - statistics group, history group, alarms group, events group
- RFC 1850—*OSPF Version 2 Management Information Base*
- RFC 1902—*Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1903—*Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 2096— *IP Forwarding Table MIB*
- RFC 2115—*Management Information Base for Frame Relay DTEs Using SMIv2*
- RFC 2127—*ISDN Management Information Base using SMIv2*
    - isdnMibBearerGroup, isdnMibSignalingGroup, isdnMibBasicRate Group
- RFC 2206—*RSVP Management Information Base using SMIv2*
- RFC 2618—*RADIUS Authentication Client MIB*
- RFC 2620—*RADIUS Accounting Client MIB*
- RFC 2674—*Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions*

- RFC 2787—*Definitions of Managed Objects for the Virtual Router Redundancy Protocol*
- RFC 2954—*Definitions of Managed Objects for Frame Relay Service*
- RFC 3020—*Definitions of Managed Objects for Monitoring and Controlling the UNI/NNI Multilink Frame Relay Function*
- *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)* (draft-ietf-mpls-ldp-mib-14.txt)
- *Definitions of Textual Conventions for Multiprotocol Label Switching (MPLS) Management* (draft-ietf-mpls-tc-mib-10.txt)
- *Dynamic Host Configuration Protocol (DHCP) Server MIB* (draft-ietf-dhc-server-mib-06.txt)
- *Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base* (draft-ietf-mpls-ftn-mib-09.txt)
- *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base* (draft-ietf-mpls-lsr-mib-14.txt)
- *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base* (draft-ietf-mpls-te-mib-14.txt)

Supported standard MIBs

The Secure Router supports the standard MIBs described in “Supported standard MIBs” (page 17). All MIBs are SMIv2 compliant.

Table 1
Supported standard MIBs

MIB name	Description
PPP-LCP-MIB.mib	Defines the Managed Objects for the Link Control Protocol of the Point-to-Point Protocol.
PPP-IP-NCP-MIB.mib	Defines the Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol.
VRRP-MIB.mib	Defines the Managed Objects for the Virtual Router Redundancy Protocol.
IANAifType-MIB.mib	Defines the enumerated values of the ifType object from the IANAifType textual convention.
IF-MIB.mib	Defines the Interfaces Group MIB using SMIv2.
ISDN-MIB.mib	Defines ISDN Management Information Base using SMIv2.
DIAL-CONTROL-MIB.mib	Defines the Dial Control Management Information Base using SMIv2.

MIB name	Description
RADIUS-AUTH-CLIENT-MIB.mib	Defines the RADIUS Authentication Client MIB.
RADIUS-ACC-CLIENT-MIB.mib	Defines the RADIUS Accounting Client MIB.
MAU-MIB.mib	Defines the Managed Objects for IEEE 802.3 Medium Attachment Units.
EtherLike-MIB.mib	Defines the Managed Objects for the Ethernet-like Interface Types.
INET-ADDRESS-MIB.mib	Defines the Textual Conventions for Internet Network Addresses.
INTEGRATED-SERVICES-MIB.mib	Defines the Integrated Services Management Information Base using SMIv2.
BGP4-MIB.mib	Defines the Managed Objects for BGP-4.
BRIDGE-MIB.mib	Defines the Managed Objects for Bridges.
P-BRIDGE-MIB.mib	Defines the Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions.
RIPv2-MIB.mib	Defines the Extension of RIP Version 2 MIB.
DIFFSERV-DSCP-TC-MIB.mib	Defines the Textual convention for Differentiated Services Architecture.
DIFFSERV-MIB.mib	Defines the Management Information Base for the Differentiated Services Architecture.
DVMRP-STD-MIB.mib	Defines the Distance-Vector Multicast Routing Protocol MIB.
IEEE8021-PAE-MIB.mib	Defines the Dot1x MIB.
MPLS-TC-STD-MIB.mib	Defines the Textual Conventions for Multiprotocol Label Switching (MPLS) Management.
MPLS-TE-STD-MIB.mib	Defines the MPLS Traffic Engineering (TE) MIB.
MPLS-FTN-STD-MIB.mib	Defines the MPLS Forwarding Equivalence Class to Next Hop Label Forwarding Entry (FEC-to-NHLFE) MIB.
MPLS-LSR-STD-MIB.mib	Defines the MPLS Label Switching Router (LSR) MIB.
MPLS-LDP-STD-MIB.mib	Defines the Managed Objects for the MPLS and Label Distribution Protocol (LDP) MIB.
OSPF-MIB.mib	Defines the OSPF Version 2 MIB.
OSPFV3-MIB.mib	Defines the OSPF Version 3 MIB.
OSPF-TRAP-MIB.mib	Defines the OSPF Trap MIB.

Supported enterprise-specific MIBs

The Secure Router supports the Nortel enterprise-specific MIBs described in Table 2 "Supported enterprise-specific MIBs" (page 19). All MIBs are SMIv2 compliant.

Table 2
Supported enterprise-specific MIBs

MIB name	Description
BUNDLE-MIB.mib	Defines objects related to bundle and link configuration.
CHASSIS-MIB.mib	Defines objects related to chassis serial number and model number.
CONFIG-MGMT-MIB.mib	Defines objects related to saving configurations for network.
DSX-TC-MIB.mib	Defines textual conventions for DSX MIBs. This MIB should be compiled before any other DSX MIBs. This MIB does not contain any objects that can be used for management operations.
DSX-TE1-MIB.mib	Defines objects for interface cards that support TE1. These include configuration and statistics for ANSI/ATT/IETF and USER. These objects only pertain to Layer 1.
DSX-TE3-MIB.mib	Defines objects for interface cards that support TE3. These include configuration and statistics for ANSI/IETF and USER. These objects only pertain to Layer 1.
ENVIRONMENT-MIB.mib	Defines environment-related objects, for example, temperature and fans.
FR-MIB.mib	Defines objects related to configuration and statistics for Frame Relay and MFR bundles.
GENERIC-HDLC-MIB.mib	Defines objects related to configuration and statistics for generic HDLC bundles.
IP-MIB.mib	Defines objects related to IP addressable interfaces and static routes.
PPP-MIB.mib	Defines objects related to PPP/MLPPP bundles for configuration and statistics.
SNMP-MIB.mib	Defines objects related to SNMP community and trap_host configurations
SYSTEM-MIB.mib	Defines objects related to system information, for example, IP address, host name, and DNS
NORTEL-MIB.mib	Defines the Nortel Networks top-level MIB
ENTERPRISE-DATA-MIB.mib	Defines the EDN enterprise Data root MIB
QOSSLA-MIB.mib	Defines the QOS SLA notifications

SNMP statistics

The Secure Router supports operational show commands that provide extensive statistical information about the SNMP data stream. For detailed statistics collection on Ethernet interfaces, the Secure Router uses the remote monitoring (RMON) standard. For more information on RMON, see "Remote monitoring" (page 20).

SNMP network management connectivity

Network management connectivity for the SNMP service is established by using the command line interface (CLI). For more information about how to configure a management interface, see *Nortel Secure Router 2330/4134 Commissioning* (NN47263-302) .

Remote monitoring

Remote monitoring (RMON) is an industry standard, RFC 1757, that uses SNMP to monitor Ethernet LAN segments and provide network statistics. Configure RMON on the Secure Router to obtain information about the Layer 1 and Layer 2 environments. RMON collects information about physical connections, performance, and configuration. Use RMON to detect a sudden change in network traffic and solve a problem before it becomes critical.

RMON runs continuously even when there are no clients checking statistics. You can configure RMON to send trap messages when an error condition occurs that exceeds a configured maximum threshold.

An RMON agent is a noninteractive monitor on a LAN segment. The agent reads and copies each frame sent on the local LAN and updates counters based on the contents of the frames. The agent saves the captured information until a remote managing station requests it. The managing station is not actively involved in the data collection.

You cannot configure RMON on the management port. You can configure RMON on the following Ethernet ports:

- Chassis Ethernet ports
- 10-port GE LAN card Ethernet ports
- 24-port POE LAN card Ethernet ports
- 24-port FE LAN card Ethernet ports
- 44-port GE LAN card Ethernet ports

RMON MIB groups

The Secure Router supports the MIB groups identified in Table 3 "Supported RMONv1 MIB groups" (page 21). Only SNMP get operations on the RMON MIB are supported. Set operations are not supported.

Table 3
Supported RMONv1 MIB groups

RMON group	Function	Elements
Statistics	Contains statistics measured by the probe for each monitored interface on the device.	Packets dropped and sent, bytes sent (octets), broadcast and multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores them for later retrieval.	Sample period, number of samples, and items sampled.
Alarm	Takes periodic statistical samples from variables in the probe and compares them with configured thresholds. If the monitored variable exceeds a threshold, an event is generated.	Alarm type, interval, starting threshold, and stop threshold. Includes the alarm table and requires the implementation of the event group.
Event	Controls the generation and notification of events from the device.	Event type, description, and last time the event sent.

Performance considerations

Management traffic is a concern when you use remote monitoring. When you monitor at finer levels of granularity, there are a number of interactions between the application and the RMON agent that raise the possibility of congestion caused by the increased management traffic.

If you collect statistics infrequently, the data collection does not use significant bandwidth but it offers little valuable information. Keep timing and traffic levels in mind when you configure remote monitoring.

RMON agents are economical in their use of network bandwidth. Based on 10-second polling intervals, traffic loads for common RMON functions such as providing a summary screen of activity, network statistics, or host statistics consume a small fraction of 1% of Ethernet bandwidth. As a result, RMON agents typically do not affect normal Ethernet segment activities.

Dynamic host configuration protocol version 4

The Dynamic Host Configuration Protocol version 4 (DHCPv4) provides the configuration parameters and IP addresses to the Internet Hosts. DHCPv4 is built on a client-server model. The DHCPv4 servers allocate network addresses and configuration parameters to dynamically configured DHCPv4 clients. The communication between DHCPv4 clients and DHCPv4 servers passes through Bootstrap Protocol (BOOTP) relay agent.

The DHCPv4 server provides the following parameters to the DHCPv4 client:

- IP address
- Default gateway
- Domain Name Server (DNS) address
- NetBIOS setting

DHCPv4 implementation

The DHCPv4 server and BOOTP relay implementation need the following modules:

- “Remote Database” (page 22)
- “DHCPv4 server address pool” (page 23)
- “DHCPv4 relay functionality” (page 23)

Remote Database

The remote database maintains current bindings and the leases for the DHCPv4 server, that are allocated to the clients. This database also times out the leases and ensures that there is no conflict in address assignments. The storage happens in memory or on to the flash for permanent store or to a remote host URL location using FTP. Storing the lease database in the flash is not recommended due to restricted file system limitations. It is recommended to store the lease database on to a remote host by configuring a URL location. The DHCPv4 server uses ftp to transfer the leases to the URL location and on every reboot restores the leases from this URL location. The maximum number of leases that the DHCPv4 server can support is limited to the amount of memory needed to store a lease record and the amount of system memory available. It is limited to have a total 4000 leases as the maximum upper limit for 256 MB of system memory.

DHCPv4 server address pool

The DHCPv4 server stores the DHCP parameters for the client in server pools. Each pool has an associated name and serves a specific subnet. The parameters like IP address range, lease times, MAC address, and client IDs are associated with each pool entry. These entries are configured for manual or dynamic binding.

DHCPv4 relay functionality

The DHCPv4 relay functionality is used to relay the DHCPv4 client requests to the DHCPv4 server and get the DHCP parameters. The DHCPv4 server accepts relayed requests only from the relay servers configured.

DHCPv4 over VLAN

With Release 10.2 and later, you can configure DHCP server and DHCP Relay on VLAN interfaces.

Dynamic host configuration protocol version 6

The Dynamic Host Configuration Protocol version 6 (DHCPv6) supports Internet Protocol version 6 (IPv6). DHCPv6 enables DHCPv6 servers to transmit configuration parameters to IPv6 nodes using extensions. It automatically allocates reusable network addresses and reduces the cost of managing IPv6 nodes in environments where administrators require more control over the allocation of IP addresses. DHCPv6 server manages network resources such as IP addresses, Network Time Protocol (NTP), Domain Name System (DNS), and other server addresses at a centralized location. DHCP relay facilitates initial communication between the DHCPv6 server and the DHCPv6 client when they are on different links. DHCPv6 model works across relays without a DHCPv6 server on each link.

Autoconfiguration

Autoconfiguration is a mechanism that does not require any manual intervention to configure a host in a network environment.

Following are the types of autoconfiguration methods:

- “Stateless address autoconfiguration” (page 23)
- “Stateful address autoconfiguration” (page 24)

Stateless address autoconfiguration

The stateless address autoconfiguration does not require a manually configured server but enables IPv6 hosts to configure the IP addresses using a local IPv6 router. However, this method lacks network access control capabilities and manages only IP addressing.

Stateful address autoconfiguration

The stateful autoconfiguration involves a client and a server. When an unconfigured node is unable to locate router advertisements on the network it uses DHCPv6 to configure an interface.

DHCPv6 UDP ports

DHCPv6 uses the following Internet User Datagram Protocol (UDP) ports:

- "546" (page 24)
- "547" (page 24)

546

DHCPv6 servers use 546 client port as the destination port to send messages to clients and relays. In addition, the relays or agents use this port as the destination port for messages sent to the clients.

547

DHCPv6 clients use 547 agent port as the destination port to send messages to agents or relays. In addition, relays use this port as the destination port for messages sent to the servers.

Multicast address

DHCPv6 uses the following multicast addresses:

- "DHCP agent address FF02::1:2" (page 24)
- "DHCP server address FF05::1:3" (page 24)

DHCP agent address FF02::1:2

DHCP clients use this link-scoped multicast address to communicate with the on-link agent. All agents within the same DHCP domain belong to this multicast group.

DHCP server address FF05::1:3

DHCP clients or relays use this site-scoped multicast address to communicate with servers within the site in one of the following scenarios:

- When the client or relay sends messages to all servers.
- When the client or relay does not know the server's unicast address.

Client/Server operation

DHCPv6 servers and DHCPv6 clients on the same link communicate directly with each other. DHCPv6 requires relays to be set up on the client's link when the client and the server are on different links. Relays receive messages from the client and forward them to a set of DHCPv6 servers.

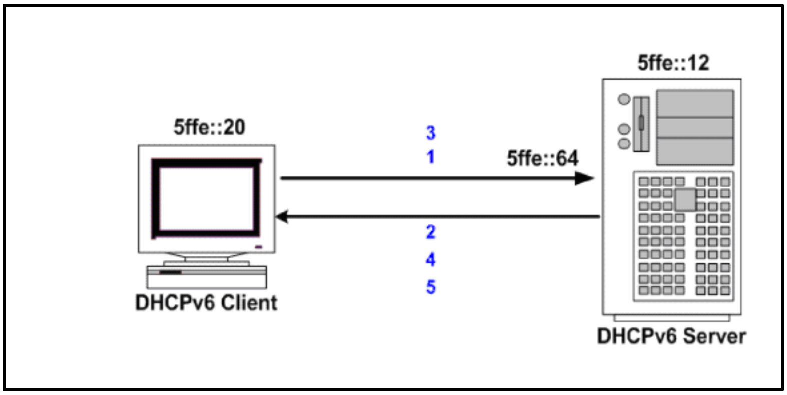
- "When the client and the server are on the same link" (page 25)
- "When the client and the server are on different link" (page 26)

When the client and the server are on the same link

The client and the server on the same link communicate with each other as follows:

1. The client sends a SOLICIT message to locate suitable servers.
2. Multiple servers respond to the SOLICIT message by sending a DHCP ADVERTISE message to the client.
3. The client sends a DHCP REQUEST message to the DHCPv6 server that has the highest preference value.
4. The server responds to the client's message by sending a DHCP REPLY message. The DHCP REPLY message contains the IPv6 address and configuration parameters required by the client.
5. The client sends a DHCP RELEASE message to return one or more IPv6 addresses to the server when it has completed using an IPv6 address.

Figure 2
Client and server on same link

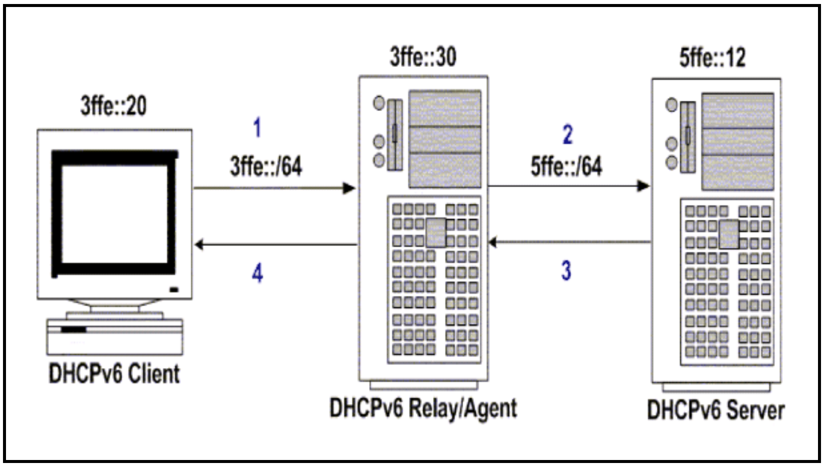


When the client and the server are on different link

The client and the server on different links communicate with each other as follows:

1. The client sends SOLICIT message to locate servers that are able to offer the required services.
2. The relay forwards the client’s message to servers by sending RELAY-FORWARD message.
3. The servers respond to the client’s message by sending a SERVER-FORWARD message.
4. The relay forwards the servers messages to the client by sending ADVERTISE messages.

Figure 3
Client and server on different link



Remote OAM access and network management protocols

The Secure Router supports a variety of remote-access and network management protocols for system operation, maintenance, and administration (OAM) tasks. This section provides information about the following topics:

- “FTP” (page 26)
- “TFTP” (page 27)
- “Telnet” (page 27)

FTP

The Secure Router supports the File Transfer Protocol (FTP) as documented in RFC 959. FTP is not a secure file transfer protocol. FTP does not encrypt transferred data. Use FTP access only after you determine that it is safe to do so in your specific network scenario. If you need to transfer data over a network or network segment that is not secure, use the Secure FTP capability provided by the SSH service. For more information on SSH, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

The SR2330/4134 supports a maximum of 4 FTP sessions at a time. FTP is disabled by default on the SR2330/4134.

TFTP

The Trivial File Transfer Protocol (TFTP) (RFC 1350) is a version of the FTP but does not use a password. TFTP is not a secure file transfer protocol. Use TFTP access only after you determine that it is safe to do so in your specific network scenario. If you need to transfer data over a network or network segment that is not secure, use the Secure FTP capability provided by the SSH service.

For more information on SSH, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600) .

The SR2330/4134 supports a maximum of 4 TFTP sessions at a time and more than 32MB of image downloading is not supported. TFTP is disabled by default on the SR2330/4134.

Telnet

The Secure Router supports Telnet (RFC 854). Use a Telnet session to log on to the Secure Router to perform system OAM tasks. Telnet is not a secure remote access protocol; data transmitted in a Telnet session is not encrypted and passwords are transmitted in clear text.

Use Telnet only after you determine that it is safe to use it in your specific network scenario. If your management network is not secure, use the Secure Shell (SSH) protocol to log on remotely. For more information on SSH, see *Nortel Secure Router 2330/4134 Security — Configuration and Management* (NN47263-600).

The SR2330/4134 supports a maximum of 16 Telnet sessions, if no console session is active. With an active console session, a maximum of 15 Telnet sessions is supported. Telnet is disabled by default on the SR2330/4134.

SNMP configuration

Configure the Simple Network Management Protocol (SNMP) on the Nortel Secure Router 4134.

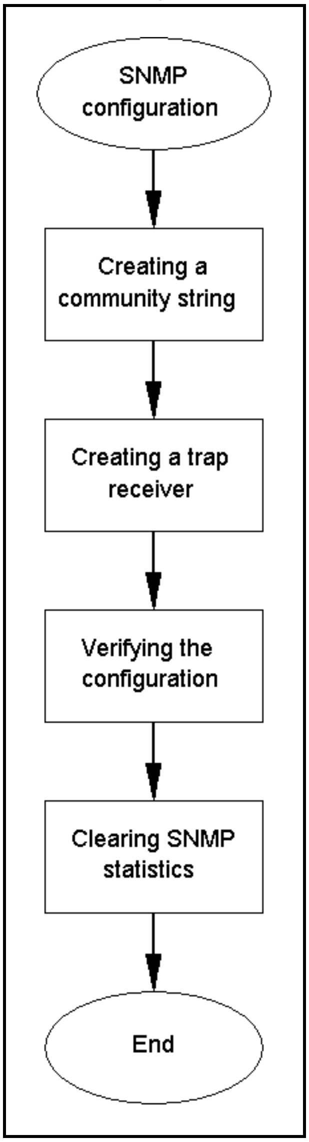
Prerequisites to SNMP configuration

- Before you perform SNMP configuration ensure that the interfaces are functional.
- Ensure that proper routes are added to the manager and the agent, if the management station is in a different network.
- Ensure that the MIB file is uploaded to the management station.

SNMP configuration procedures

This task flow shows you the sequence of procedures you use to configure SNMP on the Nortel Secure Router 4134. To link to any procedure, go to "SNMP configuration procedure navigation" (page 30)

Figure 4
SNMP configuration procedures



SNMP configuration procedure navigation

- "Creating a community string" (page 33)
- "Creating a trap receiver" (page 34)
- "Verifying the configuration" (page 36)
- "Clearing SNMP statistics" (page 37)

Enabling SNMP server

Enable SNMP server to access next-level commands for configuring the MIB database for all systems.

Procedure steps

Step	Action
1	To enter configuration mode, enter: `configure terminal`
2	To select SNMP server configuration, enter: `snmp-server`
3	To enable the SNMP server, enter: `snmp-enable`

--End--

Configuring SNMP source

Configure the SNMP source IP address.

Procedure steps

Step	Action
1	To enter configuration mode, enter: `configure terminal`
2	To select SNMP server configuration, enter: `snmp-server`
3	To configure the SNMP source, enter: `snmp-source <IP address>`

--End--

Table 4
Variable definitions

Variable	Value
<IP address>	SNMP source IP address

Configuring SNMP server chassis ID

Configure SNMP server chassis ID to name the SNMP host system.

Procedure steps

Step	Action
1	To enter configuration mode, enter: `configure terminal`
2	To select SNMP server configuration, enter: `snmp-server`
3	To configure the SNMP server chassis ID: `chassis-id <name>`

--End--

Table 5
Variable definitions

Variable	Value
<name>	name of the host system

Configuring SNMP contact

Configure SNMP contact to specify a contact person for the SNMP MIB.

Procedure steps

Step	Action
1	To enter configuration mode, enter: `configure terminal`
2	To select SNMP server configuration, enter: `snmp-server`
3	To configure SNMP contact, enter: `contact <“name”>`

--End--

Table 6
Variable definitions

Variable	Value
<“name”>	name of the person to contact regarding the SNMP MIB. Use up to eight characters and enclose in quotes.

Configuring SNMP location

Configuring SNMP location defines the SNMP host system location.

Procedure steps

Step	Action
1	To enter configuration mode, enter: `configure terminal`
2	To select SNMP server configuration, enter: `snmp-server`
3	To configure SNMP location, enter: `location <"string">`

--End--

Table 7
Variable definitions

Variable	Value
<"string">	location of the host system, specified in quotation marks.

Creating a community string

Create the community string to configure the secure router for performing the SNMP operation.

You can configure a maximum of 10 SNMP community strings.

Procedure steps

Step	Action
1	To enter configuration mode, enter: `configure terminal`
2	To select SNMP server configuration, enter: `snmp-server`
3	To create a community string: `community <string> [access_privilege {ro	rw}]`

--End--

Table 8
Variable definitions

Variable	Value
<string>	Specifies a new community string for SNMP configuration.

Creating trap source

Create trap source to configure SNMP trap messages to be sent to a specific IP address or the system default address.

Procedure steps

Step	Action

1 To enter configuration mode, enter:

```
configure terminal
```

2 To select SNMP server configuration, enter:

```
snmp-server
```

3 Create trap source

```
trap-source host <IP address>
```

--End--

Table 9
Variable definitions

Variable	Value
<IP address>	trap source IP address

Creating a trap receiver

Create a trap receiver or trap host to receive the trap/notification.

You can configure a maximum of 10 trap hosts.

Procedure steps

Step	Action

1 To enter configuration mode, enter:

```
configure terminal
```

2 To select SNMP server configuration, enter:

```
snmp-server
```

3 Create a trap receiver:

```
trap-host <ip address> [community string]
```

--End--

Table 10
Variable definitions

Variable	Value
<ip address>	is the IP address of the trap host. Use version 4 or version 6 IP address.

Enabling traps

Use this procedure to enable traps.

Procedure steps

Step	Action

1 To enter configuration mode, enter:

```
configure terminal
```

2 To select SNMP server configuration, enter:

```
snmp-server
```

3 To enable specific traps, enter

```
[no] enable traps
{bgp |
bundle |
cfm |
config |
enable-all|
environment |
frame_relay|
ospf |
snmp |
sntp |
system |
vrrp}
```

--End--

Table 11
Variable definitions

Variable	Value
[no]	Disables the specified trap.

Table 11
Variable definitions (cont'd.)

bgp	Enables or disables BGP-related traps.
bundle	Enables or disables bundle group of traps.
cfm	Enables or disables CFM group of traps.
config	Enables or disables Configuration group traps.
enable-all	Enables or disables all traps.
environment	Enables or disables Environment group traps.
frame_relay	Enables or disables Frame Relay group related traps.
ospf	Enables or disables OSPF related traps.
snmp	Enables or disables SNMP group related traps.
sntp	Enables or disables SNTP client traps.
system	Enables or disables system group traps.
vrrp	Enables or disables VRRP group traps.

Verifying the configuration

Verify the community string and trap host configuration.

Procedure steps

Step	Action
1	Display the configured SNMP community: `show snmp communities`
2	Display the configured SNMP source address: `show snmp snmp-source`
3	Display SNMP generic information: `show snmp status`
4	Display the configured trap hosts: `show snmp trap-host`
5	Display the configured trap source address:

```
show snmp trap-source
```

6 Display the configured trap version:

```
show snmp trap-version
```

7 Display the list of traps enabled or disabled:

```
show snmp traps
```

--End--

Clearing SNMP statistics

Clear the SNMP statistics to release the events generated by the agent.

Procedure steps

Step	Action
1	Clear SNMP statistics:

```
clear snmp_stats
```

--End--

RMON configuration

Configure the remote monitoring (RMON) feature on the Nortel Secure Router 4134.

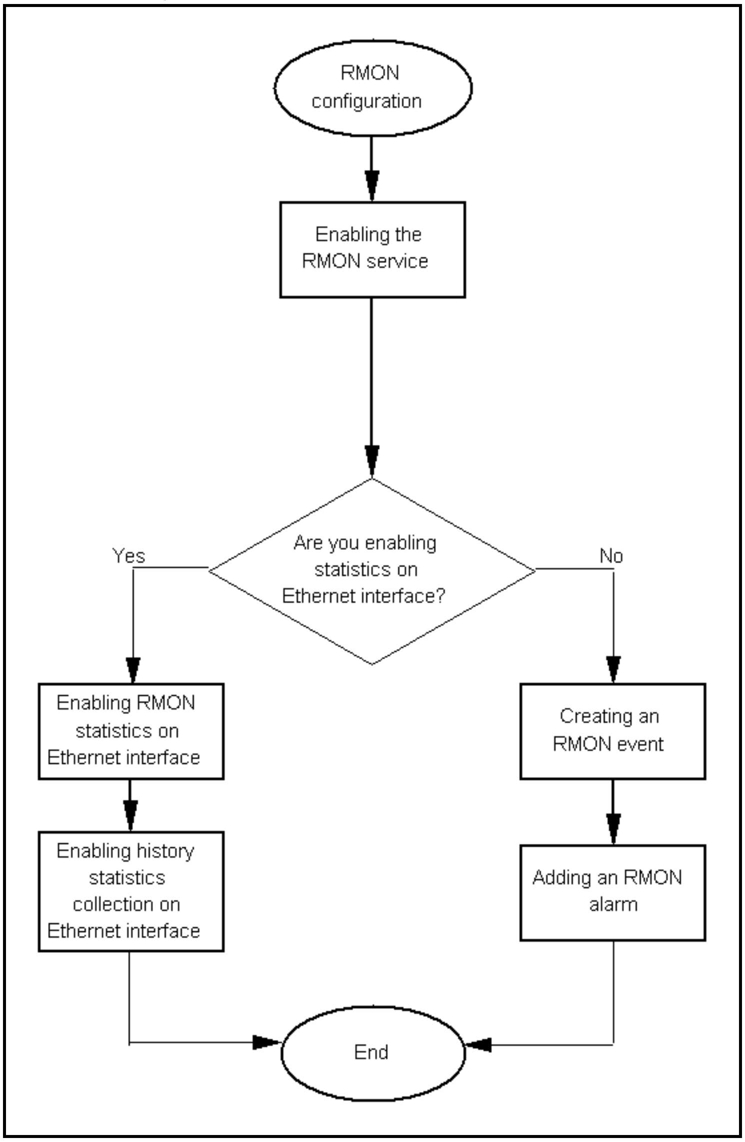
Prerequisites to RMON configuration

- Before you configure RMON, you must configure at least one Ethernet interface for monitoring. For more information on configuring Ethernet interfaces, see *Nortel Secure Router 2330/4134 Configuration — Ethernet Layer 2* (NN47263-501) .
- Ensure that the MIB file is uploaded to the management station.

RMON configuration procedures

This task flow shows you the sequence of procedures you use to configure RMON on the Nortel Secure Router 4134. To link to any task, see “RMON configuration procedure navigation” (page 40)

Figure 5
RMON configuration procedures


RMON configuration
Enabling the RMON service
Are you enabling statistics on Ethernet interface?
Yes
No
Enabling RMON statistics on Ethernet interface
Enabling history statistics collection on Ethernet interface
Creating an RMON event
Adding an RMON alarm
End

RMON configuration procedure navigation

- “Enabling the RMON service” (page 41)
- “Enabling RMON statistics on Ethernet interface” (page 41)
- “Enabling history statistics collection on Ethernet interface” (page 42)
- “Creating an event” (page 44)
- “Adding an alarm” (page 45)

Enabling the RMON service

Enable the RMON service globally on the Secure Router to collect Ethernet statistics.

Procedure steps

Step	Action
1	To enable the configuration mode, enter:

```
configure terminal
```

Step	Action
2	Enable the RMON service:

```
rmon enable
```

On the Secure Router, use the **`no`** operator to disable a feature. For example, to disable the RMON service, the command is **`no rmon enable`**.

--End--

Example of enabling the RMON service

Step	Action
1	Enable the RMON service globally:

```
SR/configure# rmon enable
```

--End--

Enabling RMON statistics on Ethernet interface

Configure RMON on an Ethernet port to collect statistics for that port. You can collect information on the packet volumes, broadcast and unicast traffic, packet size distributions, and errors.

Prerequisites

- The Ethernet interface is configured. For information on configuring Ethernet interfaces, see *Nortel Secure Router 2330/4134 Configuration — Ethernet Layer 2* (NN47263-501).

Procedure steps

Step	Action
1	To enter the configuration mode, enter:

```
configure terminal
```

2 Enable statistics collection:

```
rmon statistics ethernet<slot/port> [<owner>]
```

On the Secure Router, use the `no` operator to disable a feature. For example, to disable statistics collection, the command is `no rmon statistics ethernet<slot/port> [<owner>]`.

--End--

Table 12
Variable definitions

Variable	Value
<owner>	specifies the owner of the RMON port. The default owner is CLI-Manager.
<slot/port>	identifies the Ethernet interface on which to enable statistics collection. Identify the interface using slot/port.

Example of enabling Ethernet statistics collection

Step **Action**

1 Enable Ethernet statistics collection on Ethernet interface slot 0, port 2:

```
SR/configure/rmon# statistics ethernet0/2
```

--End--

Enabling history statistics collection on Ethernet interface

Enable collection of Ethernet history statistics to compare behavior and build baselines and trending information. The probe collects the statistics at specified intervals and saves a specified number of samples for later retrieval. You can configure a maximum of 10 history controls per interface.

Prerequisites

- The Ethernet interface is configured. For information on configuring Ethernet interfaces, see *Nortel Secure Router 2330/4134 Configuration — Ethernet Layer 2* (NN47263-501) .
- Ethernet statistics collection is enabled for the interface.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	Enable collection of Ethernet history statistics: `rmon history ethernet<slot/port> [<interval>] [<buckets>] [<owner>]` On the Secure Router, use the `no` operator to disable a feature. For example, to disable history statistics collection, the command is `no rmon history ethernet<slot/port> [<interval>] [<buckets>] [<owner>]`.

--End--

Table 13
Variable definitions

Variable	Value
<buckets>	specifies the number of samples to maintain. The default value is 50 and the maximum number is 100.
<interval>	specifies the interval, in seconds, at which to collect statistics. The default value is 1800 seconds.
<owner>	specifies the owner of the RMON port. The default owner is CLI-Manager.
<slot/port>	identifies the Ethernet interface on which to enable statistics collection. Identify the interface using slot/port.

Example of collecting Ethernet history statistics

Step	Action
1	Collect Ethernet history statistics on the Ethernet interface in slot 1, port 2 with an interval of 100 and buckets set to 20: `SR/configure# rmon history ethernet1/2 100 20`

--End--

Creating an event

Create an event to control the sending of SNMP trap messages to the remote client. The probe can signal the occurrence of many types of events such as exceeded thresholds or captured packets.

The maximum number of events is 100. The maximum number of RMON logs on the Router is 10000.

Procedure steps

Step	Action
1	To enter the configuration mode, enter:

```
configure terminal
```

Step	Action
2	Create an event:

```
rmon event <index> <type> [community <community>]
[description <description>] [owner <owner>]
```

On the Secure Router, use the `no` operator to disable a feature. For example, to disable an event, the command is `no rmon event <index> <type> [community <community>] [description <description>] [owner <owner>]`.

--End--

Table 14
Variable definitions

Variable	Value
<community>	specifies an SNMP community name if <type> is set to trap (2) or log-trap (3)
<description>	specifies a text description for the event. The value must be specified in quotation marks (" ").
<index>	specifies an index number for this event. The maximum number of events is 100
<owner>	specifies the owner of the RMON event
<type>	Specifies the type of event as one of the following: • log (1) • trap (2) • log-trap (3)

Example of creating an event

Step	Action
1	Create an event to log information:

```
SR/configure# rmon event 2 log description "event
2" owner Manager-2
```

--End--

Adding an alarm

Add an alarm to set thresholds to signal when values require further attention. The maximum number of alarms is 100.

Prerequisites

- An RMON event exists in the system.

Procedure steps

Step	Action
1	To enter the configuration mode, enter:

```
configure terminal
```

Step	Action
2	Add an alarm:

```
rmon alarm <index> <variable> <interval> <rthreshold>
<fthreshold> <revent> <fevent> [<type>] [<startup>]
[<owner>]
```

On the Secure Router, use the `no` operator to disable a feature. For example, to disable an event, the command is `no rmon alarm <index> <variable> <interval> <rthreshold> <fthreshold> <revent> <fevent> [<type>] [<startup>] [<owner>]`.

--End--

Table 15
Variable definitions

Variable	Value
<fevent>	specifies the index number of the RMON event to trigger when the value is lower than the falling threshold

Table 15
Variable definitions (cont'd.)

Variable	Value
<fthreshold>	sets the falling alarm threshold. If the value is lower than this threshold, it causes a falling alarm
<index>	specifies an index number for this alarm. The maximum number of alarms is 100
<interval>	specifies the interval, in seconds, at which to poll
<owner>	specifies the owner of the RMON alarm. The default owner is CLI-Manager
<revent>	specifies the index number of the RMON event to trigger when the value is higher than the rising threshold
<rthreshold>	sets the rising alarm threshold. If the value exceeds this threshold, it causes a rising alarm
<startup>	specifies the type of alarm generated when the event first occurs: rising, falling, or rise_fall. The default is rise_fall
<type>	specifies the sampling method as either absolute or delta (the difference). The default is absolute
<variable>	specifies the MIB object to monitor using ASN.1. ASN.1 describes a managed object in machine-independent format

Example of adding an alarm

Step	Action
1	Create a rising alarm to monitor the delta every 100 seconds:

```
SR/configure# rmon alarm 12 1.3.6.1.2.1.5.1.0
100 2300 4300 1 3 type delta startup rising owner
Manager-1
```

--End--

Clearing the event log

Use this procedure to clear the event log.

Procedure steps

Step	Action
1	To clear the event log, enter: `clear event_log`

--End--

Ethernet statistics display using RMON

Monitor Ethernet statistics to view configuration information and collected data to identify trends and potential network issues.

Monitoring Ethernet statistics procedure navigation

- “Viewing collected statistics on a specific interface” (page 49)
- “Viewing history statistics” (page 50)
- “Viewing the history statistics configuration” (page 50)
- “Viewing configured alarms” (page 50)
- “Viewing events” (page 51)
- “Viewing logs” (page 51)

Viewing collected statistics on a specific interface

Display the collected statistics on a specific interface to display all the readings of the etherStats table of the RMON MIB.

Procedure steps

Step	Action
1	Display statistics for a specific interface:

```
show rmon statistics ethernet<slot/port>
```

--End--

Table 16
Variable definitions

Variable	Value
<slot/port>	identifies the Ethernet interface on which to enable statistics collection. Identify the interface using slot/port

Viewing history statistics

Display the history statistics collected for a specific Ethernet interface.

Procedure steps

Step	Action
1	Display the history statistics:

```
show rmon ethernet_history ethernet<slot/port>
```

--End--

Table 17
Variable definitions

Variable	Value
<slot/port>	identifies the Ethernet interface on which to enable statistics collection. Identify the interface using slot/port

Viewing the history statistics configuration

Display the running configuration for collecting Ethernet history statistics on a specified Ethernet interface.

Procedure steps

Step	Action
1	Display the configuration:

```
show rmon history_control ethernet<slot/port>
```

--End--

Table 18
Variable definitions

Variable	Value
<slot/port>	identifies the Ethernet interface on which to enable statistics collection. Identify the interface using slot/port

Viewing configured alarms

View generic information for all configured alarms or detailed configuration for a specific alarm.

Procedure steps

Step	Action
1	View generic information for all configured alarms:

```
show rmon alarms
```

Step	Action
2	View more detailed information on a specific alarm from the output in step 1:

```
show rmon alarm <index>
```

--End--

Table 19
Variable definitions

Variable	Value
<index>	specifies the index number associated with the alarm

Viewing events

View events to display the configuration settings and the last time the event sent.

Procedure steps

Step	Action
1	View events:

```
show rmon events [<index>]
```

--End--

Viewing logs

View logs to display the time of the event and the event description.

Procedure steps

Step	Action
1	View logs:

```
show rmon logs
```

--End--

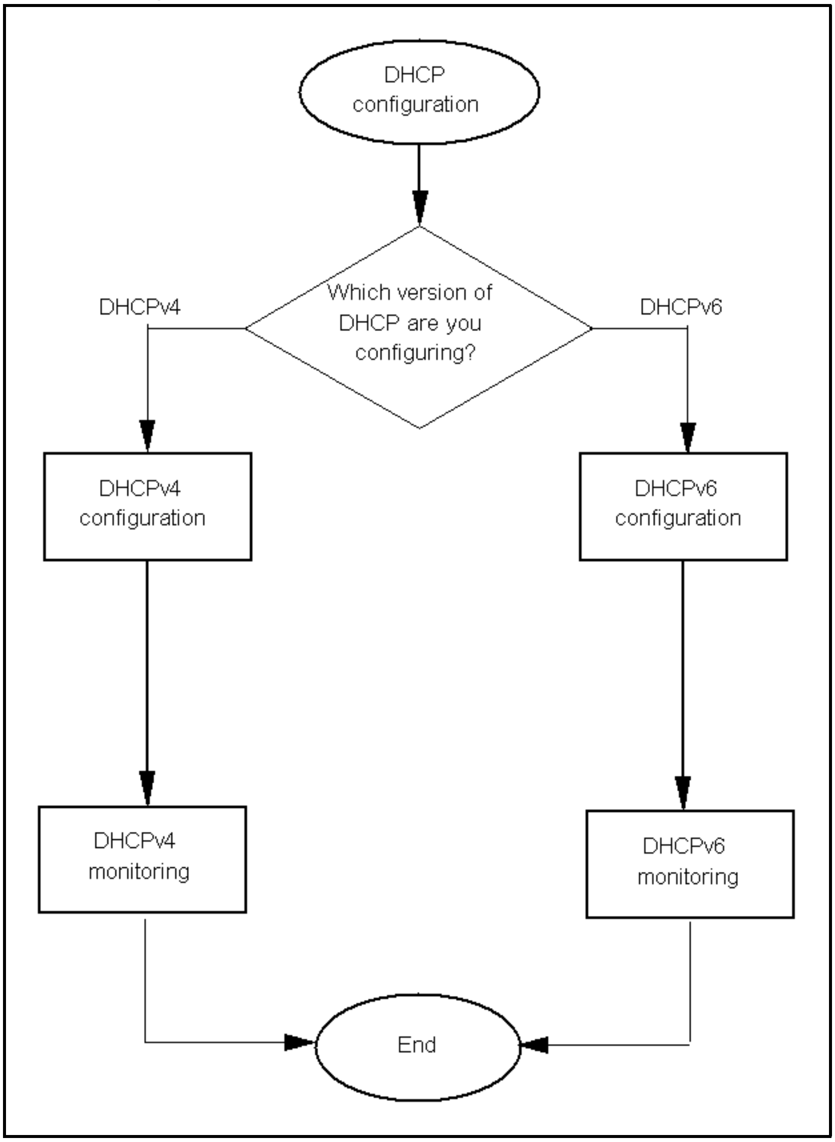
DHCP configuration

Configure and monitor DHCPv4 and DHCPv6 on the Nortel Secure Router 4134.

DHCP configuration tasks navigation

This work flow shows you the sequence of tasks you use to configure, monitor, and debug DHCP on the Nortel Secure Router 4134. To link to any task, see "DHCP configuration task navigation" (page 54)

Figure 6
DHCP configuration tasks



DHCP configuration task navigation

- “DHCPv4 configuration” (page 55)
- “DHCPv4 monitoring” (page 77)
- “DHCPv6 configuration” (page 81)
- “DHCPv6 monitoring” (page 87)

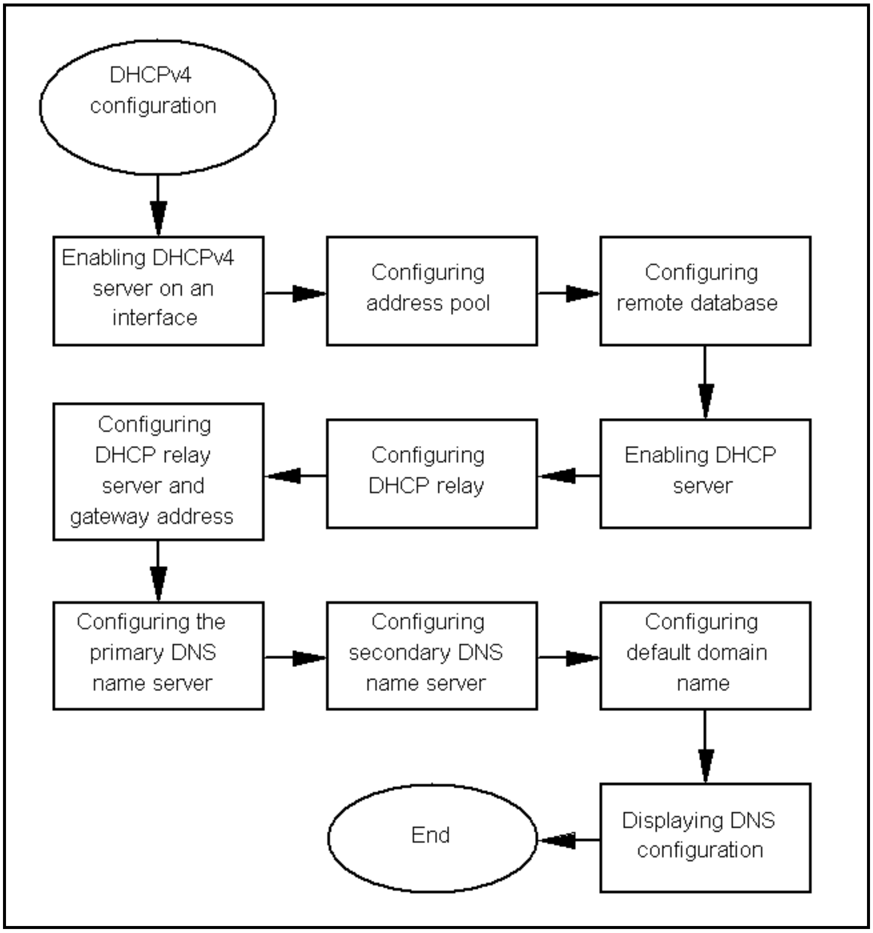
DHCPv4 configuration

Configure DHCP version 4 on the Nortel Secure Router 4134.

DHCPv4 configuration procedures

This task flow shows you the sequence of procedures you use to configure DHCPv4 on the Nortel Secure Router 4134. To link to any procedure, see "DHCPv4 configuration procedure navigation" (page 56)

Figure 7
DHCPv4 configuration procedures


DHCPv4 configuration
Enabling DHCPv4 server on an interface
Configuring address pool
Configuring remote database
Enabling DHCP server
Configuring DHCP relay
Configuring DHCP relay server and gateway address
Configuring the primary DNS name server
Configuring secondary DNS name server
Configuring default domain name
Displaying DNS configuration
End

DHCPv4 configuration procedure navigation

- “Enabling DHCPv4 server on an interface” (page 56)
- “Configuring DHCPv4 server address pool” (page 56)
- “Configuring remote database” (page 66)
- “Enabling DHCPv4 server” (page 66)
- “Configuring DHCP relay” (page 66)
- “Configuring DHCP relay server and gateway addresses” (page 67)
- “Configuring the primary DNS name server” (page 67)
- “Configuring the secondary DNS name server” (page 68)
- “Configuring the default domain name” (page 68)
- “Displaying DNS configuration” (page 68)

Enabling DHCPv4 server on an interface

Enable DHCPv4 server on an interface.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify DHCP configuration, enter: `ip dhcps`
3	To configure an interface to run the DHCP Server, enter: `interface {ethernet<slot/port>	<bundle-name>	vlan<vid>}`

--End--

Configuring DHCPv4 server address pool

Configure an address pool on DHCPv4 server.

Procedure steps

Step	Action
1	To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 Configure address pool:

```
pool <pool name>
```

--End--

Configuring the Nortel IP phone alternate VLAN ID for the address pool

Configure the Nortel IP phone alternate VLAN ID for the address pool.

Procedure steps

Step **Action**

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure alternate VLAN ID for the address pool, enter:

```
altvlan <0-65535>
```

--End--

Table 20
Variable definitions

Variable	Value
<0-65535>	Specifies the alternate VLAN ID value.

Configuring the Nortel Call Server name for the address pool

Configure the Nortel Call Server name for the address pool.

Procedure steps

Step **Action**

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure call server name for the address pool, enter:

```
callserver <A.B.C.D> [port <port>] [appserver
<A.B.C.D>] [svpserver <A.B.C.D>]
```

--End--

Table 21
Variable definitions

Variable	Value
callserver <A.B.C.D>	Specifies the call server IP address.
[port <port>]	Specifies the call server port. Range is 1024 - 65535 (default 4100).
[appserver <A.B.C.D>]	Specifies the application server IP address.
[svpserver <A.B.C.D>]	Specifies the spectraLink Voice Priority (SVP) server IP address.

Configuring the client ID for the address pool

Configure the client ID for the address pool.

Procedure steps

Step **Action**

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure Client ID for the address pool, enter:

```
clientid <client-id>
```

--End--

Table 22
Variable definitions

Variable	Value
<client-id>	Specifies the client ID in form of aa:bb:cc:dd:ee:ff.

Committing the address pool

Commit the current pool configuration.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To commit the address pool, enter:

```
commit
```

--End--

Configuring the default router address for the address pool

Configure the default router address for the address pool.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure the default router address for the address pool, enter:

```
default_router <A.B.C.D>
```

--End--

Table 23
Variable definitions

Variable	Value
<A.B.C.D>	Network number in A.B.C.D form.

Configuring the DNS server name for the address pool

Configure the DNS server name for the address pool.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure the DNS server name for the address pool, enter:

```
dnsserver <A.B.C.D>
```

--End--

Table 24
Variable definitions

Variable	Value
<A.B.C.D>	DNS server IP address.

Configuring the domain name for the address pool

Configure the domain name for the address pool.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure the domain name for the address pool, enter:

```
domain <domain>
```

--End--

Table 25
Variable definitions

Variable	Value
<domain>	Domain name string.

Configuring addresses to be excluded from address pool

Specify address ranges to be excluded from the address pool.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure addresses to be excluded from the pool, enter:

```
exclude-range <start-ip> <end-ip>
```

--End--

Table 26
Variable definitions

Variable	Value
<start-ip> <end-ip>	Specifies the starting and ending IP address range to exclude.

Configuring the host IP address for the address pool

Configure the host IP address for the address pool.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify DHCP configuration, enter: `ip dhcps`
3	To specify address pool configuration, enter: `pool <pool name>`
4	To configure the host IP address for the address pool, enter: `host <A.B.C.D> <mask>`

--End--

Table 27
Variable definitions

Variable	Value
<A.B.C.D> <mask>	Specifies the host IP address.

Configuring the hardware address for the address pool

Configure the hardware address for the address pool.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify DHCP configuration, enter: `ip dhcps`
3	To specify address pool configuration, enter: `pool <pool name>`
4	To configure the hardware address for the address pool, enter: `hwaddr <hwaddr>`

--End--

Table 28
Variable definitions

Variable	Value
<hwaddr>	Specifies the hardware address in the form of aa:bb:cc:dd:ee:ff.

Configuring the lease time for the address pool

Set the address lease time in seconds (default: 3600 seconds).

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify DHCP configuration, enter: `ip dhcps`
3	To specify address pool configuration, enter: `pool <pool name>`
4	To configure the lease time for the address pool, enter: `lease <0-4294967>`

--End--

Configuring the NetBIOS name server for the address pool

Configure the NetBIOS name server for the address pool.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify DHCP configuration, enter: `ip dhcps`
3	To specify address pool configuration, enter: `pool <pool name>`
4	To configure the NetBIOS server name for the address pool, enter:

```
netbios_name_server <A.B.C.D>
```

--End--

Table 29
Variable definitions

Variable	Value
<A.B.C.D>	NetBIOS name server IP address.

Configuring network for the address pool

Configure the network for the address pool.

Procedure steps

Step	Action
1	To enter the configuration mode, enter:

```
configure terminal
```

Step	Action
2	To specify DHCP configuration, enter:

```
ip dhcps
```

Step	Action
3	To specify address pool configuration, enter:

```
pool <pool name>
```

Step	Action
4	To configure the network for the address pool, enter:

```
network <A.B.C.D> <mask>
```

--End--

Table 30
Variable definitions

Variable	Value
<A.B.C.D> <mask>	Specifies the network number and mask.

Configuring TFTP server name for the address pool

Configure the TFTP server name for the address pool.

Procedure steps

Step	Action
1	To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure the TFTP server name for the address pool, enter:

```
tftpserver <A.B.C.D>
```

--End--

Table 31
Variable definitions

Variable	Value
<A.B.C.D>	Specifies the TFTP server IP address.

Configuring Nortel Phone Wireless server name for the address pool

Configure the Nortel Phone Wireless server name for the address pool.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify DHCP configuration, enter:

```
ip dhcps
```

3 To specify address pool configuration, enter:

```
pool <pool name>
```

4 To configure the Nortel Phone Wireless server name for the address pool, enter:

```
wireless <A.B.C.D>
```

--End--

Table 32
Variable definitions

Variable	Value
<A.B.C.D>	Specifies the wireless IP address.

Configuring remote database

Configure a remote database on DHCPv4 server.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify DHCP configuration, enter: `ip dhcps`
3	Configure remote database: `remote_database <ftp://<user>:<password>@<host>:<port>/<url-path><interval>`

--End--

Enabling DHCPv4 server

Enable the DHCPv4 server.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify DHCP configuration, enter: `ip dhcps`
3	Enable the DHCPv4 server: `enable`

--End--

Configuring DHCP relay

Configure the DHCP relay.

Procedure steps

Step	Action
1	To enter the configuration mode, enter:

```
configure terminal
```

2 To select an interface, enter:

```
interface {ethernet <slot/port> | vlan<vid>}
```

3 Configure relay:

```
dhcp-relay <A.B.C.D> <W.X.Y.Z>
```

--End--

Table 33
Variable definitions

Variable	Value
<A.B.C.D>	server IP address
<W.X.Y.Z>	gateway IP address

Configuring DHCP relay server and gateway addresses

Configure the DHCP relay server and gateway addresses.

Procedure steps

Step **Action**

1 To enter the configuration mode, enter:

```
configure terminal
```

2 To specify an interface to configure, enter:

```
interface {ethernet <slot/port> | vlan<vid>}
```

3 Configure DHCP relay server and gateway address:

```
dhcp-relay <server-ip-address> <gateway-ip-address>
```

--End--

Configuring the primary DNS name server

Configure primary DNS name server.

Step **Action**

1 To enter the configuration mode, enter:

```
configure terminal
```

2 Configure primary DNS name server:

```
ip pname_server <server name>
```

--End--

Configuring the secondary DNS name server

Configure the secondary DNS name server.

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	Configure the secondary DNS name server: `ip name_server <server-name>`

--End--

Table 34
Variable definitions

Variable	Value
<server name>	name of the server

Configuring the default domain name

Configure the default domain name.

Step	Action
1	Configure the default domain name: `ip domain_name <domain-name>`

--End--

Table 35
Variable definitions

Variable	Value
<domain-name>	name of the domain

Displaying DNS configuration

Display DNS configuration

Step	Action
1	Display DNS configuration: `show ip dns`

--End--

DHCPv4 Relay over VLAN

In the current release, the SR2330/4134 now supports DHCPv4 relay on VLAN interfaces.

A DHCP server can assign key parameters to a DHCP client including IP address, default gateway, and domain-name server. The client needs these parameters to communicate with the network to which it is connected.

If the client is connected to a network that contains a DHCP server, the server can reply directly to the client requests. But if the DHCP server is in a remote network, the client requests cannot reach the server.

To allow local client requests to reach the remote DHCP server, you can configure an SR2330/4134 interface in the local network as a DHCP relay agent. The relay agent can forward DHCP client requests from the local network to a DHCP server in the remote network. When the server replies, the relay agent forwards the responses back to the client on the local network.

For the DHCP server to accept requests from a DHCP relay agent, you must specify the relay agent IP address on the DHCP server.

Configuring DHCP relay on a VLAN

Use this procedure to specify a VLAN interface as a DHCP relay agent and to specify the address of the DHCP server to which DHCP packets are to be relayed. A maximum of four DHCP server addresses can be configured on an interface.

You can also optionally specify the gateway address. If this address is specified, it is used as the source IP address of the DHCP broadcasts to be relayed; otherwise, the interface IP address is used. The DHCP server uses the gateway address to communicate with the relay agent.

Prerequisites

- On the DHCP server, you must specify the IP address of the SR2330/4134 interface that is serving as the DHCP relay agent.

Step	Action
1	To access configuration mode, enter: `configure terminal`
2	To access the VLAN configuration, enter: `interface vlan <vlan-id>`
3	To configure DHCP relay on the VLAN, enter: `[no] dhcp-relay <server-address> [<gateway>]`

--End--

Table 36
Variable definitions

Variable	Value
<server-address>	Specifies the IP address of the DHCP server (A.B.C.D).
[<gateway>]	Specifies the gateway IP address (A.B.C.D).
[no]	Removes the specified DHCP server address.

Displaying DHCP relay

Use this procedure to display the current DHCP relay configuration.

Step	Action
1	To display the DHCP relay configuration, enter: `show dhcp-relay`

--End--

Procedure job aid: sample command output

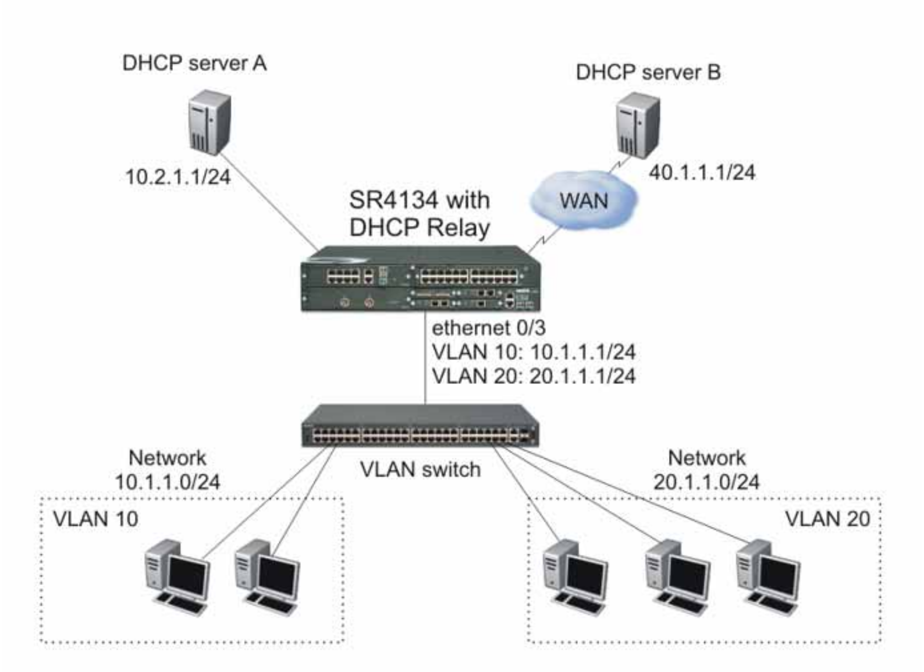
The following sample shows output from the `show dhcp-relay` command.

```
DHCP RELAY CONFIGURATION
------------------------
Interface DHCP Server Address Gateway Address
------------------------------------------------------
vlan10 10.2.1.1 10.1.1.1
vlan10 40.1.1.1 10.1.1.1
vlan20 10.2.1.1 20.1.1.1
vlan20 40.1.1.1 20.1.1.1
```

Example of configuring DHCP relay on a VLAN

The following figure shows a sample topology in which an SR2330/4134 VLAN interface is configured as a DHCP relay agent.

Figure 8
DHCP relay over VLAN configuration example



The following shows the configurations required on the SR4134 trunk port to enable DHCP relay for the connected VLANs. DHCP servers A and B operate as the remote DHCP servers. In this case, DHCP server A is configured as the preferred server and, if A is unreachable, DHCP server B provides service.

DHCP Relay configuration

```
SR/configure# interface ethernet 0/3
Configuring existing Ethernet interface
SR/configure/interface/ethernet (0/3)# switchport mode
```

```
trunk
SR/configure/interface/ethernet (0/3)# switchport trunk
allow vlan 10,20
SR/configure/interface/ethernet (0/3)# exit

SR/configure# interface vlan vlan10
SR/configure/interface/vlan vlan10# ip address 10.1.1.1 24
SR/configure/interface/vlan vlan10# dhcp-relay 10.2.1.1
10.1.1.1
DHCP RELAY: Server address set to 10.2.1.1
SR/configure/interface/vlan vlan10# dhcp-relay 40.1.1.1
10.1.1.1
DHCP RELAY: Server address set to 40.1.1.1
SR/configure/interface/vlan vlan10# exit

SR/configure# interface vlan vlan20
SR/configure/interface/vlan vlan20# ip address 20.1.1.1 24
SR/configure/interface/vlan vlan20# dhcp-relay 10.2.1.1
20.1.1.1
DHCP RELAY: Server address set to 10.2.1.1
SR/configure/interface/vlan vlan20# dhcp-relay 40.1.1.1
20.1.1.1
DHCP RELAY: Server address set to 40.1.1.1
```

DHCP Server A configuration

In this topology, if DHCP Server A is an SR2330/4134, the following configuration can be used to specify address pools, enable the DHCP server on an interface, and specify the DHCP relay interface. DHCP Server A provides service for both VLAN 10 and VLAN 20.

DHCP pool configuration for subnet 10.1.1.0/24

```
ServerA/configure# ip dhcps
ServerA/configure/ip/dhcps# pool pool1
ServerA/configure/ip/dhcps/pool pool1# network
10.1.1.0 24
ServerA/configure/ip/dhcps/pool pool1# lease 1000
ServerA/configure/ip/dhcps/pool pool1# default_router
10.1.1.1
ServerA/configure/ip/dhcps/pool pool1# netbios_name_
server 120.1.1.1
ServerA/configure/ip/dhcps/pool pool1# tftpserver
64.64.11.11
ServerA/configure/ip/dhcps/pool pool1# dnsserver
164.164.4.5
ServerA/configure/ip/dhcps/pool pool1# exclude-range
10.1.1.1 10.1.1.10
```

```
ServerA/configure/ip/dhcps/pool pool1# domain Nortel
ServerA/configure/ip/dhcps/pool pool1# commit
ServerA/configure/ip/dhcps/pool pool1# exit
ServerA/configure/ip/dhcps# enable
```

DHCP pool configuration for subnet 20.1.1.0/24

```
ServerA/configure# ip dhcps
ServerA/configure/ip/dhcps# pool pool2
ServerA/configure/ip/dhcps/pool pool2# network
20.1.1.0 24
ServerA/configure/ip/dhcps/pool pool2# lease 1000
ServerA/configure/ip/dhcps/pool pool2# default_router
20.1.1.1
ServerA/configure/ip/dhcps/pool pool2# netbios_name_
server 120.1.1.1
ServerA/configure/ip/dhcps/pool pool2# tftpserver
64.64.11.11
ServerA/configure/ip/dhcps/pool pool2# dnsserver
164.164.4.5
ServerA/configure/ip/dhcps/pool pool2# exclude-range
20.1.1.1 20.1.1.10
ServerA/configure/ip/dhcps/pool pool2# domain Nortel
ServerA/configure/ip/dhcps/pool pool2# commit
ServerA/configure/ip/dhcps/pool pool2# exit
ServerA/configure/ip/dhcps# enable
```

Enabling the DHCP server on an interface

```
ServerA/configure# interface ethernet 0/1
ServerA/configure/interface/ethernet 0/1# ip address
10.2.1.1 24
ServerA/configure/interface/ethernet 0/1# exit
ServerA/configure# ip dhcps
ServerA/configure/ip/dhcps# interface ethernet0/1
ServerA/configure/ip/dhcps# enable
```

Specifying the DHCP relay agents on DHCP server A

```
ServerA/configure/ip/dhcps# relay 10.1.1.1 10.1.1.0
ServerA/configure/ip/dhcps# relay 20.1.1.1 20.1.1.0
```

Enabling DHCP client and relay debug messages

Use this procedure to enable DHCP client and relay debug messages. Use the no version of the command to disable the debug messages.

Step	Action
1	To enable the DHCP relay debug messages, enter:

```
[no] debug dhcp_relay enable_debug
```

--End--

Table 37
Variable definitions

Variable	Value
[no]	Disables DHCP relay debug messages.

DHCPv4 monitoring

Monitor the DHCPv4 on the Nortel Secure Router 4134.

DHCPv4 monitoring procedures

This task flow shows you the sequence of procedures you use to monitor DHCPv4 on the Nortel Secure Router 4134. To link to any procedure, see "DHCPv4 monitoring procedure navigation" (page 77)

DHCPv4 monitoring procedure navigation

Displaying DHCPv4 server configuration

Display the DHCPv4 server configuration on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display DHCPv4 server configuration: `show ip dhcps config`

--End--

Displaying DHCPv4 server interface

Display the DHCPv4 server interface on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display DHCPv4 server interface: `show ip dhcps interfaces`

--End--

Displaying DHCPv4 server address pool

Display the DHCPv4 server address pool on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display DHCPv4 server address pool: `show ip dhcps address_pools`

--End--

Displaying DHCPv4 server binding

Display the DHCPv4 server binding on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display DHCPv4 server binding: `show ip dhcps bindings`

--End--

Displaying DHCPv4 server statistics

Display the DHCPv4 server statistics on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display DHCPv4 server statistics: `show ip dhcps statistics`

--End--

Displaying DHCP relay state

Display the DHCP relay state on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display DHCP relay state: `show dhcp-relay`

--End--

Clearing DHCPv4 server statistics

Clear the DHCP server statistics.

Procedure steps

Step	Action
1	Clear DHCP server statistics: `clear ip dhcps statistics`

--End--

Clearing DHCPv4 server bindings

Clear the DHCP server bindings.

Procedure steps

Step	Action
1	Clear DHCPv4 server bindings

```
clear ip dhcps bindings
```

--End--

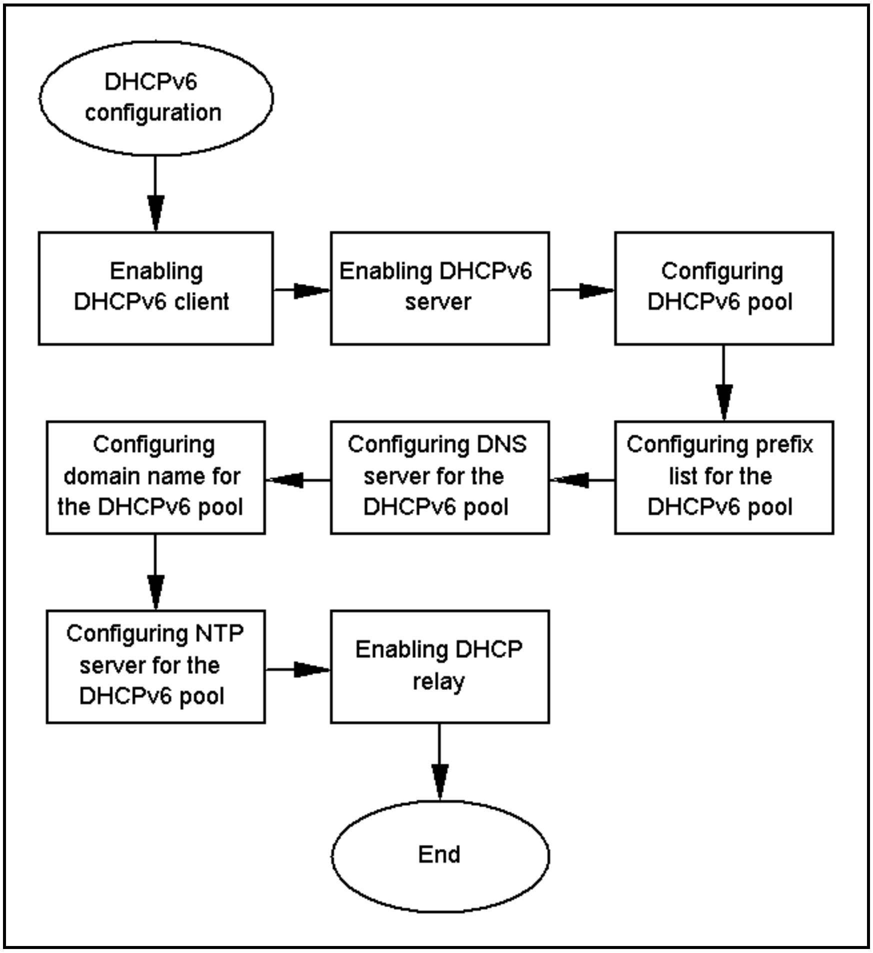
DHCPv6 configuration

Configure the DHCPv6 on the Nortel Secure Router 4134.

DHCPv6 configuration procedures

This task flow shows you the sequence of procedures you use to configure DHCPv6 on the Nortel Secure Router 4134. To link to any procedure, see "DHCPv6 configuration procedure navigation" (page 82)

Figure 9
DHCPv6 configuration procedures


DHCPv6 configuration
Enabling DHCPv6 client
Enabling DHCPv6 server
Configuring DHCPv6 pool
Configuring prefix list for the DHCPv6 pool
Configuring DNS server for the DHCPv6 pool
Configuring domain name for the DHCPv6 pool
Configuring NTP server for the DHCPv6 pool
Enabling DHCP relay
End

DHCPv6 configuration procedure navigation

Enabling DHCPv6 client

Enable the DHCPv6 client on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify an Ethernet interface to configure, enter: `interface ethernet <slot port>`
3	Enable DHCPv6 client `ipv6 dhcp client pd <prefix name>`

--End--

Enabling DHCPv6 server

Enable the DHCPv6 server on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	To specify an Ethernet interface to configure, enter: `interface ethernet <slot port>`

3 Enable the DHCPv6 server:

```
ipv6 dhcp server <pool name>
```

--End--

Configuring DHCPv6 pool

Configure the DHCPv6 pool on the Nortel Secure Router 4134.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 Configure the DHCPv6 pool:

```
ipv6 dhcp pool <pool-name>
```

--End--

Configuring prefix list for the DHCPv6 pool

Configure static prefix list for DHCPv6 server on the Nortel Secure Router 4134.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 Select DHCPv6 pool:

```
ipv6 dhcp pool <pool-name>
```

3 Configure prefix delegation:

```
prefix-delegation ipv6_prefix <prefix_len>
<client-duid>
```

--End--

Table 38
Variable definitions

Variable	Value
<prefix_len>	IPv6 prefix (X:X::X:X/M)
<client-duid>	DUID in hh:hh:tt:tt:m1:m2:m3:m4:m5:m6, last 6 bytes are MAC

Configuring DNS server for the DHCPv6 pool

Configure the IPv6 address to the DNS server that has to be delegated to DHCPv6 client.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	Select DHCPv6 pool: `ipv6 dhcp pool <pool-name>`
3	Configure DNS server: `dns-server <dns_server_ipv6_address>`

--End--

Table 39
Variable definitions

Variable	Value
<dns_server_ipv6_address>	IPv6 address of DNS server

Configuring the domain name for the DHCPv6 pool

Configure the domain name that has to be delegated to the DHCPv6 client.

Procedure steps

Step	Action
1	To enter the configuration mode, enter: `configure terminal`
2	Select DHCPv6 pool: `ipv6 dhcp pool <pool-name>`

3 Configure the domain name:

```
domain-name <domain_name>
```

--End--

Table 40
Variable definitions

Variable	Value
<domain_name>	domain name

Configuring the NTP server for the DHCPv6 pool

Configure the IPv6 address on the NTP server that has to be delegated to the DHCPv6 client.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2 Select DHCPv6 pool:

```
ipv6 dhcp pool <pool-name>
```

3 Configure the NTP server:

```
ntp-server <ntp_server_ipv6_address>
```

--End--

Table 41
Variable definitions

Variable	Value
<ntp_server_ipv6_address>	IPv6 address of NTP server

Enabling DHCPv6 relay

Enable the DHCPv6 relay on the Nortel Secure Router 4134.

Procedure steps

Step	Action

1 To enter the configuration mode, enter:

```
configure terminal
```

2. To specify an Ethernet interface to configure, enter:

   ```
   interface ethernet <slot port>
   ```

3. Enable the DHCPv6 relay:

   ```
   ipv6 dhcp relay server-ipv6 <server-ipv6 address>
   ```

--End--

DHCPv6 monitoring

Monitor the DHCPv6 status on the Nortel Secure Router 4134.

DHCPv6 monitoring procedures

This task flow shows you the sequence of procedures you use to monitor DHCPv4 on the Nortel Secure Router 4134. To link to any procedure, see "DHCPv6 monitoring procedure navigation" (page 87)

DHCPv6 monitoring procedure navigation

- "Displaying DHCPv6 interface" (page 87)
- "Displaying DHCPv6 pool" (page 87)
- "Displaying DHCPv6 binding" (page 88)
- "Displaying DHCPv6 DUIDs" (page 88)

Displaying DHCPv6 interface

Display the DHCPv6 enabled interface for the server and the client on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display the DHCPv6 interface:

```
show ipv6 dhcp interface
```

--End--

Displaying DHCPv6 pool

Display the DHCPv6 pool configuration on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display the DHCPv6 pool: `show ipv6 dhcp pool`

--End--

Displaying DHCPv6 binding

Display DHCPv6 binding provided by the server on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display the DHCPv6 binding: `show ipv6 dhcp binding`

--End--

Displaying DHCPv6 DUIDs

Display DHCPv6 DUIDs corresponding to the server and the client on the Nortel Secure Router 4134.

Procedure steps

Step	Action
1	Display the DHCPv6 DUIDs `show ipv6 dhcp duids`

--End--

Configuring access protocols

Configure access protocols to perform system operation, maintenance, and administration (OAM) tasks remotely.

Configuring access protocols procedure navigation

- "Configuring Telnet" (page 89)
- "Configuring the FTP" (page 90)
- "Enabling the TFTP" (page 91)

Configuring Telnet

Enable Telnet to log on to the Secure Router to perform OAM tasks remotely.

Procedure steps

Step	Action
1	Enable the Telnet server on the Secure Router: **`telnet_server`**
2	Configure the Telnet session timeout: **`telnet_timeout <seconds>`**
3	Configure a Telnet session display banner: **`telnet_banner <banner> [<banner#>]`**
4	Configure a Telnet session motd banner: **`telnet_banner <banner> [<motd_banner>]`**
5	Display Telnet session: **`show telnet`**
6	Clear Telnet session: **`clear telnet_session <1-16>`**

```
clear telnet_sessions
```

--End--

Table 42
Variable definitions

Variable	Value
<banner>	sets the banner text. Enter up to 255 characters
<banner#>	creates longer descriptions using banner1 and banner2. Each banner command is limited to 255 characters
<motd_banner>	configures message of the day
<seconds>	specifies the number of seconds after which an inactive Telnet session times out. The default is 900 seconds. 0 seconds indicates the session does not timeout
<1-16>	telnet session range

Configuring the FTP

Enable the File Transfer Protocol (FTP) to transfer data within a secured network.

Procedure steps

Step	Action
1	Enable the FTP server on the Secure Router:

```
ftp_server
```

2	Create the FTP user account:

```
ftp_user <username>
```

3	Enter the password for the new FTP user account.
4	Enter the password again to confirm it.
5	Display FTP:

```
show ftp
```

--End--

Table 43
Variable definitions

Variable	Value
<username>	creates the new username for the FTP account

Enabling the TFTP

Enable the Trivial File Transfer Protocol (TFTP) to transfer data within a secured network.

Procedure steps

Step	Action

1 Enable the TFTP server on the Secure Router:

```
tftp_server
```

2 Display TFTP:

```
show tftp_server_info
```

--End--

Nortel Secure Router 2330/4134

Configuration — Network Management

Release: 10.2
Publication: NN47263-602
Document revision: 03.01
Document release date: 7 September 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com