Nortel Ethernet Routing Switch 2500 Series

Configuration — IP Routing and Multicast

NN47215-503

Document status: Standard
Document version: 03.01
Document date: 27 October 2008

Sourced in Canada and the United States of America

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).
2. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
3. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 2500 Series Configuration — IP Routing and Multicast* for Release 4.2.

Features

See the following sections for information about feature changes:

IP routing

The Nortel Ethernet Routing Switch 2500 Series now supports wire-speed IP routing between VLANs. With routing globally enabled, if you assign an IP address to a VLAN, IP routing is enabled for that VLAN. In addition, for each IP address assigned to a VLAN interface, the Ethernet Routing Switch adds a directly connected or local route to its routing table based on the IP address/mask assigned.

After you create routable VLANs though IP address assignment, you can create static routes. With static routes, you can manually create specific routes to a destination IP address. In this release, the Ethernet Routing Switch supports local static routes only. Nonlocal static routes are not supported, nor are dynamic routing protocols.

For more information about IP routing fundamentals, see "IP routing fundamentals" (page 17).

Related routing features

BootP/DHCP relay

The Nortel Ethernet Routing Switch 2500 Series now supports BootP/DHCP relay, which forwards BootP or DHCP broadcasts to the IP address of a remote server. Routers must support BootP/DHCP relay so that hosts can access configuration information from servers several router hops away.

For more information about DHCP relay fundamentals, see "BootP/DHCP relay " (page 26).

UDP broadcast forwarding

To allow UDP broadcasts to reach a remote server, the Ethernet Routing Switch now supports UDP broadcast forwarding, which forwards the broadcasts to the server through a Layer 3 VLAN interface.

For more information about UDP broadcast forwarding fundamentals, see "UDP broadcast forwarding" (page 29).

Directed broadcasts

The Ethernet Routing Switch now supports directed broadcasts. With this feature enabled, the switch can determine if an incoming unicast frame is a directed broadcast for one of its interfaces. If so, the switch forwards the datagram onto the appropriate network using a link-layer broadcast.

For more information about directed broadcasts fundamentals, see "Directed broadcasts" (page 31).

ARP

The Address Resolution Protocol (ARP) allows the Ethernet Routing Switch to dynamically learn Layer 2 Media Access Control (MAC) addresses, and to build a table with corresponding Layer 3 IP addresses.

For more information about ARP fundamentals, see "ARP" (page 31).

Static ARP

In addition to the dynamic ARP mechanism, the Ethernet Routing Switch now supports a static mechanism that allows for static ARP entries to be added. With Static ARP, you can manually associate a device MAC address to an IP address. You can add and delete individual static ARP entries on the switch.

For more information about Static ARP fundamentals, see "Static ARP" (page 32).

Proxy ARP

The Ethernet Routing Switch now supports Proxy ARP, which allows the switch to respond to an ARP request from a locally attached host that is intended for a remote destination. It does so by sending an ARP response back to the local host with the MAC address of the switch interface that is connected to the host subnet. The reply is generated only if the switch has an active route to the destination network.

For more information about Proxy ARP fundamentals, see "Proxy ARP" (page 32).

IP blocking for stacks

IP blocking is a Layer 3 feature of the Nortel Ethernet Routing Switch 2500 Series that provides safeguards for a stack where Layer 3 VLANs have port members across multiple stack units. IP Blocking is used whenever a unit leaves a stack or is rebooting inside the context of a stack. Depending on the setting in use, Layer 3 functionality is either continued or blocked by this feature.

You can set the IP Blocking mode on the base unit to either none or full.

When IP blocking is set to full, if any units leave the stack, those units run in Layer 2 mode.

When IP blocking is set to none, if any units leave the stack, the Layer 3 configurations applied to the stack are still applied on the individual units.

For more information about IP blocking fundamentals, see "IP blocking for stacks" (page 33).

Other changes

See the following sections for information about changes that are not feature-related:

Content changes related to IGMP snooping

This document contains modified IP multicast and IGMP snooping sections that originally existed in the *Configuration — VLANs, Spanning Tree, and Link Aggregation* document. The existing IGMP snooping configuration content has been modified to be procedural instead of a list of referenced commands (see "IGMP snooping configuration using NNCLI" (page 87)), and overview sections describing IP multicast and IGMP have been added (see "IGMP fundamentals" (page 37)). In addition, a description of an interworking issue with Windows clients has been included (see "IGMP snooping interworking with Windows clients" (page 49)).

Introduction

This document provides procedures and conceptual information to configure IP routing features on the Nortel Ethernet Routing Switch 2500 Series, including static routes, Proxy ARP, DHCP Relay, and UDP forwarding. It also provides procedures and conceptual information to manage multicast traffic using IGMP snooping.

NNCLI command modes

NNCLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter NNCLI in User EXEC mode and use the **enable** command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC `2526T>`	No entrance command, default mode	**exit** or **logout**

Command mode and sample prompt	Entrance commands	Exit commands
Privileged EXEC `2526T#`	**`enable`**	**`exit`** or **`logout`**
Global Configuration `2526T(config)#`	From Privileged EXEC mode, enter: **`configure`**	To return to Privileged EXEC mode, enter: **`end`** or **`exit`** To exit NNCLI completely, enter: **`logout`**
Interface Configuration `2526T(config-if)#`	From Global Configuration mode, to configure a port, enter: **`interface fastethernet <port number>`** To configure a VLAN, enter: **`interface vlan <vlan number>`**	To return to Global Configuration mode, enter: **`exit`** To return to Privileged EXEC mode, enter: **`end`** To exit NNCLI completely, enter: **`logout`**

For more information, see *Nortel Ethernet Routing Switch 2500 Series Fundamentals* (NN47215-102).

Navigation

IP routing fundamentals

This chapter provides an introduction to IP routing and related features used in the Nortel Ethernet Routing Switch 2500 Series.

IP addressing overview

An IP version 4 (IPv4) address consists of 32 bits expressed in a dotted-decimal format (XXX.XXX.XXX.XXX). The IPv4 address space is divided into classes, with classes A, B, and C reserved for unicast addresses, and accounting for 87.5 percent of the 32-bit IP address space. Class D is reserved for multicast addressing. The following table lists the breakdown of the IP address space by address range and mask.

Table 1
IP address classifications

Class	Address Range	Mask	Number of Networks	Nodes per Network
A	1.0.0.0 - 127.0.0.0	255.0.0.0	127	16 777 214
B	128.0.0.0 - 191.255.0.0	255.255.0.0	16 384	65 534
C	192.0.0.0 - 223.255.255.0	255.255.255 .0	2 097 152	255
D	224.0.0.0 - 239.255.255.254			
E	240.0.0.0 - 240.255.255.255			

Note 1: Class D addresses are primarily reserved for multicast operations, although the addresses 224.0.0.5 and 224.0.0.6 are used by OSPF and 224.0.0.9 is used by RIP.

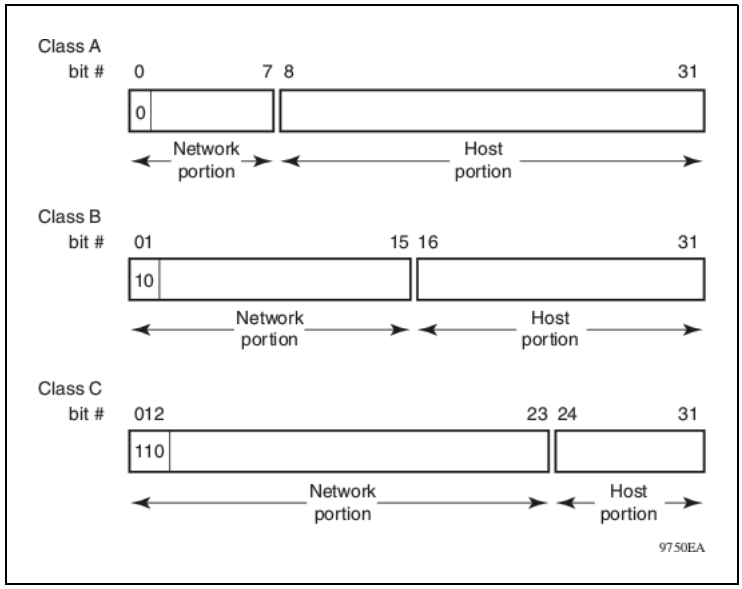
Note 2: Although technically part of Class A addressing, network 127 is reserved for loopback.

Note 3: Class E addresses are reserved for research purposes.

To express an IP address in dotted-decimal notation, each octet of the IP address is converted to a decimal number and separated by decimal points. For example, the 32-bit IP address 10000000 00100000 00001010 10100111 is expressed in dotted-decimal notation as 128.32.10.167.

Each IP address class, when expressed in binary notation, has a different boundary point between the network and host portions of the address, as shown in the following figure. The network portion is a network number field from 8 through 24 bits. The remaining 8 through 24 bits identify a specific host on the network.

Figure 1
Network and host boundaries in IP address classes



Subnet addressing

Subnetworks (or subnets) are an extension of the IP addressing scheme. With subnets, organizations can use one IP address range for multiple networks. Subnets are two or more physical networks that share a common network-identification field (the network portion of the 32-bit IP address).

A subnet address is created by increasing the network portion to include a subnet address, thus decreasing the host portion of the IP address. For example, in the address 128.32.10.0, the network portion is 128.32, while the subnet is found in the first octet of the host portion (10). A subnet mask is applied to the IP address and identifies the network and host portions of the address.

The following table illustrates how subnet masks used with Class B and Class C addresses can create differing numbers of subnets and hosts. This example shows the use of the zero subnet, which is permitted on a Nortel Ethernet Routing Switch 2500 Series.

Table 2
Subnet masks for Class B and Class C IP addresses

Number of bits	Subnet Mask	Number of Subnets (Recommended)	Number of Hosts per Subnet
Class B			
2	255.255.192.0	2	16 382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16 382	2
Class C			
1	255.255.255.128	0	126
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Variable-length subnet masking (VLSM) is the ability to divide an intranet into pieces that match network requirements. Routing is based on the longest subnet mask or network that matches.

IP routing

To configure IP routing on the Nortel Ethernet Routing Switch 2500 Series, you must create virtual router interfaces by assigning an IP address to a virtual local area network (VLAN). The following sections provide more details about IP routing functionality.

For a more detailed description about VLANs and their use, see *Nortel Ethernet Routing Switch 2500 Series Configuration - VLANs, Spanning Tree, and Link Aggregation*.

IP routing using VLANs

The Nortel Ethernet Routing Switch 2500 Series supports wire-speed IP routing between VLANs. To create a virtual router interface for a specified VLAN, you must associate an IP address with the VLAN.

The virtual router interface is not associated with any specific port. The VLAN IP address can be reached through any of the ports in the VLAN. The assigned IP address also serves as the gateway through which packets are routed out of that VLAN. Routed traffic can be forwarded to another VLAN within the switch or stack.

When the Nortel Ethernet Routing Switch 2500 Series is routing IP traffic between different VLANs, the switch is considered to be running in Layer 3 mode; otherwise, the switch runs in Layer 2 mode. When you assign an IP address to a Layer 2 VLAN, the VLAN becomes a routable Layer 3 VLAN. You can assign a single and unique IP address to each VLAN.

You can configure the global status of IP routing to be enabled or disabled on the Nortel Ethernet Routing Switch 2500 Series. By default, IP routing is disabled.

In this release, the Nortel Ethernet Routing Switch 2500 Series supports local routes and static routes. With local routing, the switch automatically creates routes to each of the local Layer 3 VLAN interfaces. With static routing, you must manually enter the routes to the destination IP addresses.

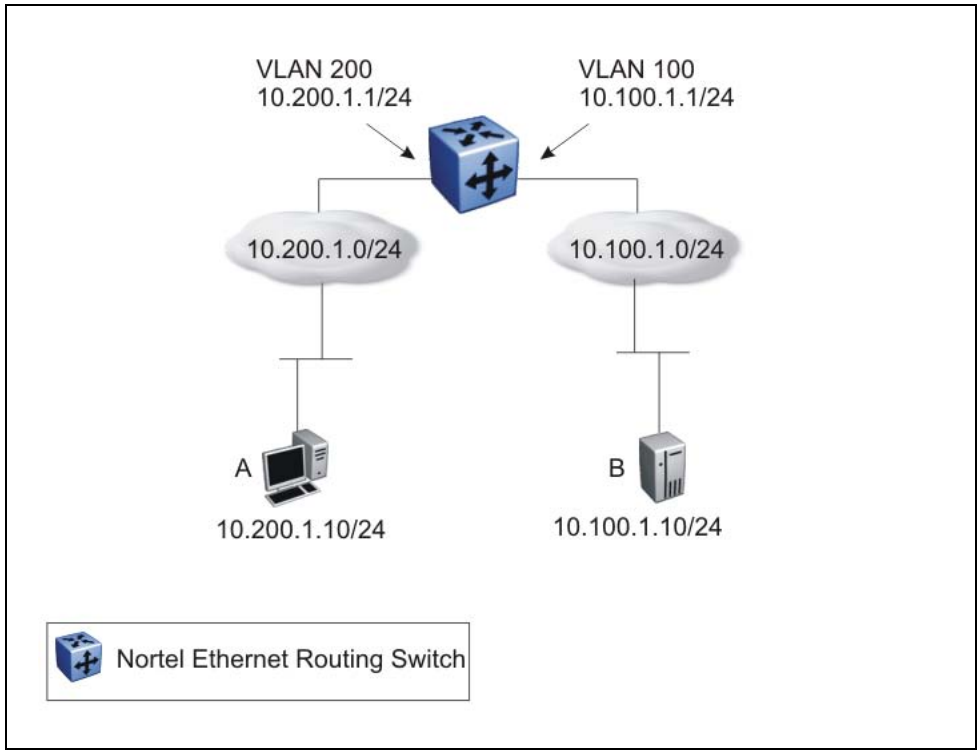
Local routes

With routing globally enabled, if you assign an IP address to a VLAN, IP routing is enabled for that VLAN. In addition, for each IP address assigned to a VLAN interface, the Ethernet Routing Switch adds a directly connected or local route to its routing table based on the IP address/mask assigned.

Local routing example

The following figure shows how the Ethernet Routing Switch can route between Layer 3 VLANs. In this example, the Ethernet Routing Switch has two VLANs configured. IP Routing is enabled globally on the switch and on the VLANs, each of which has an assigned IP address.

Figure 2
Local routes example



IP address 10.100.1.1/24 is assigned to VLAN 100, and IP address 10.200.1.1/24 is assigned to VLAN 200. As IP Routing is enabled, two local routes become active on the Nortel Ethernet Routing Switch as described in the following table.

	Network	Net-mask	Next-hop	Type
1	10.100.1.0	255.255.255.0	10.100.1.1	LOCAL
2	10.200.1.0	255.255.255.0	10.200.1.1	LOCAL

At this stage, both hosts A (10.200.1.10) and B (10.100.1.10) are reachable from the Ethernet Routing Switch. However, to achieve Layer 3 connectivity between A and B, additional configuration is required. Host A must know how to reach network 10.100.1.0/24, and host B must know how to reach network 10.200.1.0/24.

On host A, you must configure a route to network 10.100.1.0/24 through 10.200.1.1, or configure 10.200.1.1 as the default gateway for the host.

On host B, you must configure a route to network 10.200.1.0/24 through 10.100.1.1, or configure 10.100.1.1 as the default gateway for the host.

With these routes configured, the Ethernet Routing Switch can perform inter-VLAN routing, and packets can flow between hosts A and B.

Static routes

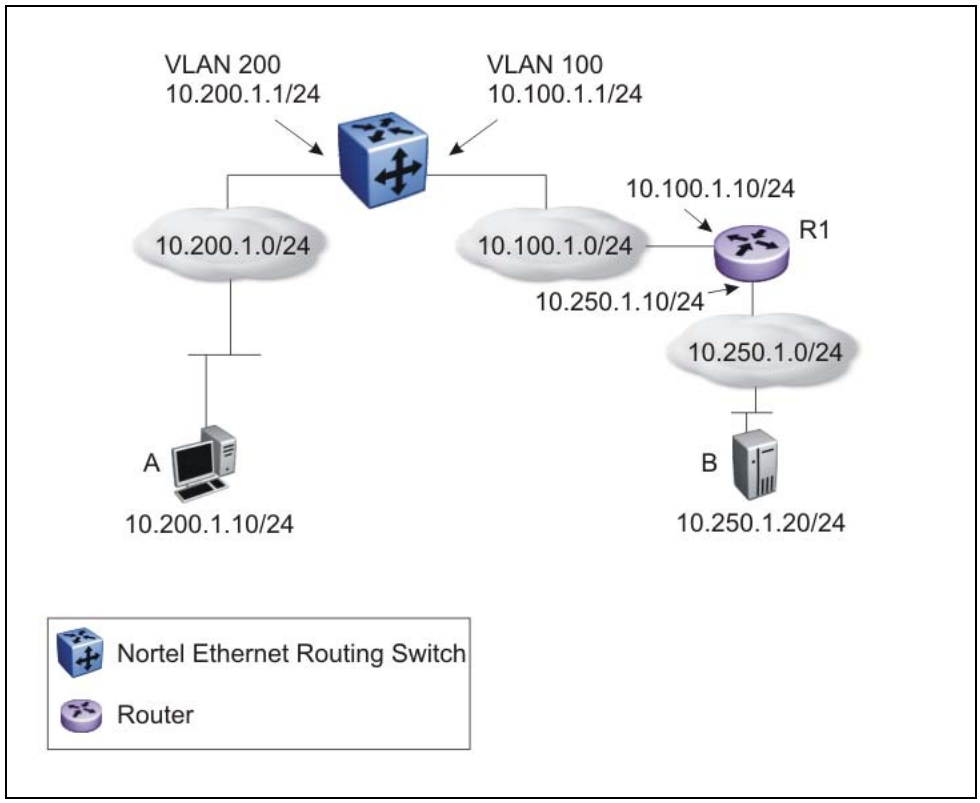
After you create routable VLANs though IP address assignment, you can create static routes. With static routes, you can manually create specific routes to a destination IP address. In this release, the Ethernet Routing Switch supports local static routes only. For a route to become active on the switch, the next-hop IP address for the route must be on a directly connected network. Nonlocal static routes are not supported.

Static routes are not easily scalable. Thus, in a large or growing network, this type of route management may not be optimal.

Static routing example

The following figure shows an example of static routing on the Ethernet Routing Switch.

Figure 3
Static routes



In this example, two Layer 3 devices are used to create a physical link between hosts A and B. This network contains an Ethernet Routing Switch and another Layer 3 router, R1.

In this setup, the local route configuration from "Local routing example" (page 21) still applies. However, in this case, network 10.100.1.0/24 stands in between networks 10.200.1.0/24 and 10.250.1.0/24. To achieve end-to-end connectivity, router R1 must know how to reach network 10.200.1.0/24, and the Ethernet Routing Switch must know how to reach network 10.250.1.0/24. On the Ethernet Routing Switch, you can accomplish this using static routing. With static routing, you can configure a route to network 10.250.1.0/24 through 10.100.1.10. In this case, the following routes are active on the Ethernet Routing Switch.

	Network	Net-mask	Next-hop	Type
1	10.100.1.0	255.255.255.0	10.100.1.1	LOCAL
2	10.200.1.0	255.255.255.0	10.200.1.1	LOCAL
3	10.250.1.0	255.255.255.0	10.100.1.10	STATIC

To obtain Layer 3 connectivity between the hosts, additional routes are required. Host A requires a route to 10.250.1.0/24 using 10.200.1.1 as the next hop, or with 10.200.1.1 as the default gateway. Host B requires a route to 10.200.1.0/24 using 10.250.1.10 as the next hop, or with 10.250.1.10 as the default gateway.

The configuration for router R1 to reach network 10.200.1.0/24 is dependent on the type of router used.

Default routes

Default routes specify a route to all networks for which there are no explicit routes in the Forwarding Information Base or the routing table. This static default route is a route to the network address 0.0.0.0 as defined by the Institute of Electrical and Electronics Engineers (IEEE) Request for Comment (RFC) 1812 standard.

The Ethernet Routing Switch uses the default route 0.0.0.0/0.0.0.0 for all Layer 3 traffic that does not match a specific route. This traffic is forwarded to the next-hop IP address specified in the default route.

Route scaling

The Nortel Ethernet Routing Switch 2500 Series supports a maximum of 256 local routes and up to 32 static routes, including the default route (Destination = 0.0.0.0, Mask = 0.0.0.0).

Management VLAN

With IP routing enabled on the switch or stack, you can use any of the virtual router IP addresses for device management over IP. Any routable Layer 3 VLAN can carry the management traffic for the switch, including Telnet, Web, Simple Network Management Protocol (SNMP), BootP, and Trivial File Transfer Protocol (TFTP). Without routing enabled, the management VLAN is reachable only through the switch or stack IP address, and only through ports that are members of the management VLAN. The management VLAN always exists on the switch and cannot be removed.

When routing is enabled on the Nortel Ethernet Routing Switch 2500 Series switches, the management VLAN behaves similar to other routable VLANs. The IP address is reachable through any virtual router interface, as long as a route is available.

Management route

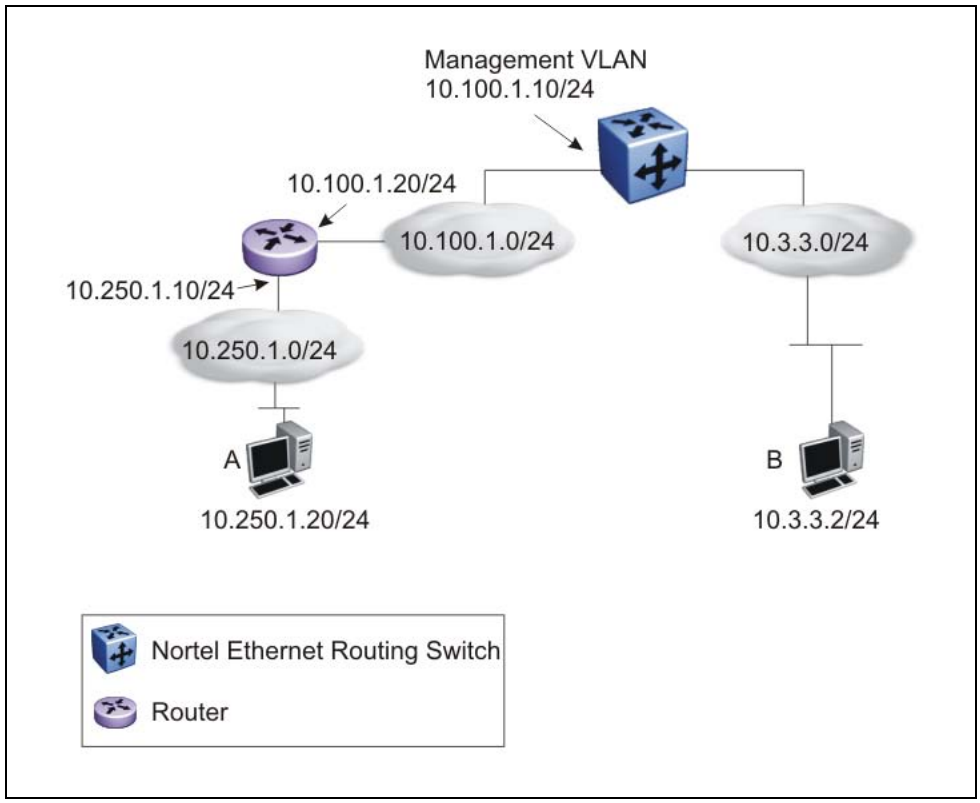
On the Ethernet Routing Switch, you can configure a management route from the Management VLAN to a particular subnet. The management route is a static route that allows incoming management connections from the remote network to the management VLAN.

The management route transports traffic between the specified destination network and the Management VLAN only. It does not carry inter-VLAN routed traffic from the other Layer 3 VLANs to the destination network. This provides a management path to the router that is inaccessible from the other Layer 3 VLANs. While you can access the management VLAN from all static routes, other static routes cannot route traffic to the management route.

To allow connectivity through a management route, you must enable IP routing globally and on the management VLAN interface.

The following figure shows an example of a management route allowing access to the management VLAN interface.

Figure 4
Management route



As network 10.250.1.0/24 is not directly connected to the Ethernet Routing Switch, to achieve connectivity from host 10.250.1.20 to the management VLAN, the Ethernet Routing Switch must know how to reach network 10.250.1.0/24. On the Ethernet Routing Switch, you can configure a management route to network 10.250.1.0/24 through 10.100.1.20. In this case, the following management route is active on the Ethernet Routing Switch.

	Network	Net-mask	Next-hop	Type
1	10.250.1.0	255.255.255.0	10.100.1.20	MANAGEMENT

With this configured route, host A at 10.250.1.20 can perform management operations on the Ethernet Routing Switch. To do so, Host A also requires a route to 10.100.1.0/24 using 10.250.1.10 as the next hop, or with 10.250.1.10 as the default gateway.

If a Layer 3 VLAN is also configured for network 10.3.3.0/24, this provides a local route that host B at 10.3.3.2 can use to access the switch. However, host B cannot communicate with host A, as the route to network 10.250.1.0/24 is a management route only. To provide connectivity between the two hosts, you must configure a static route to 10.250.1.0/24.

Related routing features

The following sections describe features that are related to and dependent on the IP routing functionality.

BootP/DHCP relay

Dynamic Host Configuration Protocol (DHCP) is a mechanism to assign network IP addresses on a dynamic basis to clients who request an address. DHCP is an extension of the Bootstrap protocol (BootP). BootP/DHCP clients (workstations) generally use User Datagram Protocol (UDP) broadcasts to determine their IP addresses and configuration information. If such a host is on a VLAN that does not include a DHCP server, the UDP broadcasts are by default not forwarded to servers located on different VLANs.

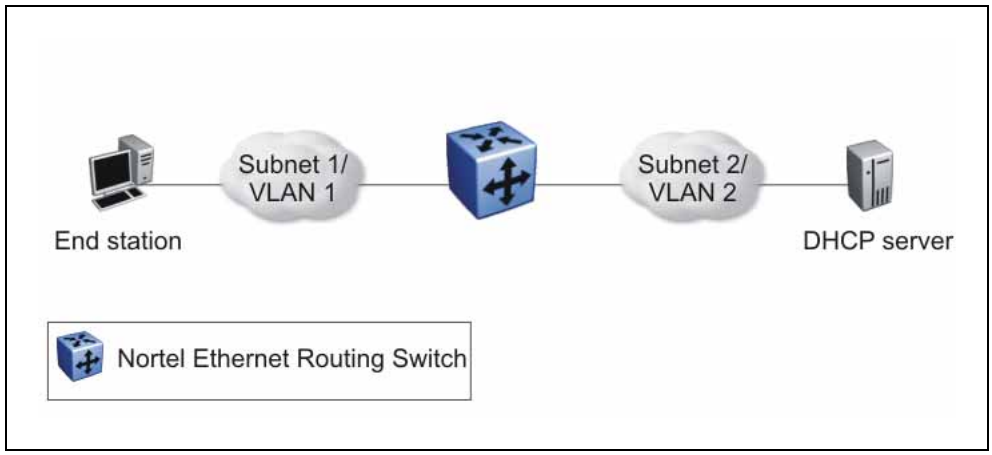
The Nortel Ethernet Routing Switch 2500 Series can resolve this issue using DHCP relay, which forwards the DHCP broadcasts to the IP address of the DHCP server. Network managers prefer to configure a small number of DHCP servers in a central location to lower administrative overhead. Routers must support DHCP relay so that hosts can access configuration information from servers several router hops away.

With DHCP relay enabled, the switch can relay client requests to DHCP servers on different Layer 3 VLANs or in remote networks. It also relays server replies back to the clients.

To relay DHCP messages, you must create two Layer 3 VLANs: one connected to the client and the other providing a path to the DHCP server. You can enable DHCP relay on a per-VLAN basis.

The following figure shows a DHCP relay example, with an end station connected to subnet 1, corresponding to VLAN 1. The Nortel Ethernet Routing Switch 2500 Series connects two subnets by means of the virtual routing function. When the end station generates a DHCP request as a limited UDP broadcast to the IP address of all 1s (that is, 255.255.255.255), with the DHCP relay function enabled, the Ethernet Routing Switch forwards the DHCP request to the host address of the DHCP server on VLAN 2.

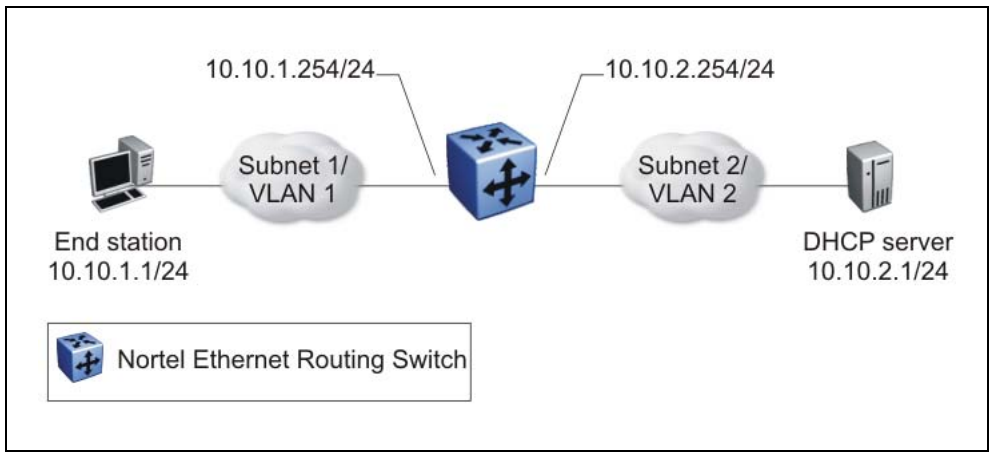
Figure 5
DHCP relay operation



Forwarding DHCP packets

In the following figure, the DHCP relay agent address is 10.10.1.254. To configure the Nortel Ethernet Routing Switch 2500 Series to forward DHCP packets from the end station to the server, use 10.10.2.1 as the server address.

Figure 6
Forwarding DHCP packets



All BootP and DHCP broadcast packets that appear on the VLAN 1 router interface (10.10.1.254) are then forwarded to the DHCP server. In this case, the DHCP packets are forwarded as unicast to the DHCP server IP address.

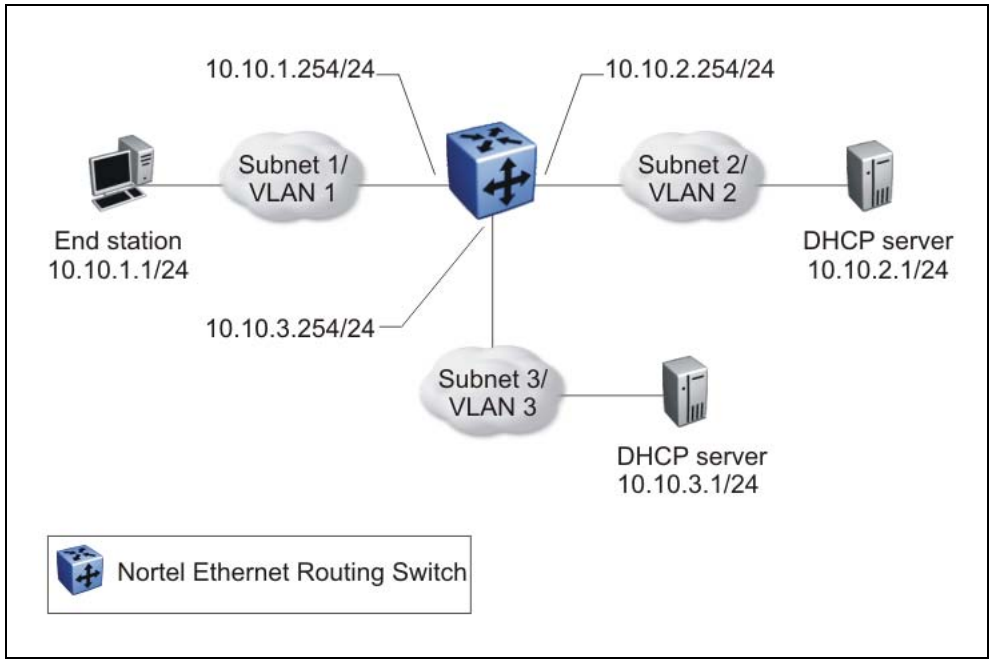
Multiple DHCP servers

Most enterprise networks use multiple DHCP servers for fault tolerance. The Nortel Ethernet Routing Switch 2500 Series can forward DHCP requests to multiple servers. You can configure up to 256 servers to receive copies of the forwarded DHCP messages.

To configure DHCP client requests to be forwarded to multiple different server IP addresses, specify the client VLAN as the DHCP relay agent for each of the destination server IP addresses.

In the following figure, two DHCP servers are located on two different VLANs. To configure the Nortel Ethernet Routing Switch 2500 Series to forward copies of the DHCP packets from the end station to both servers, specify the IP address of VLAN 1 (10.10.1.254) as the DHCP relay agent address and associate this relay agent with each of the DHCP server addresses, 10.10.2.1 and 10.10.3.1.

Figure 7
Multiple DHCP servers



Differences between DHCP and BootP

With DHCP relay, the Nortel Ethernet Routing Switch 2500 Series supports the relay of DHCP and the Bootstrap protocol (BootP). The following differences between DHCP and BootP are specified in RFC 2131:

- BootP enables the retrieval of an American Standard Code for Information Interchange (ASCII) configuration file name and configuration server address.
- A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask, and the IP address of the default router (default gateway).
- DHCP defines mechanisms through which clients can be assigned a network address for a finite lease (allowing for reuse of IP addresses).
- DHCP provides the mechanism for clients to acquire all of the IP configuration parameters they need to operate.

DHCP uses the BootP message format defined in RFC 951. The remainder of the options field consists of a list of tagged parameters that are called *options*(RFC 2131).

UDP broadcast forwarding

By default, User Datagram Protocol (UDP) broadcast frames received on one VLAN are not routed to another VLAN. To allow UDP broadcasts to reach a remote server, the Ethernet Routing Switch supports UDP broadcast forwarding, which forwards the broadcasts to the server through a Layer 3 VLAN interface.

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address. The packet is sent as a unicast packet to the server.

When a UDP broadcast is received on a router interface, it must meet the following criteria to be considered for forwarding:

- It must be a MAC-level broadcast.
- It must be an IP-limited broadcast.
- It must be for a configured UDP protocol.
- It must have a time-to-live (TTL) value of at least 2.

For each ingress interface and protocol, the UDP broadcast packets are forwarded only to a unicast host address (for example, to the unicast IP address of the server).

When the UDP forwarding feature is enabled, a filter is installed that compares the UDP destination port of all packets against all the configured UDP forwarding entries. If a match occurs, the destination IP of the incoming

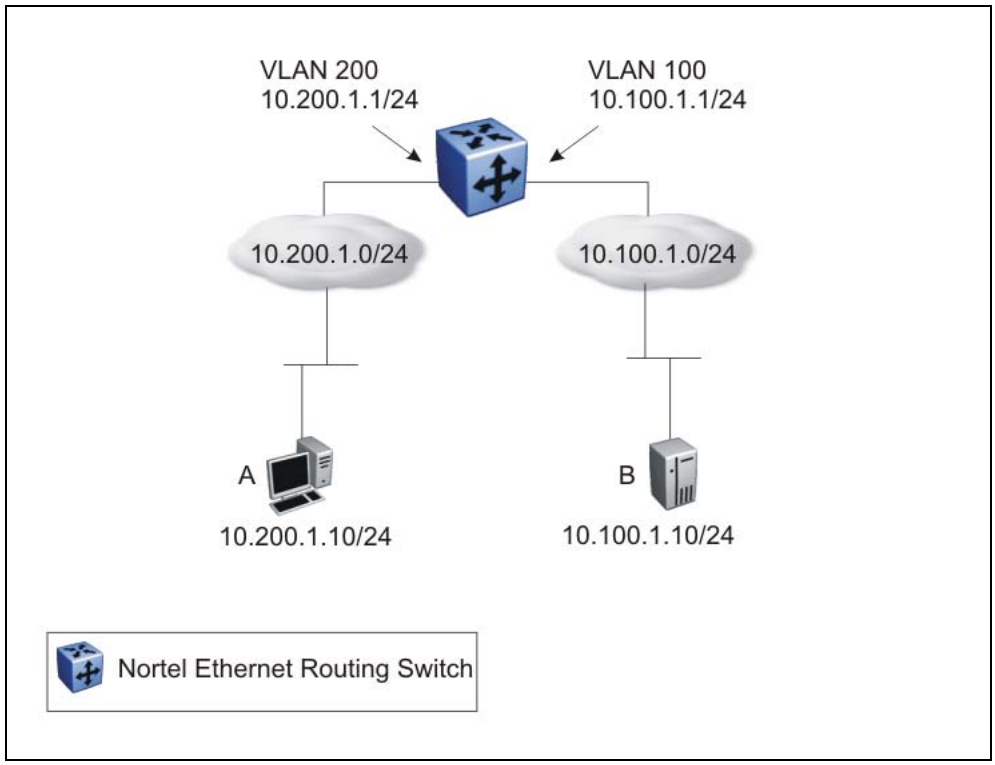
packet is checked for consistency with the user-configured broadcast mask value for this source VLAN. If these conditions are met, the TTL field from the incoming packet is overwritten with the user-configured TTL value, the destination IP of the packet is overwritten with the configured destination IP, and the packet is routed to the destination as a unicast frame.

UDP forwarding example

Figure 8 "UDP forwarding example" (page 30) shows an example of UDP broadcast forwarding. In this case, if host A (10.200.1.10) needs a certain service (for example, a custom application that listens on UDP port 12345), it transmits a UDP broadcast frame. By default, the Ethernet Routing Switch does not forward this frame to VLAN 100, and because server B (10.100.1.10) is not on VLAN 200, the host cannot access that service.

With UDP broadcast forwarding enabled, the host can access the service. In this case, you must list port 12345 as a valid forwarding port, and specify VLAN 200 as the source VLAN.

Figure 8
UDP forwarding example



When the switch receives an incoming packet on VLAN 200 that matches the configured UDP destination port (12345), and the destination IP is consistent with the broadcast mask value for the VLAN, then the switch applies the new destination IP (here, 10.100.1.10) to the packet and routes it to the destination as a unicast frame.

Directed broadcasts

With the directed broadcasts feature enabled, the Ethernet Routing Switch can determine if an incoming unicast frame is a directed broadcast for one of its interfaces. If so, the switch forwards the datagram onto the appropriate network using a link-layer broadcast.

With IP directed broadcasting enabled on a VLAN, the Ethernet Routing Switch forwards direct broadcast packets in the following two ways:

- through a connected VLAN subnet to another connected VLAN subnet
- through a remote VLAN subnet to the connected VLAN subnet

By default, this feature is disabled.

ARP

The Address Resolution Protocol (ARP) allows the Ethernet Routing Switch to dynamically learn Layer 2 Media Access Control (MAC) addresses, and to build a table with corresponding Layer 3 IP addresses.

Network stations using the IP protocol need both a physical (MAC) address and an IP address to transmit a packet. If a network station knows only the IP address of a network host, ARP enables the network station to determine the physical address of the network host and bind the 32-bit IP address to a 48-bit MAC address. A network station can use ARP across a single network only, and the network hardware must support physical broadcasts.

If a network station wants to send a packet to a host but knows only the host IP address, the network station uses ARP to determine the physical address of the host as follows:

1. The network station broadcasts a special packet, called an ARP request, that asks the host at the specified IP address to respond with its physical address.
2. All network hosts receive the broadcast message.
3. Only the specified host responds with its hardware address.
4. The network station then maps the host IP address to its physical address and saves the results in an address resolution table for future use.
5. The network station ARP table displays the association of the known MAC addresses to IP addresses.

The lifetime for the learned MAC addresses is a configurable parameter. The switch executes ARP lookups when this timer expires.

The default timeout value for ARP entries is 6 hours.

Static ARP

In addition to the dynamic ARP mechanism, the Ethernet Routing Switch supports a static mechanism that allows for static ARP entries to be added. With Static ARP, you can manually associate a device MAC address to an IP address. You can add and delete individual static ARP entries on the switch.

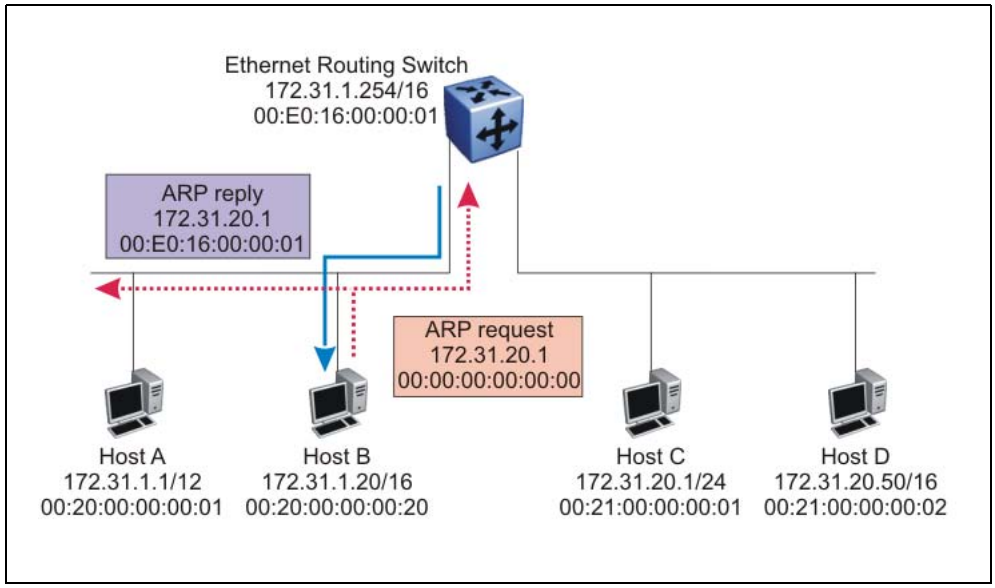
Proxy ARP

Proxy ARP allows the Ethernet Routing Switch to respond to an ARP request from a locally attached host that is intended for a remote destination. It does so by sending an ARP response back to the local host with the MAC address of the switch interface that is connected to the host subnet. The reply is generated only if the switch has an active route to the destination network.

With Proxy ARP enabled, the connected host can reach remote subnets without the need to configure default gateways.

The following figure is an example of proxy ARP operation. In this example, host B wants to send traffic to host C, so host B sends an ARP request for host C. However, the Nortel Ethernet Routing Switch 2500 Series is between the two hosts, so the ARP message does not reach host C. To enable communication between the two hosts, the Nortel Ethernet Routing Switch 2500 Series intercepts the message and responds to the ARP request with the IP address of host C but with the MAC address of the switch itself. Host B then updates its ARP table with the received information.

Figure 9
Proxy ARP Operation



Nortel recommends Proxy ARP as a temporary fix only, for example, if you are gradually moving hosts from one addressing scheme to another and you still want to maintain connectivity between the disparately-addressed devices. You do not want Proxy ARP running as a general rule because it causes hosts to generate ARP messages for every address that they want to reach on the Internet.

IP blocking for stacks

IP blocking is a Layer 3 feature of the Nortel Ethernet Routing Switch 2500 Series that provides safeguards for a stack where Layer 3 VLANs have port members across multiple stack units. IP Blocking is used whenever a unit leaves a stack or is rebooting inside the context of a stack. Depending on the setting in use, Layer 3 functionality is either continued or blocked by this feature.

You can set the IP Blocking mode on the base unit to either none or full.

When IP blocking is set to full, if any units leave the stack, those units run in Layer 2 mode. No Layer 3 settings remain on the units.

When IP blocking is set to none, if any units leave the stack, the Layer 3 configurations applied to the stack are still applied on the individual units.

In a stack environment of 2 units, Nortel recommends that you use IP blocking mode none. In this case, you can expect the following functional characteristics:

- If either the stack base unit or nonbase unit becomes nonoperational, Layer 3 functionality continues to run on the remaining unit.

A disadvantage of this configuration is that if the nonoperational unit does not rejoin the stack, address duplication occurs.

In stack environments of more than 2 units, Nortel recommends that you use IP blocking mode full. In this case, you can expect the following functional characteristics:

- If the stack base unit becomes nonoperational, the following occurs:
  - The temporary base unit takes over base unit duties.
  - The temporary base unit takes over responsibility to manage Layer 3 functionality in the stack. When this occurs, the system updates the MAC addresses associated with each routing interface to be offset from the temporary base unit MAC address (rather than the base unit MAC address). During this period, some minor disruption may occur to routing traffic until end stations update their ARP cache with the new router MAC addresses. The Nortel Ethernet Routing Switch 2500 Series sends out gratuitous ARP messages on each routed VLAN for 5 minutes at 15 second intervals to facilitate quick failover in this instance.
  - If the nonoperational base unit does not rejoin the stack, no Layer 3 functionality runs on the unit.
- If a stack nonbase unit becomes nonoperational, the following occurs:
  - The stack continues to run normally with the base unit controlling Layer 3 functionality.
  - If the nonoperational nonbase unit does not rejoin the stack, no Layer 3 functionality runs on the unit.

By default, the IP blocking mode is none (disabled).

Routing feature capabilities and limitations

The following list describes the routing feature capabilities and limitations on the Ethernet Routing Switch:

- Nonlocal static routes are not available for this release. For a route to become active, the corresponding next-hop IP address must be reachable through a directly connected subnet.
- A maximum of 256 local routes, and up to 32 static routes including the default route (Destination = 0.0.0.0 Mask = 0.0.0.0) are supported.
- The maximum number of management routes is 4.
- The maximum number of dynamic ARP entries is 1000.
- The maximum number of static ARP entries is 256.

- When adding a static ARP entry for a VLAN subnet, the IP address associated with the MAC address must be in the subnet for the VLAN. Otherwise the following error message is returned:

```
% Cannot modify settings
IP address does not match with VLAN subnet.
```

- UDP broadcast forwarding supports the following capabilities:
  - — You can configure a maximum of 128 UDP port/protocol entries.
  - — You can configure a maximum of 128 UDP forwarding lists.
  - — You can configure a maximum of 16 ports (with their IP addresses) in one forwarding list.
  - — You can bind a maximum of 16 VLANs to the same UDP forwarding list.

IGMP fundamentals

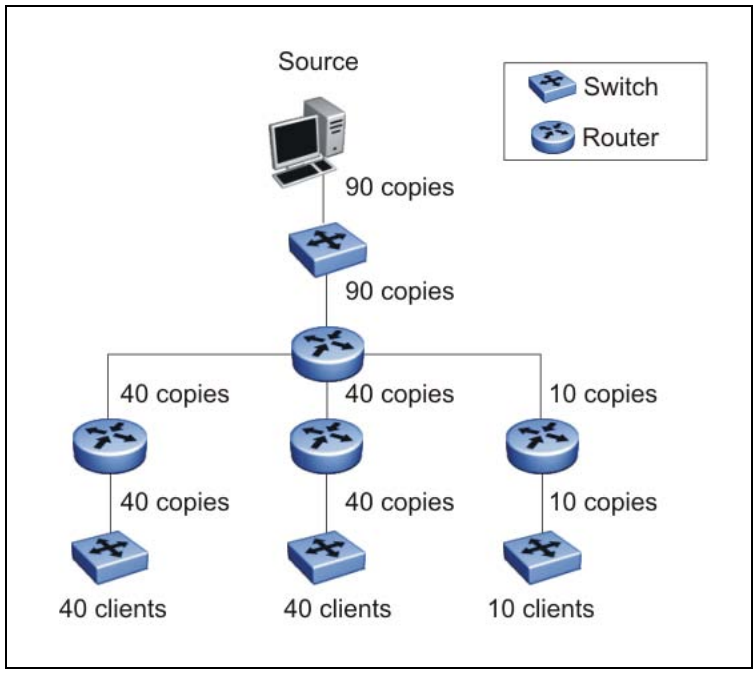
This chapter provides an overview of IP multicast and Internet Group Management Protocol (IGMP). To support multicast traffic, the Nortel Ethernet Routing Switch 2500 Series provides support for IGMP snooping.

Navigation

Overview of IP multicast

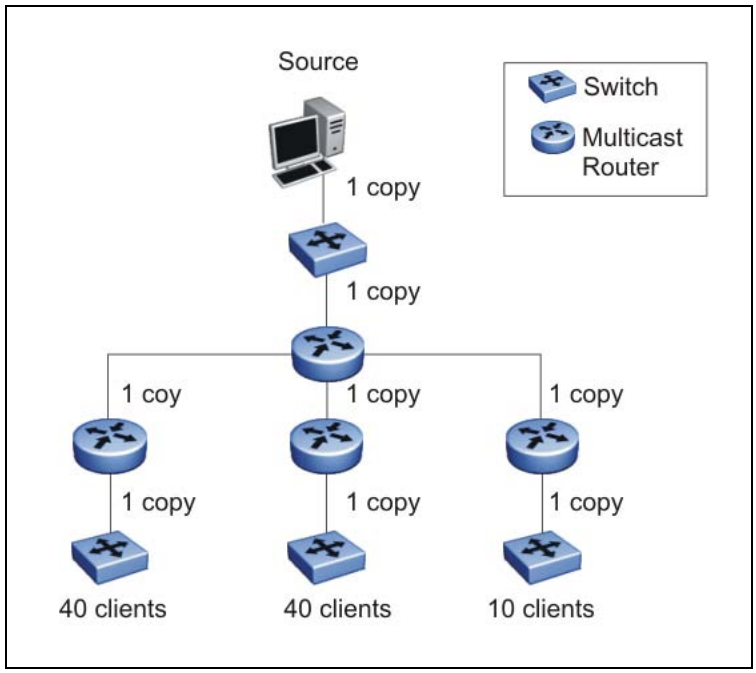
Most traditional network applications such as Web browsers and e-mail employ unicast connections in which each client sets up a separate connection to a server to access specific data. However, with certain applications such as audio and video streaming, more than one client accesses the same data at the same time. With these applications, if the server sends the same data to each individual client using unicast connections, the multiple connections waste both server and network capacity. For example, if a server offers a 1 Mbit/sec live video stream for each client, a 100 Mbit/sec network interface card (NIC) on the server could be completely saturated after 90 client connections. The following figure shows an example of this waste of resources.

Figure 10
Wasteful propagation of multiple copies of the same unicast stream



Multicasting provides the ability to transmit only one stream of data to all the interested clients at the same time. The following figure shows a simple example of how multicasting works. The source of the multicast data forwards only one stream to the nearest downstream router, and each subsequent downstream router forwards a copy of the same data stream to the recipients who are registered to receive it.

Figure 11
One stream replicated using multicasting



This one-to-many delivery mechanism is similar to broadcasting except that, while broadcasting transmits to all hosts in a network, multicasting transmits only to registered host groups. Because multicast applications transmit only one stream of data, which is then replicated to many receivers, multicasting saves a considerable amount of bandwidth.

Clients that want to receive the stream must register with the nearest multicast router to become a part of the receiving multicast group.

One downside to multicasting is that the multicast streams transmit data using User Datagram Protocol (UDP) packets, which are not as reliable as Transmission Control Protocol (TCP) packets.

Applications that use multicasting to transmit data include the following:

- multimedia conferencing
- real-time data multicasts (such as stock tickers)
- gaming and simulations

Multicast groups

To receive a multicast stream from a particular source, hosts must register with the nearest multicast router. The router adds all interested hosts to a multicast group, which is identified by a multicast IP address.

Multicast routers use Internet Group Membership Protocol (IGMP) to learn the existence of host group members on their directly attached subnets. To identify the hosts that want to be added to a group, a querier router sends out IGMP queries to each local network. A host that wants to belong to the group sends a response in the form of an IGMP membership report.

Each multicast router maintains a multicast routing table that lists each source, group (S,G) pair, which identifies the IP address of the source and the multicast address of the receiving group. For each (S,G) pair, the router maintains a list of downstream forwarding ports to which the multicast traffic is forwarded, and the upstream port where the multicast traffic is received.

Multicast addresses

Each multicast host group is assigned a unique multicast address. To reach all members of the group, a sender uses the multicast address as the destination address of the datagram.

An IP version 4 multicast address is a Class D address (the high-order bits are set to 1110) from 224.0.1.0 to 239.255.255.255. These addresses are assigned statically for use by permanent groups and dynamically for use by transient groups.

On the Ethernet Routing Switch 2500 Series, you cannot use 24-bit subnets like 224.0.0.0/24 and 224.128.0.0/24 for multicast data traffic. This restriction applies to the entire multicast address range from 224.0.0.0/8 to 239.128.0.0/8.

IGMP overview

IGMP is the Layer 3 protocol used by IP multicast routers to learn the existence of multicast group members on their directly attached subnets (see RFC 2236). With IGMP, hosts can register their desired group memberships to their local querier router.

A multicast querier router communicates with hosts on a local network by sending IGMP queries. The router periodically sends a general query message to each local network of the router. A host that wants to join a multicast group sends a response in the form of a membership report requesting registration with a group. After the querier router registers hosts to a group, it forwards all incoming multicast group packets to the registered host networks. As long as any host on a subnet continues to participate in the group, all hosts, including nonparticipating end stations on that subnet, receive the IP Multicast stream.

IGMP versions are backward compatible and can all exist together on a multicast network.

The following sections provide more details on the differences between the different IGMP versions.

IGMPv1 operation

IGMP version 1 is the simplest of the IGMP versions and is widely deployed.

IGMPv1 supports the following two message types:

- 0x11 – Membership Query message. Packets are sent to the all-systems multicast group (224.0.0.1).
- 0x12 – Membership Report message. Packets are sent to the group that the host intends to join.

The IGMPv1 router periodically sends host membership queries (also known as general queries) to its attached local subnets to inquire if any hosts are interested in joining any multicast groups. The interval between queries is a configurable value on the router. A host that wants to join a multicast group sends a membership report message to the nearest router, one report for each joined multicast group. After receiving the report, the router adds the Multicast IP address and the host port to its forwarding table. The router then forwards any multicast traffic for that multicast IP address to all member ports.

The router keeps a list of multicast group memberships for each attached network, and a Group Membership Interval timer for each membership. Repeated IGMP membership reports refresh the timer. If no reports are received before the timer expires, the router sends a query message.

In some cases, the host does not wait for a query before it sends report messages to the router. Upon initialization, the host can immediately issue a report for each of the multicast groups that it supports. The router accepts and processes these asynchronous reports the same way it accepts requested reports.

IGMPv1 leave process

After hosts and routers are in a steady state, they communicate in a way that minimizes the exchange of queries and reports. The designated routers set up a path between the IP Multicast stream source and the end stations, and periodically query the end stations to determine whether they want to continue to participate. As long as any host on the subnet continues to participate, all hosts, including nonparticipating end stations on the subnet, receive the IP Multicast stream.

If all hosts on the subnet leave the group, the router continues to send general queries to the subnet. If no hosts send reports after three consecutive queries, the router determines that no group members are present on the subnet.

IGMPv2 operation

IGMPv2 extends the IGMPv1 features by implementing a host leave message to quickly report group membership termination to the routing protocol. Instead of routers sending multiple queries before determining that hosts have left a group, the hosts can send a leave message. This feature is important for multicast groups with highly volatile group membership.

The IGMPv2 join process is similar to the IGMPv1 join process.

IGMPv2 also implements a querier election process.

IGMPv2 adds support for the following three new message types:

- 0x11 – General Query and Group Specific Query message.
- 0x16 – Version 2 Membership Report (sent to the destination IP address of the group being reported)
- 0x17 – Version 2 Membership Leave message (sent to all-router [224.0.0.2] multicast address)

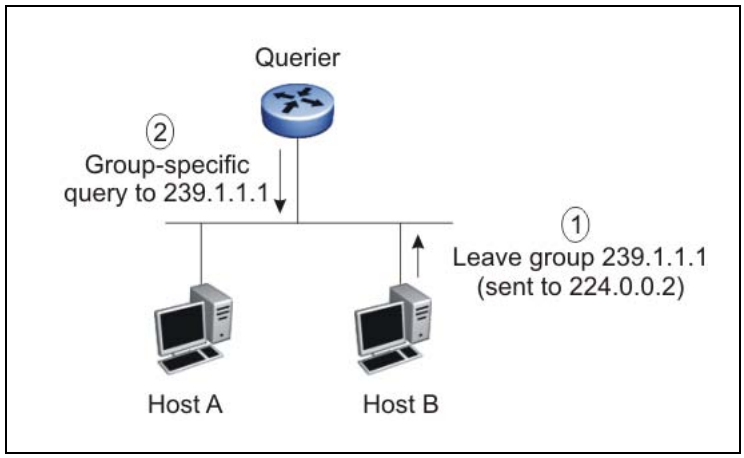
IGMPv2 also supports IGMPv1 messages.

Host leave process

With IGMPv2, if the host that issued the most recent report leaves a group, the host issues a leave message. The multicast router on the network then issues a group-specific query to determine whether other group members are present on the network. In the group-specific query message, the Group Address field is the group being queried (the Group Address field is 0 for the General Query message). If no host responds to the query, the router determines that no members belonging to that group exist on that interface.

The following figure shows an example of how IGMPv2 works.

Figure 12
IGMPv2



In this example, the following occurs:

- The host sends a leave message (to 224.0.0.2).
- The router sends a group-specific query to group 239.1.1.1.
- No IGMP report is received.
- Group 239.1.1.1 times out.

Querier election process

Normally only one querier exists per subnet. When multiple IGMPv2 routers are present on a network, the router with the lowest IP address is elected to send queries. All multicast routers start up as a querier on each attached network. If a multicast router receives a query message from a router with a lower IP address, the router with the higher IP address becomes a nonquerier on that network.

IGMP requests for comment

For additional information on IGMP, see the following requests for comment (RFC):

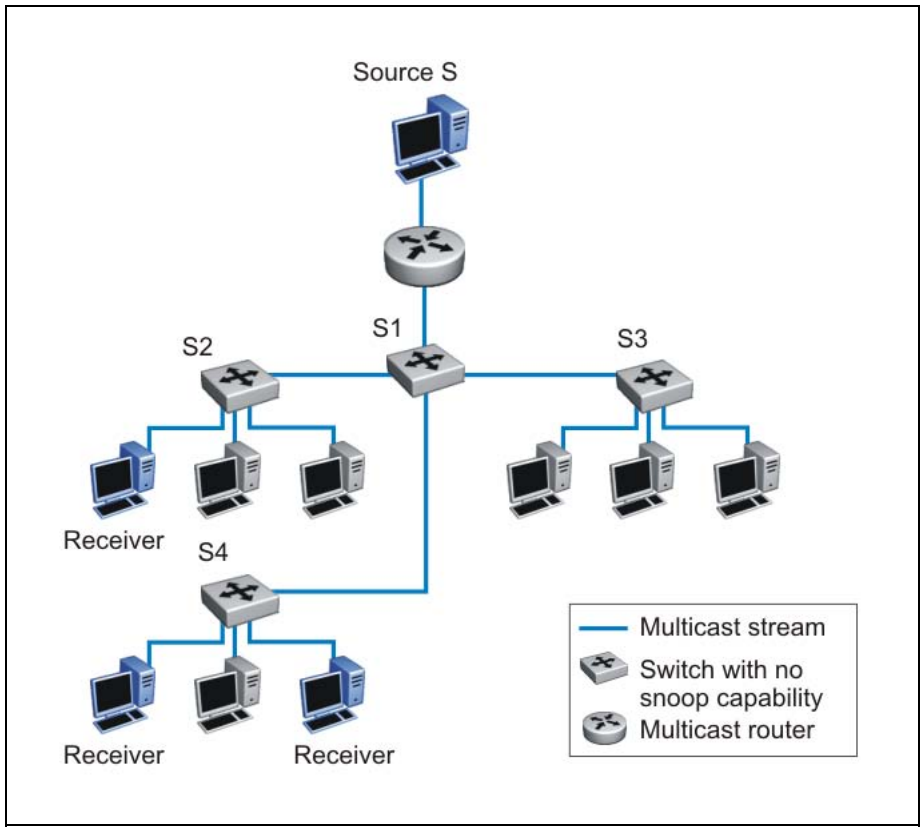
- For IGMPv1, see RFC 1112.
- For IGMPv2, see RFC 2236.
- For IGMP snooping, see RFC 4541.
- For IGMP management information bases (MIB), see RFC 2933.

IGMP snooping

If at least one host on a VLAN specifies that it is a member of a group, by default, the Nortel Ethernet Routing Switch 2500 Series forwards to that VLAN all datagrams bearing the multicast address of that group. All ports on the VLAN receive the traffic for that group.

The following figure shows an example of this scenario. Here, the IGMP source provides an IP Multicast stream to a designated router. Because the local network contains receivers, the designated router forwards the IP Multicast stream to the network. Switches without IGMP snoop enabled flood the IP Multicast traffic to all segments on the local subnet. The receivers requesting the traffic receive the desired stream, but so do all other hosts on the network. Although the nonparticipating end stations can filter the IP Multicast traffic, the IP Multicast traffic still exists on the subnet and consumes bandwidth.

Figure 13
IP multicast propagation on a LAN without IGMP snooping

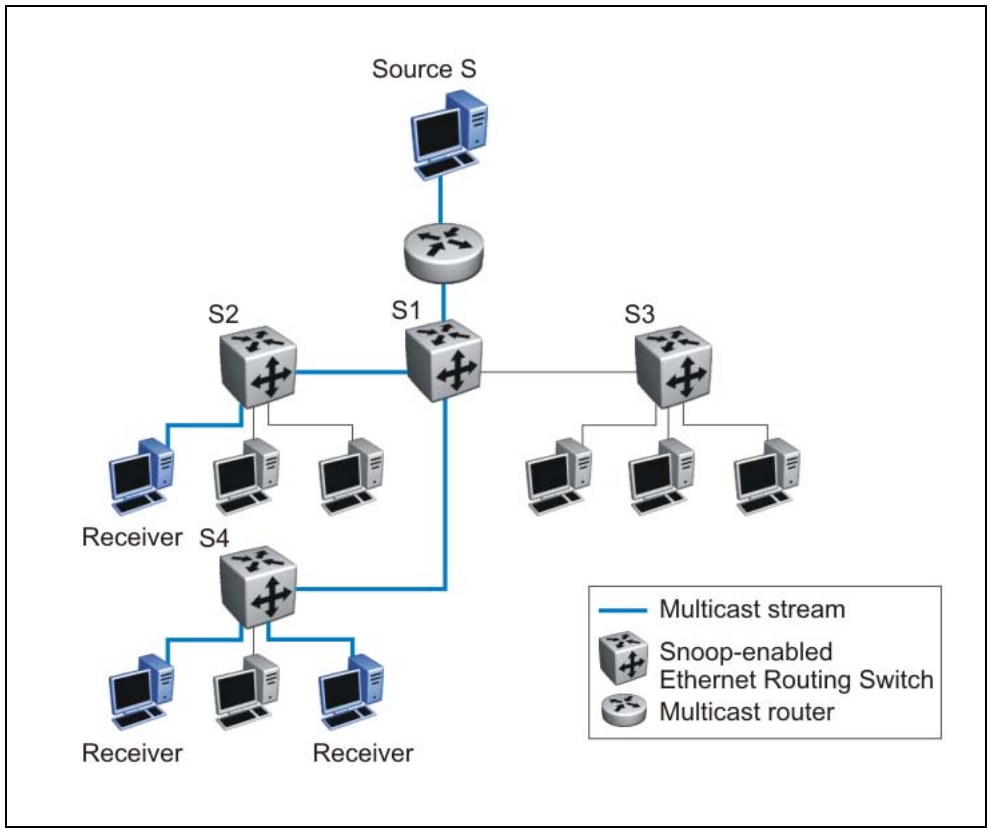


To prune ports that are not group members from receiving the group data, the Nortel Ethernet Routing Switch 2500 Series supports IGMP snoop for IGMPv1 and IGMPv2. With IGMP snoop enabled on a VLAN, the switch forwards the multicast group data to only those ports that are members of the group. When using IGMP snoop, VLANs can provide the same benefit as IP Multicast routers, but in the local area.

The Ethernet Routing Switch 2500 Series identifies multicast group members by listening to IGMP packets (IGMP reports, leaves, and queries) from each port. The switch suppresses the reports by not forwarding them out to other VLAN ports, forcing the members to continuously send their own reports. The switch uses the information gathered from the reports to build a list of group members. After the group members are identified, the switch blocks the IP Multicast stream from exiting any port that does not connect to a group member, thus conserving bandwidth.

As shown in the following figure, after the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast data.

Figure 14
Ethernet Routing Switch running IGMP snooping



The switch continues to forward the IGMP membership reports from the hosts to the multicast routers, and also forwards queries from multicast routers to all port members of the VLAN.

IGMP proxy

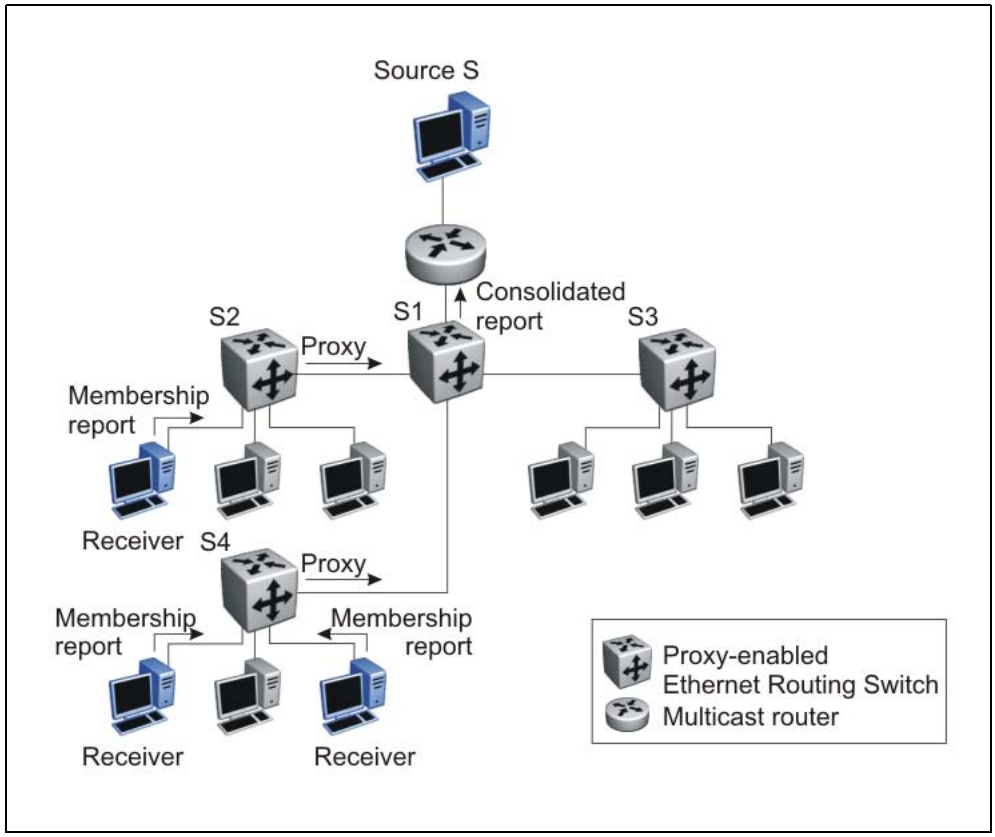
With IGMP snoop enabled, the switch can receive multiple reports for the same multicast group. Rather than forward each report upstream, the Ethernet Routing Switch 2500 Series can consolidate these multiple reports by using the IGMP proxy feature. With IGMP proxy enabled, if the switch receives multiple reports for the same multicast group, it does not transmit each report to the upstream multicast router. Instead, the switch forwards the first report to the querier and suppresses the rest. If new information emerges that another multicast group is added or that a query is received since the last report is transmitted upstream, the report is then forwarded to the multicast router ports.

To enable IGMP Proxy, you must first activate IGMP snooping.

In Figure 15 "Ethernet Routing Switch running IGMP proxy" (page 46), switches S1 to S4 represent a local area network (LAN) connected to an IP Multicast router. The router periodically sends Host Membership Queries to the LAN and listens for a response from end stations. All of the clients connected to switches S1 to S4 are aware of the queries from the router.

One client, connected to S2, responds with a host membership report. Switch S2 intercepts the report from that port, and generates a proxy report to its upstream neighbor, S1. Also, two clients connected to S4 respond with host membership reports, causing S4 to intercept the reports and to generate a consolidated proxy report to its upstream neighbor, S1.

Figure 15
Ethernet Routing Switch running IGMP proxy



Switch S1 treats the consolidated proxy reports from S2 and S4 as if they were reports from any client connected to its ports, and generates a consolidated proxy report to the designated router. In this scenario, the router receives a single consolidated report from that entire subnet.

The consolidated proxy report generated by the switch remains transparent to Layer 3 of the International Standardization Organization, Open Systems Interconnection (ISO/OSI) model. (The switch IP address and Media Access Control [MAC] address are not part of proxy report generation.) The last reporting IGMP group member in each VLAN represents all of the hosts in that VLAN and IGMP group.

Forwarding of reports

When forwarding IGMP membership reports from group members, the Ethernet Routing Switch 2500 Series forwards the reports only to those ports where multicast routers are attached. To do this, the switch maintains a list of multicast querier routers and the multicast router (mrouter) ports on which they are attached. The switch learns of the multicast querier routers by listening to the queries sent by the routers where source address is not 0.0.0.0.

Static mrouter port and nonquerier

If two IGMP routers are active on a VLAN, the router with the lower IP address is the querier, and the router with the higher IP address operates as a nonquerier. Only querier routers forward IGMP queries on the VLAN; nonqueriers do not forward IGMP queries. IGMP snoop considers the port on which the IGMP query is received as the active IGMP multicast router (mrouter) port. IGMP snoop is not aware of nonquerier IGMP routers.

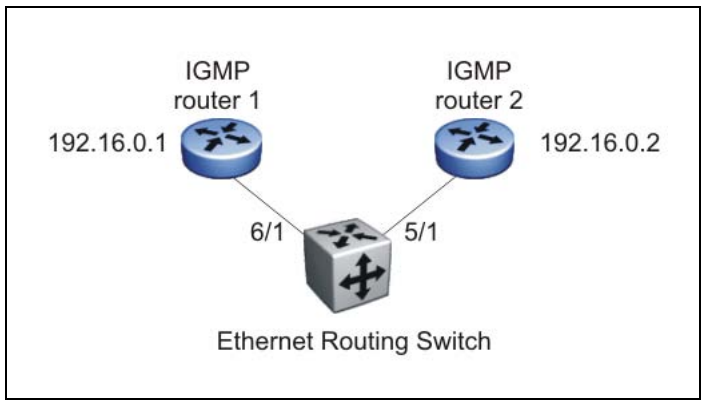
By default, IGMP snoop forwards reports to the IGMP querier router only. To allow the switch to forward reports to the nonquerier router as well, you can configure the port connected to the nonquerier as a static mrouter port.

Figure 16 "Static mrouter port and nonquerier" (page 48) shows how static mrouter ports operate. In this case, the Ethernet Routing Switch 2500 Series has port members 5/1 and 6/1 connected to IGMP routers in VLAN 10. Router 1 is the IGMP querier because it has a lower IP address than router 2. Router 2 is then considered the nonquerier.

By default, the switch learns of the multicast querier routers by listening to the IGMP queries. In this case, port 6/1 connected to querier router 1 is identified as an mrouter port.

To forward reports to IGMP router 2 as well, you can configure port 5/1 on the switch as a static mrouter port. In this case, the IGMP reports are forwarded to both routers.

Figure 16
Static mrouter port and nonquerier



Robustness value

As part of the IGMP snooping configuration, use the robustness value to configure the switch to offset expected packet loss on a subnet. If you expect a network to lose query packets, increase the robustness value.

This value is equal to the number of expected query packet losses for each query interval, plus 1. The range is from 2 to 255, and the default is 2. The default value of 2 means that one query for each query interval can be dropped without the querier aging out.

IGMP snooping configuration rules

The IGMP snooping feature operates according to specific configuration rules. When configuring your switch for IGMP snooping, consider the following rules that determine how the configuration reacts in any network topology:

- The switch supports up to 240 multicast groups.

  If the multicast group table reaches its limit, a new entry cannot be added with a JOIN message or a new sender identifying a new group. The multicast stream from the new sender is discarded by the hardware. New entries can be added again when the table is not full.

- You cannot configure port mirroring on a static mrouter port.
- If you configure a Multi-Link Trunk member as a static mrouter port, all the Multi-Link Trunk members become static mrouter ports. Also, if you remove a static mrouter port that is a Multi-Link Trunk member, all Multi-Link Trunk members are automatically removed as static mrouter port members.
- When you specify MAC addresses to be flooded on the switch the specified MAC addresses are flooded on all VLANs on the switch or stack. You cannot flood MAC addresses for a specific VLAN only.

- Static mrouter ports must be port members of at least one VLAN.
- If you configure a port as a static mrouter port, it is configured as a static mrouter port for all VLANs on that port. The IGMP configuration is propagated through all VLANs of that port.
- If you remove a static mrouter port, the membership for that port is removed from all VLANs of that port.
- When Spanning Tree is enabled, the switch learns IGMP groups only on ports that are *not* in Listening or Blocking Spanning Tree states (or, when in RSTP/MSTP mode, only on ports that are in the Designated state). The switch also learns the groups if STP is disabled on a port.
- The IGMP snooping feature is not Rate Limiting-dependent.
- You must enable the IGMP snooping feature before you can enable the IGMP proxy feature.
- You can specify static mrouter ports per VLAN and per IGMP version.

ATTENTION

Because IGMP snooping is set up per VLAN, all IGMP changes are implemented according to the VLAN configuration for the specified ports.

Default IGMP values

The following table lists the default IGMP values on the Ethernet Routing Switch.

Table 3
Default IGMP values

Parameters	Range	Default Value
Snooping	Enable/Disable	Disable
Version	1-2	2
Proxy	Enable/Disable	Disable
Query Interval	0-65535	125
Robustness Value	2-255	2

IGMP snooping interworking with Windows clients

This section describes an interworking issue between Windows clients and the Ethernet Routing Switches when IGMP snoop is enabled for multicast traffic.

Under normal IGMP snoop operation, as soon as a client joins a specific multicast group, the group is no longer unknown to the switch, and the switch sends the multicast stream only to the ports which request it.

Windows clients, in response to IGMPv2 queries from the switch, initially reply with IGMPv2 reports. However, after a period of time, the Windows clients switch to IGMPv3 reports, which the Ethernet Routing Switch does not recognize. In this case, the switch prunes the Windows client from the group and only forwards traffic to any non-Microsoft clients that are present in the group. If no other group members are left, the switch can revert to flooding all ports (in which case, the Windows client still receives the stream). Alternatively, the switch may be pruned altogether from the multicast group (in which case, the Windows client no longer receives the stream.)

To force a Windows client to only use IGMPv1 or IGMPv2 reports so that these symptoms do not occur, change the TCP/IP settings in the Windows Registry located under the following registry key:

```
HKEY_LOCAL_MACHINE
       \SYSTEM
            \CurrentControlSet
                 \Services
                      \Tcpip
                           \Parameters
```

The specific parameter which controls the IGMP Version is:

```
IGMPVersion
Key: Tcpip\Parameters
Value Type: REG_DWORD—Number
Valid Range: 2, 3, 4
Default: 4
```

To set the Windows Client to only utilize IGMPv2, change the IGMPVersion parameter to 3 (2 specifies IGMPv1, 3 specifies IGMPv2, and 4 specifies IGMPv3).

The IGMPVersion parameter may not be present in the list of the TCP/IP parameters. By default, the system assumes the IGMPv3 value (4). To configure the system for IGMPv2, create the parameter as a DWORD key in the registry and specify Decimal 3.

ATTENTION

If you edit the Windows registry incorrectly, you can severely damage your system. As a minimal safeguard, back up your system data before undertaking changes to the registry.

IP routing configuration using NNCLI

This chapter describes the procedures you can use to configure routable VLANs using the NNCLI.

The Nortel Ethernet Routing Switch 2500 Series are Layer 3 switches. This means that a regular Layer 2 VLAN becomes a routable Layer 3 VLAN if an IP address is attached to the VLAN. When routing is enabled in Layer 3 mode, every Layer 3 VLAN is capable of routing and carrying the management traffic. You can use any Layer 3 VLAN instead of the Management VLAN to manage the switch.

For more information about creating and configuring VLANs, see *Configuration — VLANs, Spanning Tree, and Link Aggregation* (NN47215-501).

IP routing configuration procedures

To configure inter-VLAN routing on the switch, perform the following steps:

Step	Action
1	Enable IP routing globally.
2	Assign IP addresses to multiple VLANs. Routing is automatically enabled on the VLAN when you assign an IP address to it.

—End—

In the above procedure, you are not required to enable IP routing as the first step. You can configure all IP routing parameters on the Nortel Ethernet Routing Switch 2500 Series before you enable routing on the switch.

Navigation

- "Configuring global IP routing status" (page 52)

Configuring global IP routing status

Use this procedure to enable and disable global routing at the switch level. By default, routing is disabled.

Procedure steps

Step	Action
1	To configure the status of IP routing on the switch, enter the following from the Global Configuration mode: `[no] ip routing`

—End—

Variable definitions

The following table describes the **`ip routing`** command variables.

Variable	Value
no	Disables IP routing on the switch.

Displaying global IP routing status

Use this command to display the status of IP routing on the switch.

Procedure steps

Step	Action
1	To display the status of IP routing on the switch, enter the following from the User EXEC mode: `show ip routing`

—End—

Configuring an IP address for a VLAN

To enable routing an a VLAN, you must first configure an IP address on the VLAN.

Procedure steps

Step	Action
1	To configure an IP address on a VLAN, enter the following from the VLAN Interface Configuration mode: `[no] ip address <ipaddr> <mask> [<MAC-offset>]`

—End—

Variable definitions

The following table describes the **`ip address`** command variables.

Variable	Value
[no]	Removes the configured IP address and disables routing on the VLAN.
<ipaddr>	Specifies the IP address to attach to the VLAN.
<mask>	Specifies the subnet mask to attach to the VLAN
[<MAC-offset>]	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address. The valid range is 1-256. Specify the value 1 for the Management VLAN only. If no MAC offset is specified, the switch applies one automatically.

Configuring IP routing status on a VLAN

Use this procedure to enable and disable routing for a particular VLAN.

Procedure steps

Step	Action
1	To configure the status of IP routing on a VLAN, enter the following from the VLAN Interface Configuration mode: `[default] [no] ip routing`

—End—

Variable definitions

The following table describes the **ip routing** command variables.

Variable	Value
default	Disables IP routing on the VLAN.
no	Disables IP routing on the VLAN.

Displaying the IP address configuration and routing status for a VLAN

Use this procedure to display the IP address configuration and the status of routing on a VLAN.

Procedure steps

Step	Action
1	To display the IP address configuration on a VLAN, enter the following from the Privileged Exec mode: **show vlan ip [vid <vid>]**

—End—

Variable definitions

The following table describes the **show vlan ip** command variables.

Variable	Value
[vid <vid>]	Specifies the VLAN ID of the VLAN to be displayed. Range is 1-4094.

Job aid

The following table shows the field descriptions for the **show vlan ip** command.

Field	Description
Vid	Specifies the VLAN ID.
ifIndex	Specifies an Index entry for the interface.
Address	Specifies the IP address associated with the VLAN.
Mask	Specifies the mask.
MacAddress	Specifies the MAC address associated with the VLAN.

Field	Description
Offset	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address.
Routing	Specifies the status of routing on the VLAN: enabled or disabled.

Displaying IP routes

Use this procedure to display all active routes on the switch.

Procedure steps

Step	Action
1	To display IP routes, enter the following from the User EXEC command mode: `show ip route [<dest-ip>] [-s <subnet> <mask>]`
	—End—

Variable definitions

The following table describes the **`show ip route`** command variables.

Variable	Value
<dest-ip>	Specifies the destination IP address of the routes to display.
[-s <subnet> <mask>]	Specifies the destination subnet of the routes to display.

Job aid

The following table shows the field descriptions for the **`show ip route`** command.

Field	Description
DST	Identifies the route destination.
MASK	Identifies the route mask.
NEXT	Identifies the next hop in the route.
COST	Identifies the route cost.
VLAN	Identifies the VLAN ID on the route.
PORT	Specifies the ports.
PROT	Specifies the routing protocols. For this release, options are LOC (local route) or STAT (static route).

Field	Description
TYPE	Indicates the type of route as described by the Type Legend in the NNCLI command display.
PRF	Specifies the route preference.

Static route configuration using NNCLI

This chapter describes the procedures you can use to configure static routes using the NNCLI.

Navigation

Configuring a static route

Create static routes to manually configure a path to destination IP address prefixes.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLANs to be routed.

Procedure steps

Step	Action
1	To configure a static route, enter the following from the Global Configuration command mode: `[no] ip route <dest-ip> <mask> <next-hop> [<cost>] [disable] [enable] [weight <cost>]`

—End—

Variable definitions

The following table describes the **ip route** command variables.

Variable	Value
[no]	Removes the specified static route.
<dest-ip>	Specifies the destination IP address for the route being added. 0.0.0.0 is considered the default route.
<mask>	Specifies the destination subnet mask for the route being added.
<next-hop>	Specifies the next hop IP address for the route being added.
[<cost>]	Specifies the weight, or cost, of the route being added. Range is 1-65535.
[enable]	Enables the specified static route.
[disable]	Disables the specified static route.
[weight <cost>]	Changes the weight, or cost, of an existing static route. Range is 1-65535.

Displaying static routes

Use this procedure to display all static routes, whether these routes are active or inactive.

Procedure steps

Step	Action
1	To display a static route, enter the following from the User EXEC command mode: **show ip route static [<dest-ip>] [-s <subnet> <mask>]**

—End—

Variable definitions

The following table describes the **show ip route static** command variables.

Variable	Value
<dest-ip>	Specifies the destination IP address of the static routes to display.
[-s <subnet> <mask>]	Specifies the destination subnet of the routes to display.

Job aid

The following table shows the field descriptions for the **show ip route static** command.

Field	Description
DST	Identifies the route destination.
MASK	Identifies the route mask.
NEXT	Identifies the next hop in the route.
COST	Identifies the route cost.
PREF	Specifies the route preference.
LCLNHOP	Specifies the local next hop status.
STATUS	Specifies the static route status. Options are ACTIVE (in use and present in routing table) or INACTV (not in use and not present in routing table).
ENABLE	Specifies the administrative state of the static route. Options are TRUE (administratively enabled) or FALSE (administratively disabled).

Configuring a management route

Use this procedure to create a management route to the far end network, with a next-hop IP address from the management VLAN's subnet. You can configure a maximum of four management routes on the switch.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the management VLAN interface.

Procedure steps

Step	Action
1	To configure a static management route, enter the following from the Global Configuration command mode: `[no] ip mgmt route <dest-ip> <mask> <next-hop>`

—End—

Variable definitions

The following table describes the **ip mgmt route** command variables.

Variable	Value
[no]	Removes the specified management route.
<dest-ip>	Specifies the destination IP address for the route being added.
<mask>	Specifies the destination subnet mask for the route being added.
<next-hop>	Specifies the next hop IP address for the route being added.

Displaying the management routes

Use this procedure to display the static routes configured for the management VLAN.

Procedure steps

Step	Action
1	To display the static routes configured for the management VLAN, enter the following from the User EXEC mode: `show ip mgmt route`

—End—

Job aid

The following table shows the field descriptions for the **`show ip mgmt route`** command.

Field	Description
Destination IP	Identifies the route destination.
Subnet Mask	Identifies the route mask.
Gateway IP	Identifies the next hop in the route.

DHCP relay configuration using NNCLI

This chapter describes the procedures you can use to configure Dynamic Host Configuration Protocol (DHCP) relay using the NNCLI.

Prerequisites to DHCP relay configuration using NNCLI

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be set as the DHCP relay agent.
- Ensure that a route (local or static) to the destination DHCP server is available on the switch.

DHCP relay configuration procedures

To configure DHCP relay, perform the following steps:

Step	Action
1	Ensure that DHCP relay is enabled globally. (DHCP relay is enabled by default.)
2	Configure the DHCP relay forwarding path by specifying a local VLAN as the DHCP relay agent and the remote DHCP server as the destination.
3	Enable DHCP relay for the specific VLAN.

—End—

Navigation

- "Configuring global DHCP relay status" (page 62)
- "Displaying the global DHCP relay status" (page 62)
- "Specifying a local DHCP relay agent and remote DHCP server" (page 63)

Configuring global DHCP relay status

Use this procedure to configure the global DHCP relay status. DHCP relay is enabled by default.

Procedure steps

Step	Action
1	To configure the global DHCP relay status, enter the following from the Global Configuration mode: `[no] ip dhcp-relay`

—End—

Variable definitions

The following table describes the **`ip dhcp-relay`** command variables.

Variable	Value
[no]	Disables DHCP relay.

Displaying the global DHCP relay status

Use this procedure to display the current DHCP relay status for the switch.

Procedure steps

Step	Action
1	To display the global DHCP relay status, enter the following from the User EXEC command mode: `show ip dhcp-relay`

—End—

Specifying a local DHCP relay agent and remote DHCP server

Use this procedure to specify a local VLAN as a DHCP relay agent on the forwarding path to a remote DHCP server. The DHCP relay agent can forward DHCP client requests from the local network to the DHCP server in the remote network.

The DHCP relay feature is enabled by default, and the default mode is BootP-DHCP.

Procedure steps

Step	Action
1	To configure a VLAN as a DHCP relay agent, enter the following from the Global Configuration mode: **`[no] ip dhcp-relay fwd-path <relay-agent-ip> <DHCP-server> [enable] [disable] [mode {bootp | bootp-dhcp | dhcp}]`**

—End—

Variable definitions

The following table describes the **`ip dhcp-relay fwd-path`** command variables.

Variable	Value
[no]	Removes the specified DHCP forwarding path.
<relay-agent-ip>	Specifies the IP address of the VLAN that serves as the local DHCP relay agent.
<DHCP-server>	Specifies the address of the remote DHCP server to which DHCP packets are to be relayed.
[enable]	Enables the specified DHCP relay forwarding path.
[disable]	Disables the specified DHCP relay forwarding path.
[mode {bootp | bootp-dhcp | dhcp}]	Specifies the DHCP relay mode: • BootP only • BootP and DHCP • DHCP only If you do not specify a mode, the default DHCP and BootP is used.

Displaying the DHCP relay configuration

Use this procedure to display the current DHCP relay agent configuration.

Procedure steps

Step	Action
1	To display the DHCP relay configuration, enter the following from the User EXEC command mode: `show ip dhcp-relay fwd-path`

—End—

Job aid

The following table shows the field descriptions for the **`show ip dhcp-relay fwd-path`** command.

Field	Description
INTERFACE	Specifies the interface IP address of the DHCP relay agent.
SERVER	Specifies the IP address of the DHCP server.
ENABLE	Specifies whether DHCP is enabled.
MODE	Specifies the DHCP mode.

Configuring DHCP relay status and parameters on a VLAN

Use this procedure to configure the DHCP relay parameters on a VLAN. To enable DHCP relay on the VLAN, enter the command with no optional parameters.

Procedure steps

Step	Action
1	To configure DHCP relay on a VLAN, enter the following from the VLAN Interface Configuration mode: `[no] ip dhcp-relay [broadcast] [min-sec <min-sec>] [mode {bootp | dhcp | bootp_dhcp}]`

—End—

Variable definitions

The following table describes the **`ip dhcp-relay`** command variables.

Variable	Value
[no]	Disables DHCP relay on the specified VLAN.
[broadcast]	Enables the broadcast of DHCP reply packets to the DHCP clients on this VLAN interface.
min-sec <min-sec>	Indicates the min-sec value. The switch immediately forwards a BootP/DHCP packet if the secs field in the BootP/DHCP packet header is greater than the configured min-sec value; otherwise, the packet is dropped. Range is 0-65535. The default is 0.
mode {bootp | dhcp | bootp_dhcp}	Specifies the type of DHCP packets this VLAN supports: • bootp - Supports BootP only • dhcp - Supports DHCP only • bootp_dhcp - Supports both BootP and DHCP

Displaying the DHCP relay configuration for a VLAN

Use this procedure to display the current DHCP relay parameters configured for a VLAN.

Procedure steps

Step	Action
1	To display the DHCP relay VLAN parameters, enter the following from the Privileged EXEC command mode: **`show vlan dhcp-relay [<vid>]`**

—End—

Variable definitions

The following table describes the **`show vlan dhcp-relay`** command variables.

Variable	Value
[<vid>]	Specifies the VLAN ID of the VLAN to be displayed. Range is 1-4094.

Job aid

The following table shows the field descriptions for the **`show vlan dhcp-relay`** command.

Field	Description
IfIndex	Indicates the VLAN interface index.
MIN_SEC	Indicates the min-sec value. The switch immediately forwards a BootP/DHCP packet if the secs field in the BootP/DHCP packet header is greater than the configured min-sec value; otherwise, the packet is dropped.
ENABLED	Indicates whether DHCP relay is enabled on the VLAN.
MODE	Indicates the type of DHCP packets this interface supports. Options include none, BootP, DHCP, and both.
ALWAYS_ BROADCAST	Indicates whether DHCP reply packets are broadcast to the DHCP client on this VLAN interface.

Displaying DHCP relay counters

Use this procedure to display the current DHCP relay counters. This includes the number of requests and the number of replies.

Procedure steps

Step	Action
1	To display the DHCP relay counters, enter the following from the User EXEC command mode: `show ip dhcp-relay counters`

—End—

Job aid

The following table shows the field descriptions for the **`show ip dhcp-relay counters`** command.

Field	Description
INTERFACE	Indicates the interface IP address of the DHCP relay agent.
REQUESTS	Indicates the number of DHCP requests.
REPLIES	Indicates the number of DHCP replies.

Clearing DHCP relay counters for a VLAN

Use this procedure to clear the DHCP relay counters for a VLAN.

Procedure steps

Step	Action
1	To clear the DHCP relay counters, enter the following from the VLAN Interface Configuration command mode: `ip dhcp-relay clear-counters`

—End—

UDP broadcast forwarding configuration using NNCLI

This chapter describes the procedures you can use to configure UDP broadcast forwarding using NNCLI. UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address.

You cannot enable or disable the UDP broadcast forwarding feature on a global level. When you attach the first UDP forwarding list to a VLAN interface, the feature is enabled. When you remove the last UDP forwarding list from a VLAN, the feature is disabled.

Prerequisites to UDP broadcast forwarding using NNCLI

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a UDP forwarding interface.
- Ensure that a route (local or static) to the destination address is available on the switch.

ATTENTION

If you configure EAPOL on the switch, enable EAPOL before enabling UDP Forwarding, otherwise the UDP broadcast traffic matching UDP forward lists is forwarded regardless of the EAPOL port state (authorized, force unauthorized, or auto).

UDP broadcast forwarding configuration procedures

To configure UDP broadcast forwarding, perform the following steps:

Step	Action
1	Create UDP protocol entries that specify the protocol associated with each UDP port that you want to forward.

2 Create a UDP forwarding list that specifies the destination IP addresses for each forwarding UDP port. (You can create up to 128 UDP forwarding lists.)

3 Apply UDP forwarding lists to local VLAN interfaces.

—End—

Navigation

Configuring UDP protocol table entries

Use this procedure to create UDP protocol table entries that identify the protocols associated with specific UDP ports that you want to forward.

Procedure steps

Step	Action
1	To configure a UDP table entry, enter the following from the Global Configuration mode: `ip forward-protocol udp [<forwarding_port> <protocol_name>]`

—End—

Variable definitions

The following table describes the **`ip forward-protocol udp`** command variables.

Variable	Value
<forwarding_port>	Specifies the UDP port number. Range is 1-65535.
<protocol_name>	Specifies the UDP protocol name.

Displaying the UDP protocol table

Use this procedure to display the configured UDP protocol table entries.

Procedure steps

Step	Action
1	To display the UDP protocol table, enter the following from the User Exec mode: `show ip forward-protocol udp`

—End—

Job aid

The following table shows the field descriptions for the **`show ip forward-protocol udp`** command.

Field	Description
UDP_PORT	Indicates the UDP ports.
PROTOCOL_NAME	Indicates the name of the associated protocol.

Configuring a UDP forwarding list

Use this procedure to configure a UDP forwarding list, which associates UDP forwarding ports with destination IP addresses. Each forwarding list can contain multiple port/destination entries. You can configure a maximum of 16 port/destination entries in one forwarding list.

You can configure up to 128 forwarding lists.

Procedure steps

Step	Action
1	To configure a UDP port forwarding list, enter the following from the Global Configuration mode: `ip forward-protocol udp portfwdlist <forward_list> <udp_port> <dest_ip> [name <list_name>]`

—End—

Variable definitions

The following table describes the **ip forward-protocol udp portfwdlist** command variables.

Variable	Value
<forward_list>	Specifies the ID of the UDP forwarding list. Range is 1-128.
<udp_port>	Specifies the port on which the UDP forwarding originates.
<dest_ip>	Specifies the destination IP address for the UDP port.
<list_name>	Specifies the name of the UDP forwarding list being created (maximum 15 characters).

Applying a UDP forwarding list to a VLAN

Use this procedure to associate a UDP forwarding list with a VLAN interface (you can attach only one list at a time to a VLAN interface).

You can bind the same UDP forwarding list to a maximum of 16 different VLANs.

Procedure steps

Step	Action
1	To associate a UDP forwarding list to a VLAN, enter the following from the VLAN Interface Configuration mode: **ip forward-protocol udp [vlan <vid>] [portfwdlist <forward_list>] [broadcastmask <bcast_mask>] [maxttl <max_ttl>]**

—End—

Variable definitions

The following table describes the **ip forward-protocol udp** command variables.

Variable	Value
<vid>	Specifies the VLAN ID on which to attach the UDP forwarding list. This parameter is optional, and if not specified, the UDP forwarding list is applied to the interface specified in the **interface vlan** command.
<forward_list>	Specifies the ID of the UDP forwarding list to attach to the selected VLAN interface.

Variable	Value
<bcast_mask>	Specifies the 32-bit mask used by the selected VLAN interface to make forwarding decisions based on the destination IP address of the incoming UDP broadcast traffic. If you do not specify a broadcast mask value, the switch uses the mask of the interface to which the forwarding list is attached. (See Note 1.)
<max_ttl>	Specifies the time-to-live (TTL) value inserted in the IP headers of the forwarded UDP packets coming out of the selected VLAN interface. If you do not specify a TTL value, the default value (4) is used. (See Note 1.)
Note 1: If you specify maxttl and/or broadcastmask values with no portfwdlist specified, the switch saves the settings for this interface. If you subsequently attach portfwdlist to this interface without defining the maxttl and/or broadcastmask values, the saved parameters are automatically attached to the list. But, if when specifying the portfwdlist, you also specify the maxttl and/or broadcastmask, your specified properties are used, regardless of any previous configurations.	

Displaying the UDP broadcast forwarding configuration

Use this procedure to display the UDP broadcast forwarding configuration.

Procedure steps

Step	Action
1	To display the UDP broadcast forwarding configuration, enter the following from the User Exec mode: `show ip forward-protocol udp [interface [vlan <1-4094>]] [portfwdlist [<portlist>]`

—End—

Variable definitions

The following table describes the **`show ip forward-protocol udp`** command variables.

Variable	Value
[interface [vlan <1-4094>]]	Displays the configuration and statistics for a VLAN interface. If no VLAN is specified, the configuration for all UDP forwarding-enabled VLANs is displayed.
[portfwdlist [<forward_list>]	Displays the specified UDP forwarding list. If no list is specified, a summary of all forwarding lists is displayed.

Job aids

The following table shows the field descriptions for the **`show ip forward-protocol udp`** command.

Field	Description
UDP_PORT	Indicates the UDP ports.
PROTOCOL_NAME	Indicates the name of the protocol.

The following table shows the field descriptions for the **`show ip forward-protocol udp interfaces`** command.

Field	Description
INTF_ADDR	Indicates the IP address of the interface.
FWD LISTID	Identifies the UDP forwarding policy.
MAXTTL	Indicates the maximum TTL.
RXPKTS	Indicates the number of received packets.
FWDPKTS	Indicates the number of forwarded packets.
DRPDEST UNREACH	Indicates the number of dropped packets that cannot reach the destination.
DRP_UNKNOWN PROTOCOL	Indicates the number of packets dropped with an unknown protocol.
BDCASTMASK	Indicates the value of the broadcast mask.

The following table shows the field descriptions for the **`show ip forward-protocol udp portfwdlist`** command.

Field	Description
LIST_ID	Specifies the UDP forwarding policy number.
NAME	Specifies the name of the UDP forwarding policy.

Clearing UDP broadcast counters on an interface

Use this procedure to clear the UDP broadcast counters on an interface.

Procedure steps

Step	Action
1	To clear the UDP broadcast counters, enter the following from the Privileged Exec command mode: `clear ip forward-protocol udp counters <1-4094>`
	—End—

Variable definitions

The following table describes the **`clear ip forward-protocol udp counters`** command variables.

Variable	Value
<1-4094>	Specifies the VLAN ID.

Directed broadcasts configuration using NNCLI

This chapter describes the procedures you can use to configure and display the status of directed broadcasts using NNCLI.

Navigation

Configuring directed broadcasts

Use this procedure to enable directed broadcasts on the switch. By default, directed broadcasts are disabled.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a broadcast interface.
- Ensure that a route (local or static) to the destination address is available on the switch.

Procedure steps

Step	Action
1	To enable directed broadcasts, enter the following from the Global Configuration mode: `ip directed-broadcast enable`
	—End—

Displaying the directed broadcast configuration

Use this procedure to display the status of directed broadcasts on the switch. By default, directed broadcasts are disabled.

Procedure steps

Step	Action
1	To display directed broadcast status, enter the following from the User EXEC mode: `show ip directed-broadcast`

—End—

Static ARP and Proxy ARP configuration using NNCLI

This chapter describes the procedures you can use to configure Static ARP, Proxy ARP, and display ARP entries using the NNCLI.

Navigation

Static ARP configuration

This section describes how to configure Static ARP using the NNCLI.

Configuring a static ARP entry

Use this procedure to configure a static ARP entry.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the target VLAN.

Procedure steps

Step	Action
1	To configure a static ARP entry, enter the following from the Global Configuration mode: `[no] ip arp <A.B.C.D> <aa:bb:cc:dd:ee:ff> <unit / port> [vid <1-4094>]`

—End—

Variable definitions

The following table describes the **ip arp** command variables.

Variable	Value
[no]	Removes the specified ARP entry.
<A.B.C.D>	Specifies the IP address of the device being set as a static ARP entry.
<aa:bb:cc:dd:ee:ff>	Specifies the MAC address of the device being set as a static ARP entry.
<unit / port>	Specifies the unit and port number to which the static ARP entry is being added.
vid <1 - 4094>	Specifies the VLAN ID to which the static ARP entry is being added.

Displaying the ARP table

Use the following procedures to display the ARP table, configure a global timeout for ARP entries, and clear the ARP cache.

Navigation

- "Displaying ARP entries" (page 80)
- "Configuring a global timeout for ARP entries" (page 81)
- "Clearing the ARP cache" (page 82)

Displaying ARP entries

Use this procedure to display ARP entries.

Procedure steps

Step	Action
1	To display ARP entries, enter the following from the User Exec mode: **show arp-table** **OR** **show ip arp [<ip-addr>]** **[-s <subnet> <mask>]** **[static <ip-addr> [-s <subnet> <mask>]]** **[dynamic <ip-addr> [-s <subnet> <mask>]]** **[summary]** The **show ip arp** command is invalid if the switch is not in Layer 3 mode.

—End—

Variable definitions

The following table describes the **show ip arp** command variables.

Variable	Value
<ip-addr>	Specifies the IP address of the ARP entry to be displayed.
-s <subnet> <mask>	Displays ARP entries for the specified subnet only.
static <ip-addr> [-s <subnet> <mask>]	Displays static entries for the specified subnet. If you do not specify a subnet, all configured static entries are displayed, including those without a valid route.
dynamic <ip-addr> [-s <subnet> <mask>]	Displays dynamic entries for the specified subnet. If you do not specify a subnet, all dynamic entries are displayed.
summary	Displays a summary of ARP entries.

Job aid

The following table shows the field descriptions for **show arp-table** and **show ip arp** commands.

Field	Description
IP Address	Specifies the IP address of the ARP entry.
Age (min)	Displays the ARP age time.
MAC Address	Specifies the MAC address of the ARP entry.
VLAN-Unit/Port/Trunk	Specifies the VLAN/port of the ARP entry.
Flags	Specifies the type of ARP entry: S=Static, D=Dynamic, L=Local, B=Broadcast.

Configuring a global timeout for ARP entries

Use this procedure to configure an aging time for the ARP entries.

Procedure steps

Step	Action
1	To configure a global timeout for ARP entries, enter the following from the Global Configuration mode: **ip arp timeout <timeout>**

—End—

Variable definitions

The following table describes the **ip arp timeout** command variables.

Variable	Value
<timeout>	Specifies the amount of time in minutes before an ARP entry ages out. Range is 5-360. The default value is 360 minutes.

Clearing the ARP cache

Use this procedure to clear the cache of ARP entries.

Procedure steps

Step	Action
1	To clear the ARP cache, enter the following from the Global Configuration mode: **clear arp-cache**

—End—

Proxy ARP configuration

This section describes how to configure Proxy ARP using the NNCLI.

Navigation

- "Configuring proxy ARP status" (page 82)
- "Displaying proxy ARP status on a VLAN" (page 83)

Configuring proxy ARP status

Use this procedure to enable proxy ARP functionality on a VLAN. By default, proxy ARP is disabled.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a Proxy ARP interface.

Procedure steps

Step	Action
1	To configure proxy ARP status on a VLAN, enter the following from the VLAN Interface Configuration mode: `[default] [no] ip arp-proxy enable`

—End—

Variable definitions

The following table describes the **`ip arp-proxy enable`** command variables.

Variable	Value
[default]	Disables proxy ARP functionality on the VLAN.
[no]	Disables proxy ARP functionality on the VLAN.

Displaying proxy ARP status on a VLAN

Use this procedure to display the status of proxy ARP on a VLAN.

Procedure steps

Step	Action
1	To display proxy ARP status for a VLAN, enter the following from the User EXEC mode: `show ip arp-proxy interface [vlan <vid>]`

—End—

Variable definitions

The following table describes the **`show ip arp-proxy interface`** command variables.

Variable	Value
<vid>	Specifies the ID of the VLAN to display. Range is 1-4094.

Job aid

The following table shows the field descriptions for the **`show ip arp-proxy interface`** command.

Field	Description
Vlan	Identifies a VLAN.
Proxy ARP status	Specifies the status of Proxy ARP on the VLAN.

IP blocking configuration using NNCLI

This chapter describes the procedures you can use to configure and display the status of IP blocking in a stack using NNCLI.

Navigation

Configuring IP blocking for a stack

Use this procedure to set the IP blocking mode in the stack.

Procedure steps

Step	Action
1	To configure IP blocking, enter the following from the Global Configuration mode: `ip blocking-mode {full | none}`

—End—

Variable definitions

The following table describes the **`ip blocking-mode`** command variables.

Variable	Value
full	Select this parameter to set IP blocking to full, which never allows a duplicate IP address in a stack.
none	Select this parameter to set IP blocking to none, which allows duplicate IP addresses unconditionally.

Displaying IP blocking status

Use this command to display the status of IP blocking on the switch.

Procedure steps

Step	Action
1	To display the IP blocking mode on the switch, enter the following from the User EXEC mode: `show ip blocking-mode`
2	To display the IP blocking state on the switch, enter the following from the User EXEC mode: `show ip-blocking`

—End—

IGMP snooping configuration using NNCLI

This chapter describes the procedures you can use to configure and display IGMP snooping parameters using NNCLI.

Navigation

Configuring IGMP snooping on a VLAN

Enable IGMP snooping on a VLAN to forward the multicast data to only those ports that are members of the multicast group.

IGMP snooping is disabled by default.

Procedure steps

Step	Action
1	To enable IGMP snooping, enter the following from the Global Configuration command mode: `[default] [no] vlan igmp <vid> snooping {enable | disable}`
	—End—

Variable definitions

The following table describes the **vlan igmp snooping** command variables.

Variable	Value
default	Disables IGMP snooping on the selected VLAN.
no	Disables IGMP snooping on the selected VLAN.
<vid>	Specifies the VLAN ID.
enable	Enables IGMP snooping on the selected VLAN.
disable	Disables IGMP snooping on the selected VLAN.

Configuring IGMP proxy on a VLAN

Use this procedure to enable IGMP proxy on a snoop-enabled VLAN. With IGMP proxy enabled, the switch consolidates incoming report messages into one proxy report for that group.

IGMP proxy is disabled by default.

Prerequisites

- Enable snoop on the VLAN.

Procedure steps

Step	Action
1	To enable IGMP proxy, enter the following from the Global Configuration command mode: **[default] [no] vlan igmp <vid> proxy {enable | disable}**

—End—

Variable definitions

The following table describes the **vlan igmp proxy** command variables.

Variable	Value
default	Disables IGMP proxy on the selected VLAN.

Variable	Value
no	Disables IGMP proxy on the selected VLAN.
<vid>	Specifies the VLAN ID.
enable	Enables IGMP proxy on the selected VLAN.
disable	Disables IGMP proxy on the selected VLAN.

Configuring static mrouter ports on a VLAN

IGMP snoop considers the port on which the IGMP query is received as the active IGMP multicast router (mrouter) port. By default, the switch forwards incoming IGMP Membership Reports only to the active mrouter port.

To forward the IGMP reports to additional ports, you can configure the additional ports as static mrouter ports.

ATTENTION

The static mroute port version must match the IGMP version configured on the interface (VLAN) of the IGMP querier router.

Procedure steps

Step	Action
1	To configure IGMPv1 or IGMPv2 static mrouter ports, enter the following from the Global Configuration command mode: `[no] vlan igmp <vid> {v1-members | v2-members} {add | remove} <portlist>`

—End—

Variable definitions

The following table describes the **`vlan igmp {v1-members | v2-members}`** command variables.

Variable	Value
[no]	Removes the specified static mrouter ports.
<vid>	Specifies the VLAN on which to add the static mrouter ports.

Variable	Value
{v1-members | v2-members}	Specifies whether the static mrouter ports are IGMPv1 or IGMPv2.
<portlist>	Specifies the list of ports to add or remove as static mrouter ports.

Configuring IGMP parameters on a VLAN

Use this procedure to configure the IGMP parameters on a VLAN.

ATTENTION

The query interval and robustness values must be the same as those configured on the interface (VLAN) of the IGMP querier router.

Procedure steps

Step	Action

1	To configure IGMP parameters, enter the following from the Global Configuration command mode:
	`[default] vlan igmp <vid>`
	`[query-interval <query-int>]`
	`[robust-value <robust-val>]`

—End—

Variable definitions

The following table describes the **`vlan igmp [query-interval] [robust-value]`** command variables.

Variable	Value
default	Sets the selected parameter to the default value. If no parameters are specified, snoop is disabled and all IGMP parameters are set to their defaults.

Variable	Value
<query-int>	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. The range is 1–65535. The default value is 125 seconds.
<robust-val>	Specifies tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1. If you expect a network to lose query packets, you must increase the robustness value. Ensure that the robustness value is the same as the configured value on the multicast router (IGMP querier). The range is from 0 –255, and the default is 2. The default value of 2 means that one query for each query interval can be dropped without the querier aging out.

Displaying IGMP interface information

Use this procedure to display IGMP interface information.

Procedure steps

Step	Action
1	To display the IGMP interface information, enter the following from the Privileged Exec command mode: **`show vlan igmp <vid>`**

—End—

Variable definitions

The following table describes the **`show vlan igmp`** command variables.

Variable	Value
[vid <vid>]	Specifies the VLAN ID for which to display IGMP information. Range is 1-4094.

Job aid

The following table shows the field descriptions for the **`show vlan igmp`** command.

Field	Description
Snooping	Indicates whether snooping is enabled or disabled.
Proxy	Indicates whether proxy snoop is enabled or disabled.
Robust Value	Indicates the robustness value configured for expected packet loss on the interface.
Query Time	Indicates the frequency (in seconds) at which host query packets are transmitted on the interface.
IGMPv1 Static Router Ports	Indicates the IGMPv1 static mrouter ports.
IGMPv2 Static Router Ports	Indicates the IGMPv2 static mrouter ports.

Displaying IGMP group membership information

Display the IGMP group membership information to show the learned multicast groups and the attached ports.

Procedure steps

Step	Action
1	To display IGMP group information, enter the following from the Privileged Exec command mode: **`show vlan multicast membership <vid>`**

—End—

Variable definitions

The following table describes the **`show vlan multicast membership`** command variables.

Variable	Value
<vid>	Specifies the VLAN for which to display IP Multicast memberships.

Job aid

The following table shows the field descriptions for the **`show vlan multicast membership`** command.

Field	Description
Multicast Group Address	Indicates the multicast group address.
In Port	Indicates the physical interface or the logical interface (VLAN) that received group reports from various sources.

IP routing configuration using Device Manager

This chapter describes the procedures you can use to configure routable VLANs using Device Manager.

The Nortel Ethernet Routing Switch 2500 Series are Layer 3 switches. This means that a regular Layer 2 VLAN becomes a routable Layer 3 VLAN if an IP address is attached to the VLAN. When routing is enabled in Layer 3 mode, every Layer 3 VLAN is capable of routing as well as carrying the management traffic. You can use any Layer 3 VLAN instead of the Management VLAN to manage the switch.

IP routing configuration procedures

To configure IP routing on VLANs, perform the following steps:

Step	Action
1	Enable IP routing globally.
2	Assign an IP address to a specific VLAN.

—End—

In the above procedure, you are not required to enable IP routing as the first step. You can configure all IP routing parameters on the Nortel Ethernet Routing Switch 2500 Series before you enable routing on the switch.

Navigation

- "Configuring global IP routing status and ARP lifetime" (page 96)
- "Configuring an IP address and enabling routing for a VLAN" (page 97)
- "Displaying configured IP Addresses" (page 98)

Configuring global IP routing status and ARP lifetime

Use this procedure to enable and disable global routing at the switch level. By default, routing is disabled.

You can also use this procedure to configure the ARP lifetime on the switch.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > IP**. The IP dialog box appears with the Globals tab displayed.
2	To enable routing, select the **forwarding** option in the **Forwarding** text box.
3	To configure the ARP lifetime, modify the value in the **ARPLIfeTime** box.
4	Click **Apply**.

—End—

Variable definitions

The following table describes the Globals tab fields.

Field	Description
Forwarding	Indicates whether routing is enabled (forwarding) or disabled (nonforwarding) on the switch.
DefaultTTL	Indicates the default time-to-live (TTL) value for a routed packet. TTL is the maximum number of seconds elapsed before a packet is discarded. The value is inserted in the TTL field of the IP header of datagrams when one is not supplied by the transport layer protocol. The TTL field is also reduced by one each time the packet passes through a router. Range is 1-255. Default value is 64 seconds.
ReasmTimeout	Indicates the maximum number of seconds that received fragments are held while they await reassembly at this entity. Default value is 60 seconds.
ARPLifeTime	Specifies the lifetime in minutes of an ARP entry within the system. Range is 5-360. Default is 360 minutes.

Configuring an IP address and enabling routing for a VLAN

Use this procedure to configure an IP address and enable routing for a VLAN.

Prerequisites

- Enable routing globally on the switch.

Procedure steps

Step	Action
1	From the Device Manager menu, select **VLAN > VLANs**.
2	Select a VLAN.
3	Click **IP**. The IP, VLAN dialog box appears with the IP Address tab selected.
4	Click **Insert**. The Insert IP Address dialog box appears.
5	Type the IP address, subnet mask, and MAC address offset in the fields provided.
6	Click **Insert**.

—End—

Variable definitions

The following table describes the IP Address tab fields.

Field	Description
IpAddress	Specifies the IP address to associate with the selected VLAN.
NetMask	Specifies the subnet mask.
VlanId	Specifies the VLAN ID. A value of -1 indicates that the VLAN ID is ignored.
MacOffset	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address. The valid range is 1-256. Specify the value 1 for the Management VLAN only. If no MAC offset is specified, the switch applies one automatically.

Displaying configured IP Addresses

Use this procedure to display configured IP addresses on the switch.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > IP**.
2	Select the **Addresses** tab.

—End—

Variable definitions

The following table describes the Addresses tab fields.

Field	Description
IfIndex	Specifies the VLAN ID.
IpAddress	Specifies the associated IP address.
NetMask	Specifies the subnet mask.
BcastAddrFormat	Specifies the format of the IP broadcast address.
ReasmMaxSize	Specifies the size of the largest IP datagram that this entity can reassemble from fragmented datagrams received on this interface.
VlanId	Specifies the VLAN ID number. A value of -1 indicates that the VLAN ID is ignored.
MacOffset	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address.

Static route configuration using Device Manager

This chapter describes the procedures you can use to configure static routes using Device Manager.

Navigation

Configuring static routes

Use this procedure to configure static routes for the switch.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLANs to be routed.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > IP**.
2	Select the **Static Routes** tab.
3	Click **Insert**.

The Insert Static Routes dialog box appears.

4 In the fields provided, enter the information for the new static route.

5 Click **Insert**.

The new static route is displayed in the Static Routes tab.

—End—

Variable definitions

The following table describes the Static Routes tab fields.

Field	Description
Dest	Specifies the destination IP address of the route. 0.0.0.0 is considered the default route.
Mask	Specifies the destination mask of the route.
NextHop	Specifies the IP address of the next hop of this route.
Metric	Represents the cost of the static route. It is used to choose the best route (the one with the smallest cost) to a certain destination. The range is 1-65535. If this metric is not used, the value is set to -1.
IfIndex	Specifies the interface on which the static route is configured.
Enable	Specifies whether the route is administratively enabled (true) or disabled (false).
Status	Specifies the operational status of the route.

Displaying IP routes

Use this procedure to display the different routes known to the switch.

Routes are not be displayed until at least one port in the VLAN has link.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > IP**.
2	Select the **Routes** tab.

—End—

Variable definitions

The following table describes the Routes tab fields.

Field	Description
Dest	Specifies the destination address of the route.
Mask	Specifies the subnet mask for the route.
NextHop	Specifies the next hop for the route.
HopOrMetric	Specifies the metric associated with the route.
Interface	Specifies the interface associated with the route.
Proto	Specifies the protocol associated with the route. For this release, options are local or static.
PathType	Specifies the route path type: • i: indirect • d: direct • B: best • U: unresolved
Pref	Specifies the preference value associated with the route.

Filtering route information

Filter the routes displayed in the Routes tab to display only the desired switch routes.

Procedure steps

Step	Action
1	With the **Routes** tab open, click **Filter**. The Filter dialog box appears.
2	Using the fields provided, set the filter for the tab.
3	Click **Filter**.

—End—

Variable definitions

The following table describes the Filter tab fields.

Field	Description
Condition	When using multiple filter expressions on the tab, this is the condition that is used to join them together.
Ignore Case	Indicates whether filters are case sensitive or insensitive.
Column	Indicates the type of criteria to apply to values used for filtering.
All Records	Select this check box to clear any filters and display all rows.
Dest	Select this check box and enter a value to filter on the route destination value.
Mask	Select this check box and enter a value to filter on the route destination subnet mask value.
NextHop	Select this check box and enter a value to filter on the route next hop value.
HopOrMetric	Select this check box and enter a value to filter on the hop count or metric of the route.
Interface	Select this check box and enter a value to filter on the interface associated with the route.
Proto	Select this check box and enter a value to filter on the route protocol.
PathType	Select this check box and enter a value to filter on the route path type.
Pref	Select this check box and enter a value to filter on the route preference value.

Displaying TCP information for the switch

Use this procedure to display Transmission Control Protocol (TCP) information for the switch.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > TCP/UDP**. The Ipv4TcpUdp dialog box appears with the TCP Globals tab displayed.

—End—

Variable definitions

The following table describes the TCP Globals tab fields.

Field	Description
RtoAlgorithm	Specifies the algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
RtoMin	Specifies the minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
RtoMax	Specifies the maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
MaxConn	Specifies the limit on the total number of TCP connections that the entity can support. In entities where the maximum number of connections is dynamic, this object contains the value -1.

Displaying TCP Connections

Use this procedure to display information on the current TCP connections that the switch maintains.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > TCP/UDP**.
2	Select the **TCP Connections** tab.

—End—

Variable definitions

The following table describes the TCP Connections tab fields.

Field	Description
LocalAddressType	Specifies the local IP address type for this TCP connection.
LocalAddress	Specifies the local IP address for this TCP connection. In the case of a connection in the listen state, which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.
LocalPort	Specifies the local port number for this TCP connection.
RemAddressType	Specifies the remote IP address type for this TCP connection.
RemAddress	Specifies the remote IP address for this TCP connection.

Field	Description
RemPort	Specifies the remote port number for this TCP connection.
State	Specifies the state of this TCP connection.

Displaying TCP Listeners

Use this procedure to display information on the current TCP listeners on the switch.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > TCP/UDP**.
2	Select the **TCP Listeners** tab.
	—End—

Variable definitions

The following table describes the TCP Listeners tab fields.

Field	Description
LocalAddressType	Specifies the IP address type of the local TCP listener.
LocalAddress	Specifies the local IP address of the TCP listener. The value of this field can be represented in three possible ways, depending on the characteristics of the listening application: 1. For an application willing to accept both IPv4 and IPv6 datagrams, the value of this object is a zero-length octet string, and the value of the corresponding LocalAddressType field is unknown. 2. For an application willing to accept either IPv4 or IPv6 datagrams, the value of this object must be 0.0.0.0 or ::, with the LocalAddressType identifying the supported address type. 3. For an application that is listening for data destined only to a specific IP address, the value of this object is the specific local address, with LocalAddressType identifying the supported address type.
LocalPort	Specifies the local port number for this TCP connection

Displaying UDP endpoints

Use this procedure to display information on the UDP endpoints currently maintained by the switch.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > TCP/UDP**.
2	Select the **UDP Endpoints** tab.
3	Click **Refresh** to immediately refresh the information displayed.

—End—

Variable definitions

The following table describes the UDP Endpoints tab fields.

Field	Description
LocalAddressType	Specifies the local address type (IPv6 or IPv4).
LocalAddress	Specifies the local IP address for this UDP listener. In the case of a UDP listener that accepts datagrams for any IP interface associated with the node, the value 0.0.0.0 is used. The value of this field can be represented in three possible ways: 1. For an application willing to accept both IPv4 and IPv6 datagrams, the value of this object is a zero-length octet string, and the value of the corresponding LocalAddressType field is unknown. 2. For an application willing to accept either IPv4 or IPv6 datagrams, the value of this object must be 0.0.0.0 or ::, with the LocalAddressType identifying the supported address type. 3. For an application that is listening for data destined only to a specific IP address, the value of this object is the address for which this node is receiving packets, with LocalAddressType identifying the supported address type.
LocalPort	Specifies the local port number for this UDP listener.
RemoteAddressType	Displays the remote address type (IPv6 or IPv4).

Field	Description
RemoteAddress	Displays the remote IP address for this UDP endpoint. If datagrams from all remote systems are to be accepted, this value is a zero-length octet string. Otherwise, the address of the remote system from which datagrams are to be accepted (or to which all datagrams are to be sent) is displayed with the RemoteAddressType identifying the supported address type.
RemotePort	Displays the remote port number. If datagrams from all remote systems are to be accepted, this value is zero.
Instance	Distinguishes between multiple processes connected to the same UDP endpoint.
Process	Displays the ID for the UDP process.

DHCP relay configuration using Device Manager

This chapter describes the procedures you can use to configure DHCP relay using Device Manager.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be set as the DHCP relay agent.
- Ensure that a route (local or static) to the destination DHCP server is available on the switch.

DHCP relay configuration procedures

To configure DHCP relay using Device Manager, perform the following steps:

Step	Action
1	Configure the DHCP relay forwarding path by specifying the VLAN IP as the DHCP relay agent and the remote DHCP server as the destination, and enable DHCP relay on the VLAN.

—End—

Navigation

- "Configuring DHCP Relay " (page 107)
- "Configuring DHCP parameters on a VLAN" (page 108)
- "Displaying and graphing DHCP counters on a VLAN" (page 109)

Configuring DHCP Relay

Use this procedure to configure DHCP Relay.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > DHCP**. The DHCP Relay tab appears.
2	Click **Insert**. The Insert DHCP Relay dialog box appears.
3	In the **AgentAddr** field, enter the IP address of the local VLAN to serve as the DHCP relay agent.
4	In the **ServerAddr** field, enter the remote DHCP Server IP address.
5	Ensure the **Enable** check box is selected.
6	In the **Mode** box, select the desired DHCP relay mode.
7	Click **Insert**. The new DHCP entry appears in the DHCP Relay tab.

—End—

Variable definitions

The following table describes the DHCP Relay tab fields.

Field	Description
AgentAddr	The IP address of the local VLAN serving as the DHCP relay agent.
ServerAddr	The IP address of the remote DHCP server.
Enable	Enables (selected) or disables (cleared) DHCP relay.
Mode	Indicates whether the relay instance applies for BOOTP packets, DHCP packets, or both.

Configuring DHCP parameters on a VLAN

Use this procedure to configure the DHCP relay parameters on a VLAN.

Procedure steps

Step	Action
1	From the Device Manager menu, select **VLAN > VLANs**.

2 Select the VLAN for which DHCP relay is to be configured.

3 Click **IP**.

The IP, VLAN dialog box appears.

4 Select the **DHCP** tab.

5 To configure the DHCP relay parameters, modify the values in the fields provided, as required.

6 Click **Apply**.

—End—

Variable definitions

The following table describes the DHCP tab fields.

Field	Description
Enable	Specifies whether DHCP relay is enabled or disabled.
MinSec	Indicates the min-sec value. The switch immediately forwards a BootP/DHCP packet if the secs field in the BootP/DHCP packet header is greater than the configured min-sec value; otherwise, the packet is dropped.
Mode	Specifies the type of packets this VLAN interface forwards: BootP, DHCP, or both.
AlwaysBroadcast	Specifies whether DHCP Reply packets are broadcast to the DHCP clients on this VLAN interface.
ClearCounters	Specifies to clear the DHCP relay counters for the VLAN.
CounterClearTime	Specifies the last time the counter values in this entry were reset to 0.

Displaying and graphing DHCP counters on a VLAN

Use this procedure to display and graph the current DHCP counters on a VLAN.

Procedure steps

Step	Action
1	From the Device Manager menu, select **VLAN > VLANs**.
2	Select the VLAN for which DHCP is configured.
3	Click **IP**.

The IP, VLAN dialog box appears.

4 Select the **DHCP** tab.

5 Click **Graph**.

The DHCP Stats dialog box appears.

6 Use the buttons provided to graph selected DHCP counter information.

—End—

Variable definitions

The following table describes the DHCP Stats dialog box fields.

Field	Description
NumRequests	Indicates the number of DHCP requests.
NumReplies	Indicates the number of DHCP replies.

UDP broadcast forwarding configuration using Device Manager

This chapter describes the procedures you can use to configure and manage UDP broadcast forwarding using Device Manager. UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address.

Prerequisites to UDP broadcast forwarding configuration using Device Manager

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a UDP forwarding interface.
- Ensure that a route (local or static) to the destination address is available on the switch.

UDP broadcast forwarding configuration procedures

To configure UDP broadcast forwarding using Device Manager, perform the following steps:

Step	Action
1	Create UDP protocol entries that specify each UDP port and associated protocol that you want to forward.
2	Create UDP forwarding entries that specify the destination address for each UDP port that you want to forward.
3	Add UDP forwarding entries to a UDP forwarding list (you can create up to 128 UDP forwarding lists.)
4	Apply UDP forwarding lists to local VLAN interfaces.

—End—

Navigation

Configuring UDP protocol table entries

Use this procedure to create UDP table entries that identify the protocols associated with specific UDP ports that you want to forward.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > UDP Forwarding**. The UDP_Forward dialog box appears with the Protocols tab selected.
2	Click **Insert**. The Insert Protocols dialog box appears.
3	In the **PortNumber** box, enter the UDP port number that you want to forward.
4	In the **Name** box, enter the protocol name associated with the UDP port number.
5	Click **Insert**.

—End—

Variable definitions

The following table describes the Protocols tab fields.

Field	Description
PortNumber	Specifies the UDP port number.
Name	Specifies the protocol name associated with the UDP port.

Configuring UDP forwarding entries

Use this procedure to configure individual UDP forwarding entries, which associate UDP forwarding ports with destination IP addresses.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > UDP Forwarding**. The UDP_Forward dialog box appears.
2	Select the **Forwardings** tab.
3	Click **Insert**. The Insert Forwardings dialog box appears.
4	Use the provided fields to specify a destination address for a selected port.
5	Click **Insert**.

—End—

Variable definitions

The following table describes the Forwardings tab fields.

Field	Description
DestPort	Specifies the port on which the UDP forwarding originates (configured using the Protocols tab).
DestAddr	Specifies the destination IP address.
Id	Specifies an ID for the entry.
FwdListIdList	Indicates the UDP forward list with which this entry is associated (using the Forwarding Lists tab).

Configuring a UDP forwarding list

Use this procedure to add the UDP port/destination forwarding entries (configured in the Forwardings tab) to UDP forwarding lists. Each UDP forwarding list can contain multiple port/destination entries.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > UDP Forwarding**.
2	Select the **Forwarding Lists** tab.

3 Click **Insert**.

The Insert Forwarding Lists dialog box appears.

4 In the **Id** field, assign a unique ID to the UDP forwarding list.

5 In the **Name** field, enter a unique name for the UDP forwarding list.

6 In the **FwdIdList** field, click the ellipsis (**...**), select the desired port/destination pairs from the list, and click **OK**.

7 Click **Insert**.

—End—

Variable definitions

The following table describes the Forwarding Lists tab fields.

Field	Description
Id	The unique identifier assigned to the forwarding list.
Name	The name assigned to the forwarding list.
FwdIdList	The forwarding entry IDs associated with the port/server IP pairs created using the Forwardings tab.

Applying a UDP forwarding list to a VLAN

Use this procedure to assign a UDP forwarding list to a VLAN and to configure the related UDP forwarding parameters for the VLAN.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > UDP Forwarding**.
2	Select the **Broadcast Interfaces** tab.
3	Click **Insert**. The Insert Broadcast Interface dialog box appears.
4	In the **LocalIfAddr** field, click the **Addr** button and select a VLAN IP address from the list.
5	In the **UdpPortFwdListId** field, click the **IdList** button and select the desired UDP forwarding list to apply to the VLAN.

6 To modify the maximum TTL, modify the value in the **MaxTtl** field.

7 To specify a broadcast mask, enter a mask in the **BroadCastMask** field.

8 Click **Insert**.

—End—

Variable definitions

The following table describes the Broadcast Interface tab fields.

Field	Description
LocalIfAddr	Specifies the IP address of the local VLAN interface.
UdpPortFwdListId	Specifies the port forwarding lists associated with the interface. This ID is defined in the Forwarding Lists tab.
MaxTtl	Indicates the maximum number of hops an IP broadcast packet can take from the source device to the destination device. This is an integer value between 1 and 16.
NumRxPkts	Specifies the total number of UDP broadcast packets received by this local interface.
NumFwdPkts	Specifies the total number of UDP broadcast packets forwarded.
NumDropPkts DestUnreach	Specifies the total number of UDP broadcast packets dropped because the destination is unreachable.
NumDropPkts UnknownPort	Specifies the total number of UDP broadcast packets dropped because the destination port or protocol specified has no matching forwarding policy.
BroadCastMask	Specifies the 32-bit mask used by the selected VLAN interface to take forwarding decisions based on the destination IP address of the incoming UDP broadcast traffic. If you do not specify a broadcast mask value, the switch uses the mask of the interface to which the forwarding list is attached.

Static ARP and Proxy ARP configuration using Device Manager

This chapter describes the procedures you can use to configure Static ARP, display ARP entries, and configure Proxy ARP using Device Manager.

Navigation

Configuring static ARP entries

Use this procedure to configure static ARP entries for the switch.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the target VLAN interface.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > IP**.
2	Select the **ARP** tab.
3	Click **Insert**. The Insert ARP dialog box appears.
4	From the **Port in VLAN** list, select the VLAN to which you want to add the static ARP entry. A VLAN dialog box appears listing all member ports.
5	In the **VLAN** dialog box, select the port for this ARP entry.

The Interface(vlanId:Port) field updates with the appropriate VLAN and port information

6 In the **IPAddress** field, specify the IP address for the ARP entry.

7 In the **MacAddress** field, specify the MAC address for the ARP entry.

8 Click **Insert**.

—End—

Variable definitions

The following table describes the Insert ARP tab fields.

Field	Description
Interface	Specifies the VLAN and port to which the static ARP entry is being added.
MacAddress	Specifies the MAC address of the device being set as a static ARP entry.
IpAddress	Specifies the IP address of the device being set as a static ARP entry.
Type	Specifies the type of ARP entry: static, dynamic, or local.

Configuring Proxy ARP

Use this procedure to configure proxy ARP on the switch. Proxy ARP allows the switch to respond to an ARP request from a locally attached host (or end station) for a remote destination.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a Proxy ARP interface.

Procedure steps

Step	Action
1	From the Device Manager menu, select **IP Routing > IP**.
2	Select the **ARP Interfaces** tab.

ATTENTION
Device Manager does not display the ARP Interfaces tab if you have not enabled routing on the switch.

3 To enable proxy ARP, in the **DoProxy** field, select **enable**.

4 Click **Apply**.

—End—

Variable definitions

The following table describes the ARP Interfaces tab fields.

Field	Description
IfIndex	Specifies a configured switch interface.
DoProxy	Enables or disables proxy ARP on the interface.
DoResp	Specifies whether the sending of ARP responses on the specified interface is enabled or disabled.

IGMP snooping configuration using Device Manager

This chapter describe the procedures you can use to configure IGMP snooping using Device Manager.

Navigation

Configuring IGMP snooping

Use the following procedure to configure IGMP snooping on a switch.

Procedure steps

Step	Action
1	From the Device Manager menu bar, select **VLAN > VLANs**. The VLAN dialog box appears with the Basic tab displayed.
2	Select the **Snoop** tab.
3	To enable IGMP snoop, select **true** from the **Enable** field.
4	To enable IGMP proxy, select **true** from the **ReportProxyEnable** field.
5	To add static mrouter ports, specify the desired ports in the **Ver1MRouterPorts** field (for IGMP version 1), **Ver2MRouterPorts** field (for IGMP version 2) or **MRouterPorts** field (for both IGMP versions).
6	To configure the robustness or query interval, modify the fields provided.
7	Click **Apply**.

—End—

Variable definitions

The following table describes the Snoop tab fields.

Field	Description
VLAN ID	Specifies the VLAN ID.
Name	Specifies the VLAN name.
Enable	Specifies whether IGMP snooping is enabled or disabled.
ReportProxyEnable	Specifies whether IGMP proxy is enabled or disabled.
Robustness	Specifies tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1. If you expect a network to lose query packets, you must increase the robustness value. Ensure that the robustness value is the same as the configured value on the multicast router (IGMP querier). The range is from 0 –255, and the default is 2. The default value of 2 means that one query for each query interval can be dropped without the querier aging out.
QueryInterval	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN.
MRouterPorts	Specifies ports in the VLAN that provide connectivity to an IP Multicast router.
Ver1MRouterPorts	Specifies ports in this VLAN that provide connectivity to an IP Multicast router using IGMP version 1.
Ver2MRouterPorts	Specifies ports in this VLAN that provide connectivity to an IP Multicast router using IGMP version 2.
ActiveMRouterPorts	Specifies the active mrouter ports (dynamic and static) in this VLAN that provide connectivity to an IP Multicast router.
ActiveQuerier	Specifies the IP address of the multicast querier router.
QuerierPort	Specifies the port on which the multicast querier router is heard.
MRouterExpiration	Specifies the multicast querier router aging timeout.

IP routing configuration using Web-based management

This chapter describes the procedures you can use to configure routable VLANs using Web-based management.

The Nortel Ethernet Routing Switch 2500 Series are Layer 3 switches. This means that a regular Layer 2 VLAN becomes a routable Layer 3 VLAN if an IP address is attached to the VLAN. When routing is enabled in Layer 3 mode, every Layer 3 VLAN is capable of routing as well as carrying the management traffic. You can use any Layer 3 VLAN instead of the Management VLAN to manage the switch.

IP routing configuration procedures

To configure IP routing on VLANs, perform the following steps:

Step	Action
1	Enable IP routing globally.
2	Assign an IP address to a specific VLAN.

—End—

In the above procedure, you are not required to enable IP routing as the first step. You can configure all IP routing parameters on the Nortel Ethernet Routing Switch 2500 Series before you enable routing on the switch.

Navigation

- "Configuring an IP address and enabling routing for a VLAN" (page 124)
- "Displaying IP routes" (page 124)

Configuring an IP address and enabling routing for a VLAN

Use this procedure to enable routing globally and configure an IP address and enable routing for a VLAN.

Procedure steps

Step	Action
1	From the main menu, select **Applications > IP Routing > IPv4 Configuration**.
2	To enable IP routing globally, set the status in the **IP Routing** window to **Enable**.
3	To configure an IP address for a VLAN, in the **Create IP Interface** window, specify the IP address, subnet mask, and offset values, and ensure that the **Routing** field is set to **enable**.
4	Click **Submit**. The VLAN configuration appears in the VLAN IP Interfaces window.

—End—

Variable definitions

The following table describes the VLAN IP Interfaces window fields.

Field	Description
VID	Specifies the VLAN ID.
Action	The delete icon (X) deletes the configured IP address.
If Index	Specifies an index value for the VLAN interface.
Address	Specifies the IP address to associate with the selected VLAN.
Mask	Specifies the subnet mask.
Offset	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address. The valid range is 1-256. Specify the value 1 for the Management VLAN only. If no MAC offset is specified, the switch applies one automatically.
Routing	Specifies whether routing is enabled on the VLAN.

Displaying IP routes

Use this procedure to display the different routes known to the switch.

Procedure steps

Step	Action
1	From the main menu, select **Applications > IP Routing > IPv4 Routing Table**.

—End—

Variable definitions

The following table describes the IPv4 Routing Table fields.

Field	Description
Destination	The destination address of the route.
Mask	The subnet mask used by the route destination.
Next Hop	The next hop in the listed route.
Cost	The metric associated with the route.
Vlan - Port	The VLAN or VLAN port associated with the route.
Protocol	The protocol associated with the route (static or local).
Type	The route path type: • indirect • direct • best • unresolved
Preference	The preference value associated with the route.

Static route configuration using Web-based management

This chapter describes the procedures you can use to configure static routes using Web-based management.

Configuring static routes

Use this procedure to configure a static route.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLANs to be routed.

Procedure steps

Step	Action
1	From the main menu, select **Applications > IP Routing > IPv4 Static Routes**.
2	To add a static route, in the **Create Static Route** window, specify the destination address, subnet mask, next hop, and cost-related fields for the VLAN.
3	Click **Submit**. The static route configuration appears in the Static Routes window.

—End—

Variable definitions

The following table describes the Static Routes window fields.

Field	Description
Index	Specifies the interface on which the static route is configured.
Action	The delete icon (X) deletes the configured static route.
Destination	Specifies the destination IP address of the route. 0.0.0.0 is considered the default route.
Mask	Specifies the destination mask of the route.
Next	Specifies the IP address of the next hop of this route.
Cost	Represents the cost of the static route. It is used to choose the best route (the one with the smallest cost) to a certain destination. The range is 1-65535.
Preference	Specifies the preference value associated with the route.
Local Next Hop	True indicates that the static route becomes active only if the switch has a local route to the network. False indicates that the static route can become active if the switch has a local route or a dynamic route.
Status	Specifies the operational status of the route.
Enable	Specifies whether the route is administratively enabled (TRUE) or disabled (FALSE).

DHCP relay configuration using Web-based management

This chapter describes the procedures you can use to configure DHCP relay using Web-based management.

Prerequisites to DHCP relay configuration using Web-based management

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be set as the DHCP relay agent.
- Ensure that a route (local or static) to the destination DHCP server is available on the switch.

DHCP relay configuration procedures

To configure DHCP relay using Web-based management, perform the following steps:

Step	Action
1	Configure the DHCP relay forwarding path by specifying the VLAN IP as the DHCP relay agent and the remote DHCP server as the destination.
2	Enable DHCP relay for the specific VLAN.

—End—

Navigation

- "Configuring DHCP Relay " (page 130)
- "Configuring DHCP relay status and parameters on a VLAN" (page 130)

Configuring DHCP Relay

Use this procedure to configure DHCP Relay.

Procedure steps

Step	Action
1	From the main menu, select **Applications > DHCP Relay > DHCP Relay Configuration**.
2	In the **DHCP Relay Setting** window, ensure that the DHCP relay global status is set to **enabled**.
3	To add a DHCP relay entry, in the **Create DHCP Forwarding Path** window, specify the IP address of the local VLAN that serves as the DHCP relay agent, the remote DHCP server address, and the mode.
4	Click **Submit**. The new static DHCP relay entry appears in the DHCP Forwarding Path window.

—End—

Variable definitions

The following table describes the DHCP Relay Configuration page fields.

Field	Description
Interface	The IP address of the local VLAN serving as the DHCP relay agent.
Server	The IP address of the remote DHCP server.
Enabled	Enables (selected) or disables (cleared) DHCP relay.
Mode	Indicates whether the relay instance applies for BOOTP packets, DHCP packets, or both.
Delete DHCP Forwarding Path	When set to Yes, deletes the specified DHCP relay entry.

Configuring DHCP relay status and parameters on a VLAN

Use this procedure to configure the DHCP relay status and parameters on a VLAN.

Procedure steps

Step	Action
1	From the main menu, select **Applications > DHCP Relay > DHCP Relay VLAN**.
2	To enable DHCP relay on a VLAN, under the **Enabled** field, select **Enabled**.
3	To configure the DHCP relay parameters on a VLAN, modify the values in the fields provided.
4	Click **Submit**.

—End—

Variable definitions

The following table describes the DHCP Relay VLAN page fields.

Field	Description
IfIndex	Specifies an index value for the interface.
Interface Address	Specifies the IP address of the VLAN serving as a DHCP relay agent.
Min Sec	Indicates the min-sec value. The switch immediately forwards a BootP/DHCP packet if the secs field in the BootP/DHCP packet header is greater than the configured min-sec value; otherwise, the packet is dropped.
Enabled	Specifies whether DHCP relay is enabled or disabled.
Mode	Specifies the type of packets this VLAN interface forwards: BootP, DHCP, or both.
Always Broadcast	Specifies whether DHCP Reply packets are broadcast to the DHCP clients on this VLAN interface.
Requests Counter	Specifies the number of requests.
Replies Counter	Specifies the number of replies.
Clear Counters	Specifies to clear the DHCP relay counters for the VLAN.

Static ARP configuration using Web-based management

This chapter describes the procedure you can use to configure static ARP using Web-based management.

Configuring static ARP entries

Use this procedure to configure static ARP entries for the switch.

Prerequisites

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the target VLAN interface.

Procedure steps

Step	Action
1	From the main menu, select **Applications > IP Routing > IPv4 ARP**.
2	To add a static ARP entry, in the **Create Static ARP** window, specify the IP address, unit, port, VLAN ID, and MAC address.
3	Click **Submit**. The new static ARP entry appears in the ARP Entries window.
4	To configure the ARP lifetime for the switch, modify the value in the **ARP Life Time** field.
5	To clear the ARP cache for the switch, click the delete icon (X) in the **Delete All ARPs** window.

—End—

Variable definitions

The following table describes the ARP Entries window fields.

Field	Description
Action	The delete icon (X) deletes the specified static ARP entry.
IP Address	Specifies the IP address of the device being set as a static ARP entry.
MAC Address	Specifies the MAC address of the device being set as a static ARP entry.
VLAN-Unit/Port/Trunk	Specifies the VLAN and port to which the static ARP entry is being added.
Type	Specifies the type of ARP entry: static, dynamic, or local.

IGMP snooping configuration using Web-based management

This chapter describes the procedures you can use to configure IGMP snooping using Web-based management.

Navigation

Configuring IGMP snooping

Use this procedure to configure IGMP using Web-based management.

Procedure steps

Step	Action
1	From the main menu, select **Applications > IGMP > IGMP Configuration**.
2	In the **Action** column, click the icon for the VLAN you want to configure. The IGMP: VLAN Configuration window appears. The configurations you make in this page affect only the VLAN specified in the VLAN field.
3	To enable IGMP snooping, select **Enabled** from the **Snooping** field.
4	To enable IGMP proxy, select **Enabled** from the **Proxy** field.
5	To configure static mrouter ports, select the ports from the appropriate **Static Router Ports** box (**Version 1** for IGMPv1 or **Version 2** for IGMPv2).
6	To configure the robustness value and query interval, modify the values in the fields provided.

7 Click **Submit**.

The VLAN Configuration page refreshes, and the settings are saved.

—End—

Variable definitions

The following table describes the fields in the IGMP VLAN Setting window.

Fields	Description
VLAN	Specifies the VLAN ID.
Snooping	Enables or disables the IGMP snooping feature. The default setting is Disabled.
Proxy	Enables or disables the IGMP proxy feature. With this feature enabled, the switch consolidates IGMP Host Membership Reports received on its downstream ports and generates a consolidated proxy report for forwarding to its upstream neighbor. The default setting is Disabled.
Robust Value	Specifies the robustness value. You can use this parameter to set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, increase the Robust Value field to a higher value. The default setting is 2.
Query Time	Specifies the query time (in seconds). You can use this parameter to control the number of IGMP messages allowed on the subnet by varying the query interval (the interval between general queries sent by the multicast router). The default setting is 125 seconds.
Static Router Ports (Version 1 and Version 2)	Specifies static mrouter ports associated with the VLAN.

Displaying multicast membership

Use the following procedure to display Multicast membership using Web-based management.

Procedure steps

Step	Action
1	From the main menu, select **Applications > IGMP > Multicast Group**.

2 In the **Multicast Group Membership Selection (View By)** window, from the **VLAN** list, select the VLAN for which to display group membership.

3 Click **Submit**.

The membership information appears in the Multicast Group Membership Table.

—End—

Variable definitions

The following table describes the Multicast Group Membership Table fields.

Field	Description
Multicast Group Address	Specifies the IP Multicast group addresses that are currently active on the associated port.
Port	Specifies the port numbers associated with the IP Multicast group addresses displayed in the IP Multicast Group Address field.

Nortel Ethernet Routing Switch 2500 Series

Configuration — IP Routing and Multicast

Publication: NN47215-503
Document status: Standard
Document version: 03.01
Document date: 27 October 2008

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

Sourced in Canada and the United States of America