Nortel Ethernet Routing Switch 8600

Configuration — IPv6 Routing

Release: 7.0
Document Revision: 03.02

www.nortel.com

NN46205-504

Nortel Ethernet Routing Switch 8600
Release: 7.0
Publication: NN46205-504
Document release date: 12 April 2010

Contents

Software license

This section contains the Nortel Networks software license.

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 forgoing 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.

New in this release

The following sections detail what's new in *Nortel Ethernet Routing Switch 8600 Configuration — IPv6 Routing* (NN46205-504) for Release 7.0.

- "Features" (page 19)
- "Changes in revision 03.02" (page 21)

Features

For information about changes that are feature-related, see the following sections.

IPv6 DHCP Relay

IPv6 DHCP clients use link-local addresses to send and receive DHCP messages. To allow a DHCP client to send a message to a DHCP server that is not attached to the same link, you must configure a DHCP relay agent on the client's link to relay messages between the client and server. The operation of the relay agent is transparent to the client.

A relay agent relays messages from clients and messages from other relay agents.

For more information, see

- "IPv6 DHCP Relay" (page 68)
- "IPv6 DHCP Relay configuration using the CLI" (page 215)
- "IPv6 DHCP Relay configuration using the NNCLI" (page 223)
- "IPv6 DHCP Relay configuration using Enterprise Device Manager" (page 211)

IPv6 VRRP

To provide fast failover of a default router for IPv6 LAN hosts, the Ethernet Routing Switch 8600 supports the Virtual Router Redundancy Protocol (VRRP v3) for IPv6 (defined in draft-ietf-vrrp-ipv6-spec-08.txt).

VRRPv3 for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol. With VRRPv3, a backup router can take over for a failed default router in approximately three seconds (using VRRPv3 default parameters). This is accomplished without any interaction with the hosts and with a minimum amount of VRRPv3 traffic.

The operation of Nortel's IPv6 VRRP implementation is similar to the existing IPv4 VRRP operation, including support for hold-down timer, critical IP, fast advertisements, and backup master. With backup master enabled, the backup switch routes all traffic according to its routing table. It does not Layer 2-switch the traffic to the VRRP master.

For more information, see:

- "IPv6 VRRP" (page 69)
- "IPv6 VRRP configuration using the CLI" (page 241)
- "IPv6 VRRP configuration using the NNCLI" (page 257)
- "IPv6 VRRP configuration using Enterprise Device Manager" (page 227)

IPv6 RSMLT

Nortel Routed Split MultiLink Trunking (RSMLT) permits rapid failover for core topologies by providing an active-active router concept to core Split MultiLink Trunking (SMLT) networks. In the event of core router failures, RSMLT manages packet forwarding, thus minimizing dropped packets during the routing protocol convergence.

While Nortel's Routed Split Multilink Trunk (RSMLT) functionality originally provided sub-second failover for IPv4 forwarding only, Release 7.0 extends RSMLT functionality to IPv6. The overall model for IPv6 RSMLT is essentially identical to that of IPv4 RSMLT. In short, RSMLT peers exchange their IPv6 configuration and track each other's state by means of IST messages. An RSMLT node always performs IPv6 forwarding on the IPv6 packets destined to the peer's MAC. When an RSMLT node detects that its RSMLT peer is down the node also terminates IPv6 traffic destined to the peer's IPv6 addresses.

For more information, see

- "IPv6 RSMLT" (page 77)
- "IPv6 RSMLT configuration using the CLI" (page 275)
- "IPv6 RSMLT configuration using the NNCLI" (page 281)
- "IPv6 RSMLT configuration using Enterprise Device Manager" (page 269)

Other changes

For information about changes that are not feature-related, see the following sections.

OSPFv3 clarification

A clarification of a difference in OSPF implementation of between IPv4 and IPv6, related to the OSPFv3 R-bit, is now added. See "R-bit" (page 57).

Enterprise Device Manager

Replaced the Device Manager configuration information with the Enterprise Device Manager (EDM). Starting with this release, EDM is replacing Device Manager as the graphical user interface.

References to classic modules removed

All references to classsic modules are removed from this document.

Changes in revision 03.02

See the following section for information about changes that have been made in revision 03.02 of this document.

8695 SF/CPU renamed to 8895 SF/CPU

The 8695 SF/CPU is renamed to the 8895 SF/CPU. All instances of 8695 SF/CPU in this document are updated to 8895 SF/CPU.

Introduction

This guide provides instructions for using the command line interface (CLI), the Nortel Command Line Interface (NNCLI) and the Enterprise Device Manager graphical user interface (GUI) to perform general network management operations on the Nortel Ethernet Routing Switch 8600. For more information about using the interfaces, see *Nortel Ethernet Routing Switch 8600 User Interface Fundamentals* (NN46205-308).

Navigation

IPv6 routing fundamentals

The router management features apply regardless of which routing protocols you use and include router Internet Protocol version 6 (IPv6) configuration and IPv6 route table management.

ATTENTION
IPv6 routing is not supported with Virtual Routing and Forwarding (VRF).

Navigation

- “IPv6 VRRP” (page 69)
- “IPv6 RSMLT” (page 77)

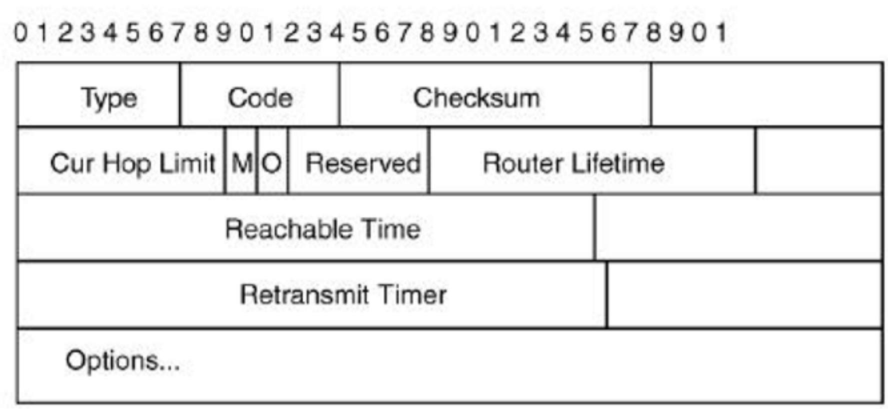
The IPv6 header

The IPv6 header contains the following fields:

- a 4-bit Internet Protocol version number, with a value of 6
- an 8-bit traffic class field, similar to Type of Service in IPv4
- a 20-bit flow label that identifies traffic flow for additional Quality of Service (QoS)
- a 16-bit unsigned integer, the length of the IPv6 payload
- an 8-bit next header selector that identifies the next header
- an 8-bit hop limit unsigned integer that decrements by 1 each time a node forwards the packet (nodes discard packets with hop limit values of 0)
- a 128-bit source address
- a 128-bit destination address

Figure 1 "IPv6 header" (page 26) illustrates the IPv6 header.

Figure 1
IPv6 header

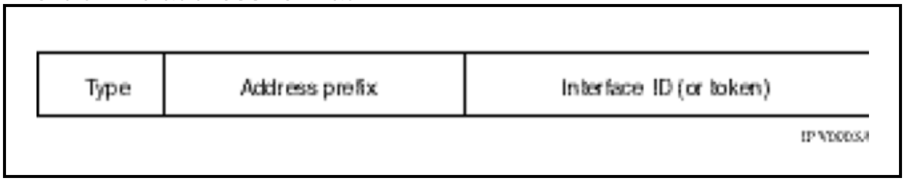


IPv6 addresses

IPv6 addresses are 128 bits in length. The address identifies a single interface or multiple interfaces. IPv4 addresses, in comparison, are 32 bits in length. The increased number of possible addresses in IPv6 solves the inevitable IP address exhaustion inherent to IPv4.

The IPv6 address contains two parts: an address prefix and an IPv6 interface ID. The first 3 bits indicate the type of address that follows. Figure 2 "128-bit IPv6 address format" (page 27) shows the IPv6 address format.

Figure 2
128-bit IPv6 address format



An example of a unicast IPv6 address is
1080:0:0:0:8:8000:200C:417A

Interface ID

The interface ID is a unique number that identifies an IPv6 node (a host or a router). For stateless autoconfiguration, the ID is 64 bits in length. See "Host autoconfiguration" (page 35). The interface ID is derived by a formula that uses the link layer 48-bit MAC address. (In most cases, the interface ID is a 64-bit interface ID that contains the 48-bit MAC address.) The IPv6 interface ID is as unique as the MAC address.

If you manually configure interface IDs or MAC addresses (or both), no relationship between the MAC address and the interface ID is necessary. A manually configured interface ID can be longer or shorter than 64 bits.

Address formats

The format for representing an IPv6 address is

n:n:n:n:n:n:n:n

n is the hexadecimal representation of 16 bits in the address; for example,

FF01:0:0:0:0:0:0:43

Each nonzero field must contain at least one numeral. Within a hexadecimal field; however, leading zeros are not required.

Certain classes of IPv6 addresses commonly include multiple contiguous fields containing hexadecimal 0. The following sample address includes five contiguous fields containing zeroes with a double colon (::):

FF01::43

You can use a double colon to compress the leading zero fields in a hexadecimal address. A double colon can appear once in an address.

An IPv4-compatible address combines hexadecimal and decimal values as follows:

x:x:x:x:x:x:d.d.d.d

x:x:x:x:x:x is a hexadecimal representation of the 6 high-order 16-bit pieces of the address, and *d.d.d.d* is a decimal representation of the four 8-bit pieces of the address; for example,

0:0:0:0:0:0:13.1.68.3

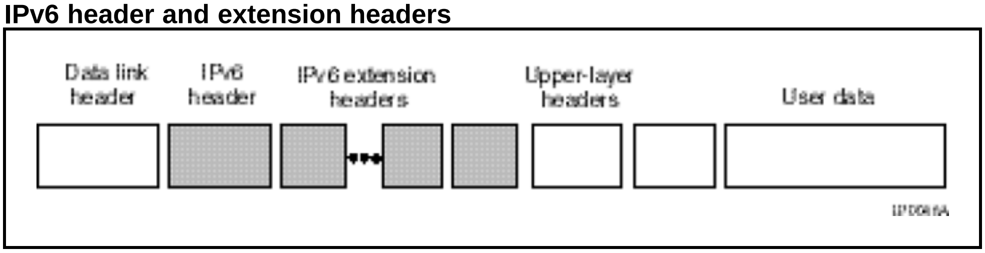
or

::13.1.68.3

IPv6 extension headers

IPv6 extension headers describe processing options. Each extension header contains a separate category of options. A packet can include zero or more extension headers; see Figure 3 "IPv6 header and extension headers" (page 28).

Figure 3
IPv6 header and extension headers



IPv6 examines the destination address in the main header of each packet it receives. This examination determines whether the router is the packet destination or an intermediate node in the packet data path. If the router is the packet destination, IPv6 examines the header extensions that contain options for destination processing. If the router is an intermediate node, IPv6 examines the header extensions that contain forwarding options.

By examining only the extension headers that apply to the operations it performs, IPv6 reduces the amount of time and processing resources required to process a packet.

IPv6 defines the following extension headers:

- The hop-by-hop extension header contains optional information that all intermediate IPv6 routers examine between the source and the destination.
- The end-to-end extension header contains optional information for the destination node.

- The source routing extension header contains a list of one or more intermediate nodes that define a path for the packet to follow through the network, to the destination. The packet source creates this list. This function is similar to the IPv4 source routing options.
- The fragmentation extension header uses an IPv6 source to send packets larger than the size specified for the path maximum transmission unit (MTU).
- The authentication extension header and the security encapsulation extension header, used singly or jointly, provide security services for IPv6 datagrams.

Comparison of IPv4 and IPv6

Table 1 "IPv4 and IPv6 differences" (page 29) compares key differences between IPv4 and IPv6.

Table 1
IPv4 and IPv6 differences

Feature	IPv4	IPv6
Address length	32 bits	128 bits
IPsec support	Optional	Required
QoS support	Limited	Improved
Fragmentation	Hosts and routers	Hosts only
MTU packet size	576 bytes	1280 bytes
Checksum in header	Yes	No
Options in header	Yes	No
Link-layer address resolution	ARP (broadcast)	Multicast Neighbor Discovery Messages
Multicast membership	IGMP	Multicast Listener Discovery (MLD)
Router discovery	Optional	Required
Uses broadcasts	Yes	No
Configuration	Manual, DHCP	Automatic, DHCP

ICMPv6

Internet Control Message Protocol version 6 (ICMPv6) maintains and improves upon features from ICMP for IPv4. ICMPv6 reports the delivery of forwarding errors, such as destination unreachable, packet too big, time exceeded, and parameter problem. ICMPv6 also delivers information messages such as echo request and echo reply.

> **ATTENTION**
> ICMPv6 plays an important role in IPv6 features such as neighbor discovery, Multicast Listener Discovery, and path MTU discovery.

Neighbor discovery

IPv6 nodes (routers and hosts) on the same link use neighbor discovery (ND) to discover link layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services for IPv4 with the Address Resolution Protocol (ARP) and router discovery. ND replaces ARP in IPv6.

Hosts use ND to discover the routers in the network that you can use as the default routers, and to determine the link layer address of neighbors attached to local links. Routers also use ND to discover neighbors and link layer information. ND also updates the neighbor database with valid entries, invalid entries, and entries migrated to various locations.

ND protocol provides you with the following services:

- address and prefix discovery: hosts determine the set of addresses that are on-link for the given link. Nodes determine which addresses or prefixes are locally reachable or remote with address and prefix discovery.
- router discovery: hosts discover neighboring routers with router discovery. Hosts establish neighbors as default packet-forwarding routers.
- parameter discovery: host and routers discover link parameters such as the link MTU or the hop limit value placed in outgoing packets.
- address autoconfiguration: nodes configure an address for an interface with address autoconfiguration. See "Host autoconfiguration" (page 35).
- duplicate address detection: hosts and nodes determine if an address is assigned to another router or a host.
- address resolution: hosts determine link layer addresses (MAC for Ethernet) of the local neighbors (attached on the local network), provided the IP address is known.
- next-hop determination: hosts determine how to forward local or remote traffic with next-hop determination. The next hop can be a local or remote router.
- neighbor unreachability detection: hosts determine if the neighbor is unreachable, and address resolution must be performed again to

update the database. For neighbors you use as routers, hosts attempt to forward traffic through alternative default routers.

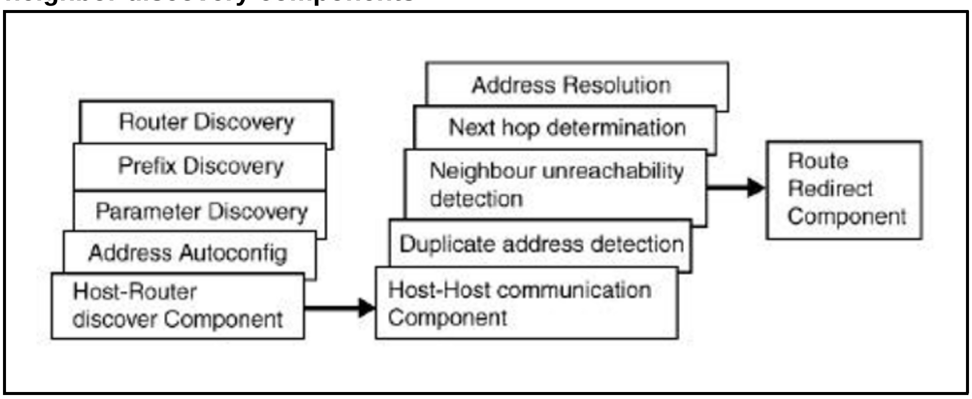
- redirect: routers inform the host of more efficient routes with redirect messages.

Neighbor discovery uses three components:

- host-router discovery
- host-host communication component
- redirect

See Figure 4 "neighbor discovery components" (page 31) for the ND components.

Figure 4
neighbor discovery components



ND messages

Table 2 "IPv6 and IPv4 neighbor comparison" (page 31) shows new ICMPv6 message types.

Table 2
IPv6 and IPv4 neighbor comparison

IPv4 neighbor function	IPv6 neighbor function	Description
ARP Request message	Neighbor solicitation message	A node sends this message to determine the link-layer address of a neighbor or to verify that a neighbor is still reachable through a cached link-layer address. You can also use neighbor solicitations for duplicate address detection.
ARP Reply message	Neighbor advertisement	A node sends this message either in response to a received neighbor solicitation message or to communicate a link layer address change.

Table 2
IPv6 and IPv4 neighbor comparison (cont'd.)

IPv4 neighbor function	IPv6 neighbor function	Description
ARP cache	Neighbor cache	The neighbor cache contains information about neighbor types on the network. See "Neighbor discovery cache" (page 32).
Gratuitous ARP	Duplicate address detection	A host or node sends a request with its own IP address to determine if another router or host uses the address. The source receives a reply from the duplicate device. Both hosts and routers use this function.
Router solicitation message (optional)	Router solicitation (required)	The host sends this message upon detecting a change in a network interface operational state. The message requests that routers generate router advertisement immediately rather than at the scheduled time.
Router advertisement message (optional)	Router advertisement (required)	Routers send this message to advertise their presence with various links and Internet parameters either periodically or in response to a router solicitation message. Router advertisements contain prefixes that you use for on-link determination or address configuration, and a suggested hop limit value.
Redirect message	Redirect message	Routers send this message to inform hosts of a better first hop for a destination.

Neighbor discovery cache

The neighbor discovery cache lists information about neighbors in your network.

The neighbor discovery cache can contain the following types of neighbors:

- static: a configured neighbor
- local: a device on the local system
- dynamic: a discovered neighbor

Table 3 "Neighbor cache states" (page 33) describes neighbor cache states.

Table 3
Neighbor cache states

State	Description
Incomplete	A node sends a neighbor solicitation message to a multicast device. The multicast device sends no neighbor advertisement message in response.
Reachable	You receive positive confirmation within the last reachable time period.
Stale	A node receives no positive confirmation from the neighbor in the last reachable time period.
Delay	A time period longer than the reachable time period passes since the node received the last positive confirmation, and a packet was sent within the last DELAY_FIRST_PROBE_TIME period. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME period of entering the DELAY state, neighbor solicitation is sent and the state changes to PROBE.
Probe	Reachability confirmation is sought from the device every retransmit timer period.

The following events affect the neighbor cache. The following events involve Layer 2 and Layer 3 interaction during processing:

- flushing the virtual LAN (VLAN) MAC
- removing a VLAN or brouter
- performing an action on all VLANs
- removing a port from a VLAN
- removing a port from a spanning tree group (STG)
- removing a multilink trunk (MLT) group from a VLAN
- removing an MLT port from a VLAN
- removing an MLT port from an STG
- performing an action that disables a VLAN, such as removing all ports from a VLAN
- disabling a tagged port that is a member of multiple routable VLANs

Table 4 "IPv4 and IPv6 neighbor discovery comparison" (page 34) shows a comparison of IPv4 and IPv6 neighbor discovery.

Table 4
IPv4 and IPv6 neighbor discovery comparison

IPv4 neighbor functions	IPv6 neighbor functions
ARP Request message	Neighbor solicitation message
ARP Reply message	Neighbor advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate address detection
Router solicitation message (optional)	Router solicitation (required)
Router advertisement message (optional)	Router advertisement (required)
Redirect message	Redirect message

Router discovery

IPv6 nodes discover routers on the local link with router discovery. The IPv6 router discovery process uses the following messages:

- “Router advertisement” (page 34)
- “Router solicitation” (page 34)

Router advertisement

Configured interfaces on an IPv6 router send out router-advertisement messages. Router-advertisements are also sent in response to router-solicitation messages from IPv6 nodes on the link.

Router solicitation

An IPv6 host without a configured unicast address sends router solicitation messages.

IPv6 and the Ethernet Routing Switch 8600

IPv6 routing provides an underlying mechanism to transmit data blocks from source to destination. The source and destination are hosts, identified by fixed-length IPv6 addresses.

The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) provide a transport facility for data transmission. TCP is a reliable mechanism. UDP is not as reliable as TCP. Routing protocols identify the shortest path from a source to a destination. The Internet Protocol defines a standard format primarily known as the IP header, required for successful delivery of datagrams.

Transport and routing protocols are not physical media dependant. The next hop path calculated by the routing protocol in path from the source to the destination can result in the next hop being connected on an Ethernet interface. In this case, the next-hop router must request a mapping of a next-hop IPv6 address to a 48-bit MAC address. The IPv6 Neighbor Discovery Protocol, described in RFC2461, defines a mechanism to identify existing or upcoming neighbors in the network. This mechanism combines the ARP, router discovery, and redirect information. Due to this combination of features, the mechanism supports the autoconfiguration of host entities.

IPv6 requires installed R or RS modules in the Ethernet Routing Switch 8600 chassis. IPv6 also requires at least one 8692 SF/CPU Enterprise Enhanced SF/CPU with SuperMezz or at least one 8895 SF/CPU (no SuperMezz is required on the 8895 SF/CPU). IPv6 on the Nortel Ethernet Routing Switch 8600 basic redistribution uses Open Shortest Path First (OSPF) v3, local, and static routes. Nonlocal next-hop static routes are possible.

Management access

The Nortel Ethernet Routing Switch 8600 contains an Ethernet port for both master and standby SF/CPUs. You configure these Ethernet ports differently from the regular switch ports. In IPv4, the protocol stack operating for these ports is different from the switch IP stack. The IPv6 functionality for the SF/CPU Ethernet port is offered only when the switch operational state is up, and is not offered from the boot monitor level.

The management port provides two functions:

- configuring IPv6 after the system boots up in the CLI and device management through the configured IPv6 address
- configuring static routes reachable through the management route for connectivity

IPv6 supports multiple addresses on each interface and for multiple addresses to management IP interface.

In addition to the management port, you can configure management routes to reach nonlocal destinations.

The Nortel Ethernet Routing Switch 8600 advertises the management port and the management route to the regular routing domain (OSPFv3), but does not include the prefix for the interface in the router advertisement.

Host autoconfiguration

The Nortel Ethernet Routing Switch 8600 can automatically configure a host (node), and assign addresses automatically.

Stateless autoconfiguration enables serverless basic configuration of IPv6 nodes and renumbering from a mathematical perspective.

Stateless autoconfiguration = network prefix (router advertisement) + IPv6 Interface Identifiers.

Stateless autoconfiguration uses the network prefix information in the router advertisement messages from the node address. The Extended Unique Identifier (EUI-64) format obtains the remaining address. The IPv6 interface address is created from the 48-bit (6-byte) MAC address as follows:

1. EUI-64 Hexadecimal digits 0xff-fe are inserted between the third and fourth bytes of the MAC address to obtain the EUI-64.
2. The universal or local bit, the second lower-order bit of the first byte of the MAC address, is complemented.

For example, the IPv6 identifier for host A uses the MAC address 00-AA-00-3F-2A-1C. To automatically assign an address, the following occurs:

1. Convert to EUI-64 format

   00-AA-00-**FF-FE**-3F-2A-1C
2. Complement the Universal/Local (U/L) bit.

   The first byte in binary form is 00000000. When the seventh bit is complemented, it becomes 00000010 (0x02).

   The result is 0**2**-AA-00-**FF-FE**-3F-2A-1C or 2AA:FF:FE3F:2A1C.

Thus, host A with MAC address 00-AA-00-3F-2A-1C, combined with network prefix 2001::/64 provided by router advertisement, uses an IPv6 address 2001::2AA:FF:FE3F:2A1C.

If no router is present, a host can generate a link-local address with the prefix FE80. The link-local address for a node with the MAC address 00-AA-00-3F-2A-1C is FE80::2AA:FF:FE3F:2A1C.

The Neighbor Discovery Protocol performs autoconfigration. See "Neighbor discovery" (page 30).

The following are the states of autoconfiguration address:

- Tentative: the address is being verified as unique (link-local address)
- Valid: an address from which unicast traffic can be sent and received and can be in one of two states
- Preferred: an address for which uniqueness was verified for unrestricted use

- Deprecated: an address that remains valid but is withheld for new communication
- Invalid: an address for which a node can no longer send or receive unicast traffic

A valid lifetime is the length of time of the preferred and depreciated state. The preferred lifetime is the length of time for the tentative, preferred, and depreciated state.

IPv6 VLANs and brouter ports

The Nortel Ethernet Routing Switch 8600 supports three logical types of interfaces that participate in the IPv6 routing arena:

- Virtual LAN interface: Release 4.1 supports port-based VLANs and protocol-based VLANs. VLANs can contain MLT and SMLT ports.
- Brouter port: In IPv4, the brouter port support is limited to the physical port. In Release 4.1, IPv6 extends support to MLTs. This support is possible because the Layer 3 software treats MLTs as logical ports. Each logical IPv6 interface can use multiple IPv6 addresses.

Tunneling

Tunneling provides a mechanism for transferring IPv6 traffic through an IPv4 network.

Manually configured tunnels

Manually configured tunnels are point-to-point. IPv6 reachability enables tunnel forwarding.

Manually configured tunnels provide communication between two isolated IPv6 domains over an IPv4 network. Create a point-to-point connection between the two isolated IPv6 devices by configuring the tunnel endpoints. Tunnel interfaces are logical point-to-point interfaces. Enable a routing protocol, such as the Open Shortest Path First (OSPF) protocol, on the interfaces to allow dynamic routing.

You cannot configure the maximum transmission unit (MTU) for tunnels. The default MTU value for tunnels is 1280. Tunnel operational status depends on the IPv4 reachability of the tunnel endpoint. The Nortel Ethernet Routing Switch 8600 attempts reachability through R or RS modules and updates IPv6 information with changes.

Configure IPv6 and IPv4 addresses at each end of the tunnel. The router or host at the source and destination of the tunnel must support both IPv4 and IPv6 protocol stacks.

Path MTU discovery

IPv6 routers do not fragment packets. The source node sends a packet equal in size to the maximum transmission unit (MTU) of the link layer. The packet travels through the network to the source. If the packet encounters a link to a smaller MTU, the router sends the source node an ICMP error message containing the MTU size of the next link.

The source IPv6 node then resends a packet equal to the size of the MTU included in the ICMP message.

The default MTU value for a regular interface is 1500.

Routing

A routing table is present on all nodes. The table stores information about IPv6 network prefixes and how to reach them. IPv6 checks the destination neighbor cache first. If the destination is not in the destination neighbor cache, the routing table determines:

- the interface used for forwarding (the next-hop interface)
- the next-hop address

The switch requires routing protocols to exchange IPv6 routing prefixes. IPv6 routes in a routing table can be:

- directly attached network routes using a 64-bit prefix
- remote network routes using a 64-bit or lower prefix
- host routes using a 128-bit prefix length
- the default route using a prefix of ::/0

Route redistribution is limited to static routes and local devices by using the OSPFv3 protocol. The only dynamic protocol supported is OSPFv3.

When you configure routing on a VLAN, an IP address is assigned to the VLAN and is not associated with any particular physical port. Brouter ports are VLANs that route IP packets and bridge nonroutable traffic in a single-port VLAN.

This section contains the following topics:

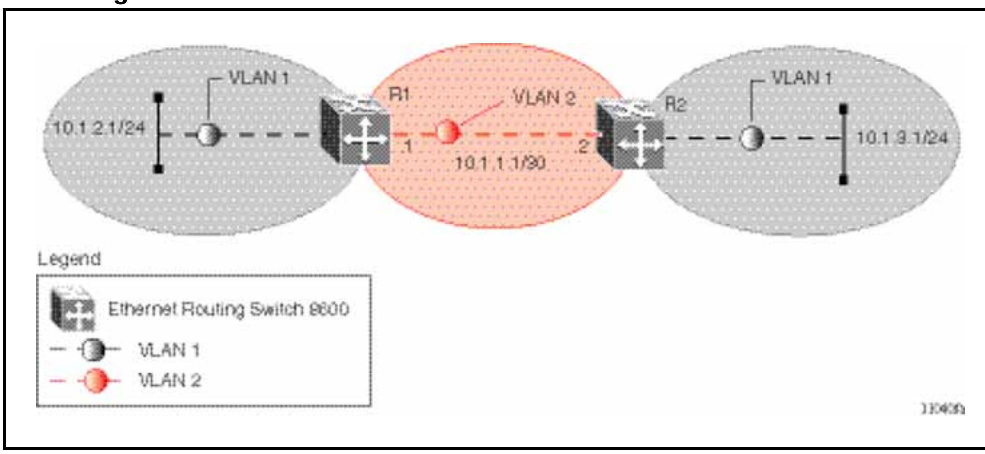
- “Virtual routing between VLANs” (page 39)
- “Brouter ports” (page 39)
- “Static routes” (page 40)
- “Open Shortest Path First protocol” (page 43)

Virtual routing between VLANs

The Nortel Ethernet Routing Switch 8600 supports wire-speed IP routing between VLANs. As shown in Figure 5 "IP routing between VLANs" (page 39), although VLAN 1 and VLAN 2 reside on the same switch, for traffic to flow from VLAN 1 to VLAN 2, you must route the traffic.

When you configure routing on a VLAN, an IP address assigned to the VLAN is the virtual router interface address for the VLAN. The VLAN IP address is called a virtual router interface because it is associated with no particular port. The VLAN IP address can be reached through any VLAN port, and frames route from the VLAN through the gateway IP address. You can forward routed traffic to another VLAN within the switch.

Figure 5
IP routing between VLANs



When you enable Spanning Tree Protocol on a VLAN, the spanning tree convergence must be stable before the routing protocol becomes active. This requirement can lead to an additional delay in IP traffic forwarding.

Because a port can belong to multiple VLANs, a one-to-one correspondence no longer exists between the physical port and the router interface.

As with any IP address, you can use virtual router interface addresses for device management. For the Simple Network Management Protocol (SNMP) or Telnet management, you can use any virtual router interface address to access the switch while routing is enabled on the VLAN.

Brouter ports

The Nortel Ethernet Routing Switch 8600 also supports brouter ports. A brouter port is a single-port VLAN that can route IP packets and bridge all nonroutable traffic. The difference between a brouter port and a standard protocol-based VLAN configured for routing is that the routing interface of the brouter port is not subject to the spanning tree state of the port.

A brouter port can be in the blocking state for nonroutable traffic while it routes IP traffic. This feature removes interruptions caused by Spanning Tree Protocol recalculations in routed traffic.

A brouter port is a one-port VLAN; therefore, each brouter port decreases the number of available VLANs by one and uses one VLAN ID.

Static routes

Static routes provide an alternative method for establishing route reachability. This function, with dynamic routes, provides routing information from the forwarding database to the forwarding plane. Only enabled static routes are submitted to the Route Table Manager (RTM), which determines the best route based on reachability, route preference, and cost. The RTM communicates all updates to best routes to the forwarding plane.

You must provide the following options to configure a static route:

- Local or Nonlocal hop option: configure a static route either with a next hop that exists on a locally attached network or a next hop that is reachable through a dynamic route. The static route is available as long as the next hop is reachable.
- Route preference: you can specify the route preference for the static routes as follows:
  - Global value for all static routes: preference is either static or dynamic routes.
  - Preference for each static route entry: if specified, this value overrides the global value for the entry. This provides flexibility to change the general behavior of a specific static route.
- Administrative status: controls when the static route is considered for forwarding. Administrative status differs from the operational status. An admin-enabled static route can still be unreachable and cannot be used for forwarding. An admin-disabled static route is operationally a nonexistent route.
- Multiple static routes: specify alternative paths to the same destination. Multiple static routes provide stability and load balancing.

To configure a default static route, supply a value of 0 for the prefix and the prefix length.

Events that affect static route operation include user-configured changes or other system events. The table below describes these changes.

Table 5
Static route operation changes

Action	Result
Changing the administrative status of the static route	Makes the static route unavailable for forwarding.
Deleting the IPv6 addresses of a VLAN or brouter port	Permanently deletes the static routes with the corresponding local neighbors from the RTM, the forwarding database, and the configuration database.
Deleting a VLAN	Removes static routes with a local next-hop option from the configuration database. Static routes with a nonlocal next-hop option become inactive (they are removed from the forwarding database).
Disabling forwarding on a VLAN or brouter port	Static routes reachable through the locally attached network become inactive.
Disabling a VLAN or brouter port	Makes the static routes inactive.
Disabling IPv6 forwarding globally	Stops forwarding all IPv6 traffic.
Learning changes about a dynamically learned neighbor	When a neighbor becomes unreachable or is deleted, the static route with the neighbor becomes inactive, and the configuration is not affected. The static route with the neighbor becomes active in the configuration and is added to the RTM and forwarding database when the neighbor becomes reachable.
Enabling a static route	Adds the route to the RTM to change certain static routes to active.
Deleting a static route	Permanently deletes a static route from the configuration.
Disabling a static route	Stops traffic on the static route but does not remove the route from the configuration.
Changing a preference	When the static route preference changes, the best routes for the entries use both static and dynamic paths

Table 5
Static route operation changes (cont'd.)

Action	Result
Deleting or disabling a tunnel	Deletes or disables a tunnel and removes the tunnel entry from the forwarding table.
Enabling the tunnel	Enables a tunnel, activates the tunnel static routes and adds an entry to the forwarding table.

The local-nexthop flag is not required for Pv6. An IPv4 device cannot learn a neighbor ARP entry unless the device uses a local route entry. In IPv6, a host can learn a neighbor entry if the device is physically connected to the neighbor (one hop).

The static route becomes active when the next hop is reachable by a dynamic route neighbor resolution. The static route takes the forwarding information from the dynamic route. If the next hop is reachable using a local route, the neighbor resolution is required.

IP static route table

The static route table is separate from the system routing table that the router uses to make forwarding decisions. Use the static route table to directly change static routes. Although the tables are separate, the system routing table automatically reflects the static routing table manager entries if the next hop address in the static route is reachable and if the static route is enabled.

The static route table is indexed by four attributes:

- Destination Network
- Destination Mask
- Next Hop
- ifIndex

The maximum number of entries is 500. You can insert static routes by using the static route table, and you can delete static routes by using either the static route table or the system routing table.

ATTENTION
The system routing table stores only active static routes with the best route preference. A static route is active only if the route is enabled and if the next hop address is reachable (for example, if a valid ARP entry exists for the next hop).

You can enter multiple routes (for example, multiple default routes) that use different costs and the lowest cost route that is reachable appears in the routing table. If you enter multiple next hops for the same route with the same cost, the switch does not replace the existing route. If you enter the same route with the same cost and a different next hop, the first route is used. However, if that first route becomes unreachable, the second route (with a different next hop) is activated with no connectivity loss.

Static routes configured for the management port apply using the natural mask of the network. Because traffic that originates from the switch refers to these routes before checking the IP routing table, the switch management traffic can be incorrectly forwarded from the management port, even though a specific route exists in the routing table.

Open Shortest Path First protocol

Open Shortest Path First (OSPF) protocol is an Interior Gateway Protocol (IGP) that distributes routing information between routers belonging to a single autonomous system (AS). OSPF is a link-state protocol intended for use in large networks.

This section contains the following topics:

Overview

In an OSPF network, each router maintains a link-state database that describes the topology of the autonomous system (AS). The database contains the local state for each router in the AS, including usable interfaces and reachable neighbors. If the router detects changes, it shares them by flooding link-state advertisements (LSAs) throughout the AS. Routers synchronize topological databases based on shared information from LSAs.

From the topological database, each router constructs a shortest-path tree, with itself as the root. The shortest-path tree provides the optimal route to each destination in the AS. Routing information from outside the AS appears on the tree as leaves.

OSPF routes IP traffic based solely on the destination IP address and the prefix in the IP packet header.

OSPFv3 is supported in IPv6 routing. OSPFv3 runs for each link rather than for each subnet. Multiple instances are possible on a single link. OSPFv3 does not support the OSPFv2 authentication feature.

Benefits

In large networks, OSPF offers the following benefits:

- Fast convergence: during topological changes, OSPF recalculates routes quickly.
- Minimal routing protocol traffic: OSPF sends updates only when changes occur and minimizes the traffic.
- Load sharing: OSPF provides support for equal-cost multipath routing. If several equal-cost routes to a destination exist, traffic is distributed equally among them.
- Type of Service: separate routes can be calculated for each IP Type of Service.

Autonomous system and areas

You can subdivide the AS into areas that group contiguous networks, routers that connect to these networks, and attached hosts. Each area uses a topological database that is invisible from outside the area. Routers within an area cannot access the topology of other areas. Subdividing the AS into areas significantly reduces routing protocol traffic compared to treating the entire AS as a single link-state domain.

Attach a router to more than one area to maintain a separate topological database for each connected area. Two routers within the same area maintain identical topological databases for that area. Assign a unique area ID to each area. The area ID 0.0.0.0 is reserved for the backbone area.

Packets route in the AS based on the source and destination addresses. If the source and destination of a packet reside in the same area, intra-area routing occurs. If the source and destination of a packet reside in different areas, inter-area routing occurs. Intra-area routing prevents the use of information obtained outside the area to protect the area from incorrect routing information. Inter-area routing must pass through the backbone area.

This section contains the following topics:

Backbone area

The backbone area consists of the following network types:

- networks and attached routers not in any other area
- routers that belong to multiple areas

The backbone is usually contiguous, but you can configure virtual links to create a noncontiguous area.

Configure virtual links between any two backbone routers that use an interface to a common nonbackbone area. Virtual links belong to the backbone and use intra-area routing only. For a description of virtual links, see “OSPF virtual links” (page 53).

The backbone distributes routing information between areas. The backbone area topology is invisible to other areas. Other area topologies are invisible to the backbone area.

The OSPF routing algorithm finds the paths with the lowest cost. The topology of the backbone dictates the backbone paths used between areas. The algorithm examines the routing table summaries for each connected area boarder router (ABR) to select inter-area paths. The OSPF behavior is modified, according to OSPF standards so that OSPF routes are not learned through an ABR unless the router connects to the backbone or through a virtual link.

Stub area

You configure stub areas at the edge of the OSPF routing domain. Stub areas use one ABR. A stub area receives no LSAs for routes outside the area, reducing the size of the link-state database. The ABR examines packets destined for outside the stub area before it forwards the packet to the destination.

The OSPF routing algorithm treats the network behind a passive interface as a stub area that forms no adjacencies. The OSPF routing algorithm advertises the network into the OSPF area as an internal route.

Not so stubby area

A not so stubby area (NSSA) replaces LSAs with a default route to prevent external LSAs from flooding the area. An NSSA can import small stub (non-OSPF) routing domains into OSPF. Like stub areas, NSSAs are at the edge of an OSPF routing domain. Non-OSPF routing domains attach to the NSSAs to form NSSA transit areas. The NSSA border router performs manual aggregation by accessing the addressing scheme of small stub domains.

Neighbors

In an OSPF network, any two routers with an interface to the same network are neighbors. Routers use the Hello Protocol to discover neighbors and to maintain neighbor relationships. On a broadcast or point-to-point network, the Hello Protocol dynamically discovers neighbors. On a nonbroadcast multiaccess network (NBMA), you must manually configure neighbors for the network.

The Hello Protocol provides bidirectional communication between neighbors. Periodically, OSPF routers send hello packets over all interfaces. These hello packets include the following information:

- the priority
- the Hello Timer and Dead Timer values
- a list of routers that sent hello packets on the interface
- the choice between designated router (DR) and backup designated router (BDR)

Routers establish bidirectional communication when one router discovers that it is listed in the neighbor router hello packet.

This section contains the following topics:

- "Neighbors on NBMA networks" (page 47)
- "Neighbor adjacencies" (page 47)
- "NBMA adjacencies" (page 47)

Neighbors on NBMA networks

NBMA interfaces with a positive router priority and a nonzero value can become the DR for the NBMA network and are configured with a list of all attached routers. The neighbors list includes each neighbor IP address and router priority. You must manually configure the IP address, mask, and router priority of neighbors on routers that can become the DR or BDR for the network.

Log messages indicate when an OSPF neighbor state changes. This log message indicates the previous state and the new state of the OSPF neighbor. The log message generated for system traps also indicates the previous state and the current state of the OSPF neighbor.

Neighbor adjacencies

Neighbors can form an adjacency to exchange routing information. When two routers form an adjacency, the routers perform a database exchange to synchronize the topological databases. When the routers synchronize databases, the routers are fully adjacent. Bandwidth is conserved because only routing change information passes between adjacent routers.

All routers connected by a point-to-point network or to a virtual link always form an adjacency. All routers on a broadcast or NBMA network form an adjacency with the DR and the BDR.

NBMA adjacencies

Before a DR is elected in an NBMA network, the router sends hello packets only to those neighbors eligible to become the DR. The NBMA DR forms adjacencies only with configured neighbors and drops all packets from other sources. The neighbor configuration also specifies to the router the expected hello behavior for each neighbor.

> **ATTENTION**
> If a router receives a hello packet from a neighbor with a priority different from the configured priority, the router automatically changes the configured priority to match the dynamically learned priority.

OSPF routers

To limit the amount of routing protocol traffic, the Hello Protocol elects a designated router (DR) and a backup designated router (BDR) on each multiaccess network. Instead of neighboring routers forming adjacencies and swapping link-state information with each other (which, on a large network, can mean a large volume of routing protocol traffic), all routers on the network form adjacencies only with the DR and the BDR and send link-state information to the DR and BDR. The DR redistributes this information to every other adjacent router.

In backup mode, the BDR receives link-state information from all routers on the network and listens for acknowledgements. If the DR fails, the BDR transitions quickly to the role of DR because routing tables are up to date.

Router types

Routers in an OSPF network can perform different roles depending on router configuration. Table 6 "Router types in an OSPF network" (page 48) describes the router types you can configure in an OSPF network.

Table 6
Router types in an OSPF network

Router Type	Description
AS boundary router (ASBR)	A router attached at the edge of an OSPF network is called an AS boundary router (ASBR). An ASBR uses one or more interfaces that run an interdomain routing protocol such as the Border Gateway Protocol (BGP). In addition, any router distributing static routes or Routing Information Protocol (RIP) routes into OSPF is an ASBR. The ASBR forwards external routes into the OSPF domain. In this way, routers inside the OSPF network learn about destinations outside their domain.
Area border router (ABR)	A router attached to two or more areas inside an OSPF network is an area border router (ABR). ABRs play an important role in OSPF networks by condensing the amount of OSPF information that is disseminated.
Internal router (IR)	A router that uses interfaces only within a single area inside an OSPF network is an internal router (IR). Unlike ABRs, IRs use topological information only about the local area.
Designated router (DR)	In a broadcast or NBMA network, a single router is the designated router (DR) for that network. A DR ensures that all routers on the network synchronize and advertise that network to the remainder of the AS.
Backup designated router (BDR)	A backup designated router (BDR) is elected in addition to the designated router (DR) and becomes the DR if required.

OSPF interfaces

An OSPF interface, or link, is configured on an IP interface. In the Nortel Ethernet Routing Switch 8600, an IP interface can be a single link (brouter port) or a logical interface configured on a VLAN (multiple ports). The underlying lower level protocols and the routing protocol itself obtain the state information associated with the interface.

The Nortel Ethernet Routing Switch 8600 designates OSPF interfaces as one of the following types:

- broadcast (active)
- nonbroadcast multiaccess (NBMA)
- point-to-point
- point-to-multipoint

> **ATTENTION**
> When you enable an OSPF interface, you cannot change the interface type. You must first disable the interface. You can then change the type and reenable the interface. For an NMBA interface, you must also first delete the manually configured neighbors.

This section contains the following topics:

- “Broadcast interface” (page 49)
- “Nonbroadcast multiaccess interface” (page 49)

Broadcast interface

Broadcast interfaces support many attached routers and can address a single physical message to all attached broadcast routers (sent to AllSPFRouters and AllDRouters).

Broadcast interfaces discover neighboring routers dynamically using the OSPF Hello Protocol. Each pair of routers on a broadcast network, such as an Ethernet, communicate directly.

Nonbroadcast multiaccess interface

Nonbroadcast multiaccess (NBMA) interfaces support many routers but cannot broadcast.

In contrast to a broadcast network where some OSPF protocol packets are multicast (sent to AllSPFRouters and AllDRouters), NBMA interfaces replicate and send OSPF packets to each neighboring router, in turn, as unicast. NBMA networks drop all OSPF packets with destination addresses to AllSPFRouters and AllDRouters.

Designated router parameters

OSPF treats an NBMA network like a broadcast network. Because many routers attach to the network, OSPF designates a router (DR) to generate the network link-state advertisements.

Because the NBMA network does not broadcast, you must manually configure neighbors for each router eligible to become the DR (those with a positive, nonzero router priority). You must also configure a PollInterval for the network.

NBMA neighbors list and priorities

NBMA interfaces with a positive, nonzero-value router priority can become the DR for the NBMA network and are configured with a list of all attached routers, or neighbors. This neighbors list includes the IP address and router priority for each neighbor.

The neighbors list is used during and after the DR-election process. When an interface to a nonbroadcast network with a nonzero priority becomes active, and before the Hello Protocol elects a DR, the router sends hello packets only to those neighbors eligible to become the DR (or those with a positive nonzero router priority). When a DR is elected, it forms adjacencies only with configured neighbors and drops all packets from other sources. This neighbor configuration communicates the expected hello behavior of each neighbor to the router.

ATTENTION
If a router that is eligible to become the DR receives a hello packet from a neighbor showing a priority different from the current configured neighbor priority, the DR changes the configured priority to match the dynamically learned priority.

NBMA PollInterval

A PollInterval also configures an NBMA interface. The PollInterval designates the interval at which OSPF sends hello packets to inactive neighboring routers. OSPF typically sends hello packets at the HelloInterval, for example, every 10 seconds. If a neighboring router becomes inactive or receives no hello packets for the established RouterDeadInterval, the NBMA interface sends hello packets at the specified PollInterval, for example, every 120 seconds.

Sending hello packets

You must configure a neighbors list for the DR to allow an NBMA network to send hello packets. If the router is eligible to become a DR (if the router priority is a positive nonzero value), it periodically sends hello packets to all neighbors that are also eligible. Any two eligible routers must always exchange hello packets for the correct DR election. Minimize the number of eligible routers on a nonbroadcast network to minimize the number of hello packets sent on that network.

A newly elected DR sends hello packets to all manually configured neighbors, synchronizes the link-state databases, establishes itself as DR, and identifies the BDR.

If a router is not eligible to become the DR, it periodically sends hello packets to both the DR and the BDR. The router also sends a hello packet in reply to a hello packet received from any eligible neighbor (other than the current DR and BDR). This process establishes an initial bidirectional relationship with any potential DR.

When hello packets are being periodically sent, the neighbor state determines the interval between the packets. If the neighbor is in the down state, the neighbor sends hello packets at the designated PollInterval, for example, every 120 seconds. Otherwise, neighbors send hello packets at the designated HelloInterval, for example, every 10 seconds.

Forming adjacencies

In an NBMA network, as in a broadcast network, all routers become adjacent to the DR and the BDR. The adjacencies form after the router priorities are assigned, the neighbors are configured, and the network DR is elected.

OSPF and IP

OSPF runs on top of IP, which means that nodes send an OSPF packet with an IP data packet header. The protocol field value in the IP header is 89, which identifies it as OSPF and distinguishes it from other packets that use an IP header.

An OSPF route advertisement expresses a destination as an IP address and a variable-length mask. The address and the mask indicate the range of destinations to which the advertisement applies.

OSPF can specify a range of networks and can send one summary advertisement that represents multiple destinations. For example, a summary advertisement for the destination 128.185.0.0 with a mask of 255.255.0.0 describes a single route to destinations 128.185.0.0 to 128.185.255.255.

OSPF packets

All OSPF packets start with a 24-octet header containing information about the OSPF version, the packet type and length, the ID of the router transmitting the packet, and the ID of the OSPF area from which the packet is sent. An OSPF packet is one of the following types:

- Hello packets

  Hello packets transmit between neighbors and are never forwarded. The Hello Protocol requires routers to send hello packets to neighbors at predefined hello intervals. If the router receives no hello packets within the specified dead interval, the neighbor router declares the other router dead.

- Database description (DD) packets

  OSPF exchanges DD packets when a link is first established between neighboring routers that synchronize the link-state databases.

- Link-state request packets

  Link-state request packets describe one or more link-state advertisements that a router requests from a neighbor. Routers send link-state requests if the information received in DD packets from a neighbor is not consistent with the router’s link-state database.

- Link-state update packets

  Link-state update packets contain one or more link-state advertisements and are sent following a change in network conditions.

- Link-state acknowledgement packets

  Link-state acknowledgement packets acknowledge receipt of link-state updates containing the header information from the received link-state advertisements.

Link-state advertisements

OSPF does not require each router to send the entire routing table to the neighbors. Instead, each OSPF router floods only link-state change information in the form of link-state advertisements (LSAs) throughout the area or AS. LSAs in OSPF are one of the following six types:

- Router-links advertisement

  A router originates one or more router LSAs for an area. Each router LSA contains interface descriptions. The router LSAs for an area describe the states of all the router interfaces to the area. Link-state ID fields distinguish multiple router LSAs.

- Network-links advertisement

  The link designated router originates a network LSA for every broadcast or NBMA link having two or more attached routers. The network LSA lists all routers attached to the link.

- Inter-area-prefix links advertisement

  The inter-area-prefix links advertisement describes an external prefix that is internal to the autonomous system.

- Inter-area-router links advertisement

  The inter-area-router links advertisement describes a path to a destination external OSPF router (an ASBR) that is internal to the Autonomous System.

- As-external links advertisement

  The as-external links advertisement describes a path to a prefix. The described path is external to the Autonomous System.

- link LSA

  OSPFv3 includes link LSA for the following three purposes:

  — to provide the router link-local address to other routers on a link

  — to distribute the prefixes associated with the link to routers on the link

  — to allow the router to insert option bits to the network LSA

AS external routes

With OSPF, the following routes are AS external (ASE) routes:

- a route to a destination outside the AS
- a static route
- a default route
- a directly connected network not running OSPF

OSPF virtual links

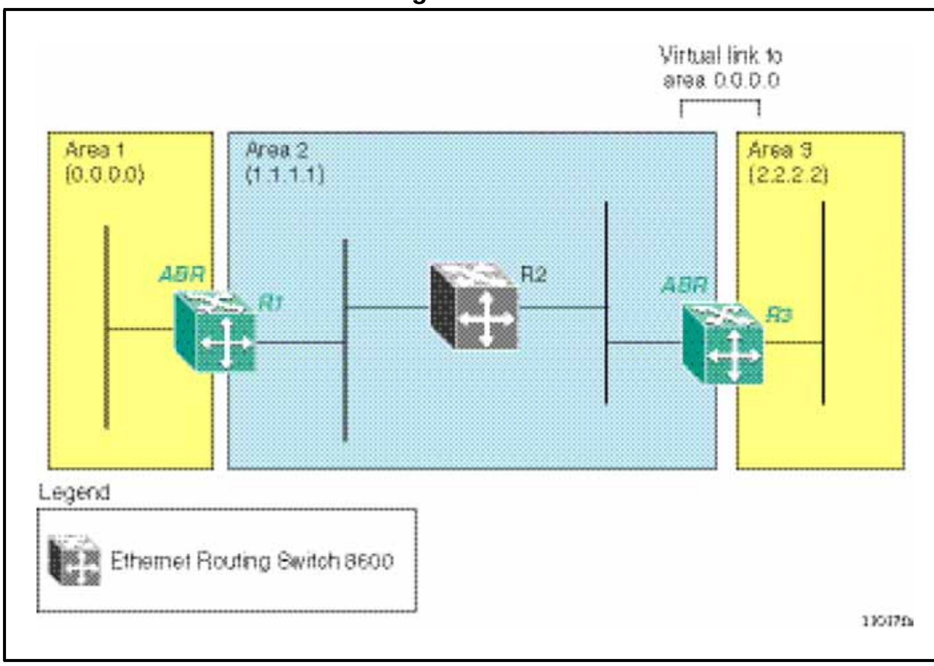
On an OSPF network, a Nortel Ethernet Routing Switch 8600 that is an ABR must connect directly to the backbone. If no physical connection is available, you can configure a virtual link automatically or manually.

An automatic virtual link provides redundancy support for critical network connections. Automatic virtual linking creates virtual paths for vital traffic paths in your OSPF network. The virtual link is available to maintain connectivity if a network connection fails, such as when an interface cable connected to the backbone (either directly or indirectly) disconnects from the switch.

Specifying automatic virtual linking ensures that a link is created to another router. When you specify automatic virtual linking, the feature is always ready to create a virtual link. Create manual virtual links if automatic virtual linking uses more resources than you want to use. With virtual links, you can conserve resources, while having specific control over virtual link placement in your OSPF configuration.

Figure 6 "Virtual link between ABRs through a transit area" (page 54) shows how to configure a virtual link between the ABR in area 2.2.2.2 and the ABR in area 0.0.0.0.

Figure 6
Virtual link between ABRs through a transit area



To configure a virtual link between the ABRs in Area 1 and Area 3, define Area 2 as the transit area between the two areas. Identify R2 as the neighbor router, through which R2 must send information to reach the backbone through R1.

Specifying ASBRs

ASBRs advertise non-OSPF routes into OSPF domains so that they can pass through the OSPF routing domain. A router can function as an ASBR if one or more of the router interfaces connects to a non-OSPF network.

Limit the number of ASBRs in your network to conserve resources, or to specifically control which routers perform as ASBRs to control traffic flow.

OSPF routing algorithm

A separate copy of the OSPF routing algorithm runs in each OSPF area. Routers that connect to multiple areas run multiple copies of the algorithm. The processes governed by the routing algorithm are as follows:

- When a router starts, it initializes the OSPF data structures and then waits for indications from lower level protocols that the interfaces are functional.
- A router uses the Hello Protocol to discover neighbors. On point-to-point and broadcast networks, the router dynamically detects neighbors by sending hello packets to the multicast address AllSPFRouters. On nonbroadcast multiaccess networks, some configuration information is required to discover neighbors.
- On all multiaccess networks (broadcast or nonbroadcast), the Hello Protocol elects a default router (DR) for the network.
- The router attempts to form adjacencies with some neighbors. On multiaccess networks, the DR determines which routers become adjacent. This behavior does not occur if a router is configured as a passive interface because passive interfaces do not form adjacencies.
- Adjacent neighbors synchronize topological databases.
- The router periodically advertises the link state and changes to the local state. LSAs include information about adjacencies to enable quick detection of dead routers on the network.
- LSAs flood throughout the area to ensure that all routers in an area use the same topological database.
- From the database, each router calculates a shortest-path tree, with itself as root. This shortest-path tree yields a routing table for the protocol.

OSPFv3

This section is an overview of the differences between Open Shortest Path First (OSPF)v3 protocol, developed for IPv6, and OSPFv2, used in IPv4. This information is compiled from RFC2740.

The IPv4 terms subnet and network are replaced in IPv6 by link. An IPv6 link is a communication medium between nodes at the link layer. You can assign multiple IP subnets (prefixes) to a link. Two IPv6 nodes with common or different prefixes can communicate over a single link.

OSPF for IPv6 operates on each link rather than each subnet as in IPv4. IPv6 makes the following changes to how packets are received and to the contents of network LSAs and hello packets:

- The OSPF packet contains no IPv6 addresses. LSA payloads carried in link state update packets contain IPv6 addresses.
- The following IDs remain at 32-bits and are not assigned IPv6 addresses: area IDs, LSA link state IDs, and OSPF router IDs.
- Router IDs identify neighboring routers by an IP address on broadcast and NBMA networks in OSPFv2.

Flooding scope

LSA flooding scope is generalized in OSPFv3 and coded in the LS type field of the LSA. The following three flooding scopes are available for LSAs:

- Link-local scope: The LSA is not flooded beyond the local link.
- Area scope: The LSA is flooded in a single OSPF area. Area scope is used in router LSAs, network LSAs, Inter-Area-Prefix-LSAs, Inter-Area-Router LSAs, and Intra-Area-Prefix-LSAs.
- AS scope: The LSA is flooded through the routing domain. AS scope is used for AS-external-LSAs.

Multiple instances per link

OSPFv3 supports multiple OSPF protocol instances on a single link. For example, you can configure a single link in two or more OSPF areas.

An Instance ID in the OSPF packet header and the OSPF interface structures allow multiple protocol instances on a single link.

Link-local addresses

IPv6 uses link-local addresses on a single link. Link-local addresses facilitate features such as neighbor discovery and autoconfiguration. Datagrams with link-local sources are not forwarded. Instead, routers assign link-local unicast addresses from the IPv6 address range.

OSPF for IPv6 assigns link-local unicast addresses to physical segments attached to a router. The source for all OSPF packets sent on OSPF physical interfaces is the associated link-local unicast address. Routers learn link-local addresses for all other nodes on links. The next-hop information during packet forwarding includes the learned addresses.

For OSPF protocol packets, you must use global scope or site-local IP addresses as the source for packets.

Link LSA is the only OSPF LSA type that includes link-local addresses. Link-local addresses must not be advertised in other LSA types.

Authentication

OSPF for IPv6 requires the IP Authentication Header and the IP Encapsulating Security Payload for authentication and security. OSPFv3 does not support the authentication feature from OSPFv2.

IPv6 uses the 16-bit one's complement checksum to protect against accidental data corruption.

Packet format

OSPFv3 runs directly over IPv6. All other addressing information is absent in OSPF packet headers. OSPFv3 is network-protocol-independent. LSA types now contain addressing information.

OSPFv3 implements the following packet changes:

- The hello packet and database description packet operations fields are expanded to 24 bits.
- The packet header does not include Authentication and AuType fields.
- The interface ID replaces the address information in the hello packet. The Interface ID becomes the network LSA link state ID if the router becomes the designated router on the link.
- R-bit and V6-bit in the options field process router LSAs during Shortest Path First (SPF) calculation. R-bits and V6-bits determine participation in topology distribution.
- The packet header includes the Instance ID, which allows multiple OSPF protocol instances on the same link.

R-bit

Unlike OSPF for IPv4, OSPFv3 for IPv6 supports the R-bit (Router bit). The R-bit indicates whether the originating node is an active router.

If the R-bit is cleared, routes that transit the advertising node cannot be calculated.

As an example, if a multi-homed host wishes to participate in routing without forwarding non-locally addressed packets, the R-bit is cleared.

Note that this means that an IPv6-enabled switch can continue to operate as an OSPFv3 neighbor even if you disable IPv6 forwarding on the switch. This behavior differs from IPv4 OSPF, in which the switch drops a neighbor if IP forwarding on the neighbor is disabled.

New LSAs

OSPFv3 includes link LSAs and Intra-Area-Prefix LSAs.

Link LSA

Link LSA uses local-link flooding scope, not flooded beyond the associated link.

Link LSAs have three purposes:

- to provide the link-local address of the router to all other nodes on the link
- to provide the list of IPv6 prefixes associated with the link
- to allow the router to associate options bits with the network LSA for the link

Intra-Area-Prefix-LSA

The Intra-Area-Prefix-LSA carries all IPv6 prefix information. In IPv4, this information is in router LSAs and Network LSAs.

Unknown LSA types

In OSPFv3, unknown LSA types are either stored and flooded as though understood or given local flooding scope. Specific behavior is coded in the LS type field of the header.

Stub area

OSPFv3 retains the concept of stub areas, which minimize link-state databases and routing table sizes.

IPv6 stub areas carry only router LSAs, network LSAs, Inter-Area-Prefix-LSAs, link LSAs, and Intra-Area-Prefix-LSAs.

Unlike IPv4, IPv6 can store LSAs with unrecognized link state (LS) types or flood them as though they are understood. Rules applied to the stub area prevent the excessive growth of the link-state database. An LSA with an unrecognized link state can be flooded only if the LSA uses area or link-local flooding scope, and the LSA U-bit is configured to 0.

Security

IPv6 uses the following key security features: Simple Network Management Protocol version 3 (SNMPv3) and Secure Shell (SSH). For detailed information, see *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601). This section contains the following topics:

- “SNMP version 3” (page 59)
- “Secure Shell” (page 62)

SNMP version 3

SNMPv3 remotely collects management data and configures devices. An SNMP agent is a software process that listens on UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to either retrieve or modify.

SNMPv3 is an SNMP framework that supplements SNMPv2 with the following:

- new SNMP message formats
- security for messages
- access control
- remote configuration of SNMP parameters

The following sections describe SNMPv3 features:

- “Authentication” (page 59)
- “Privacy” (page 59)
- “Security” (page 59)
- “SNMPv3 group option for access policies” (page 60)
- “Configuration” (page 60)
- “Feature specifics” (page 60)
- “User-based security model” (page 61)

Authentication

The message recipient uses authentication within the user-based security model (USM) to verify the message sender and whether the message is altered. USM, HMAC-MD5, and HMAC-SHA-96 support authentication protocols.

Privacy

USM is an encryption protocol for privacy. USM encrypts only the data portion of a message. The header and the security parameters are not encrypted. The privacy protocol supported using USM is CBC-DES Symmetric Encryption Protocol.

Security

SNMPv3 security protects against the following:

- Information modification: protects against altering information in transit
- Masquerade: protects against an unauthorized entity that assumes the identity of an authorized entity

- Message Stream Modification: protects against delaying or replaying messages
- Disclosure: protects against eavesdropping
- Discovery procedure: finds the SnmpEngineID of an SNMP entity for a transport address or transport endpoint address
- Time synchronization procedure: facilitates authenticated communication between entities

SNMPv3 does not protect against the following:

- Denial of service: does not prevent exchanges between a manager and an agent
- Traffic analysis: does not verify the general pattern of traffic between managers and agents

SNMPv3 group option for access policies

The access policy feature in the Ethernet Routing Switch 8600 determines the access level users who connect to the switch by using various services, such as the File Transfer Protocol (FTP), Trivial FTP (TFTP), Telnet, and rlogin. The system access policy feature is based on the access levels and the network address of the user. This feature covers services such as TFTP, HTTP, SSH, rlogin, and SNMP. With SNMPv3, community names do not map to an access level. Only the view-based Access Control Model (VACM) determines the access privileges.

Configuration

The configuration feature enables access policy services to cover SNMP. Create SNMP users and associate SNMP users with groups. Configure an access policy for each group and network.

Feature specifics

When you enable SNMP service, this policy covers all users associated with the groups configured under access policy. The access privileges either allow or deny access. If you select allow, the VACM configuration determines the access level.

The SNMP service default is disabled for all access policies.

The access level configured under access-policy policy <id> does not affect SNMP service. The VACM configuration determines SNMP access rights.

User-based security model

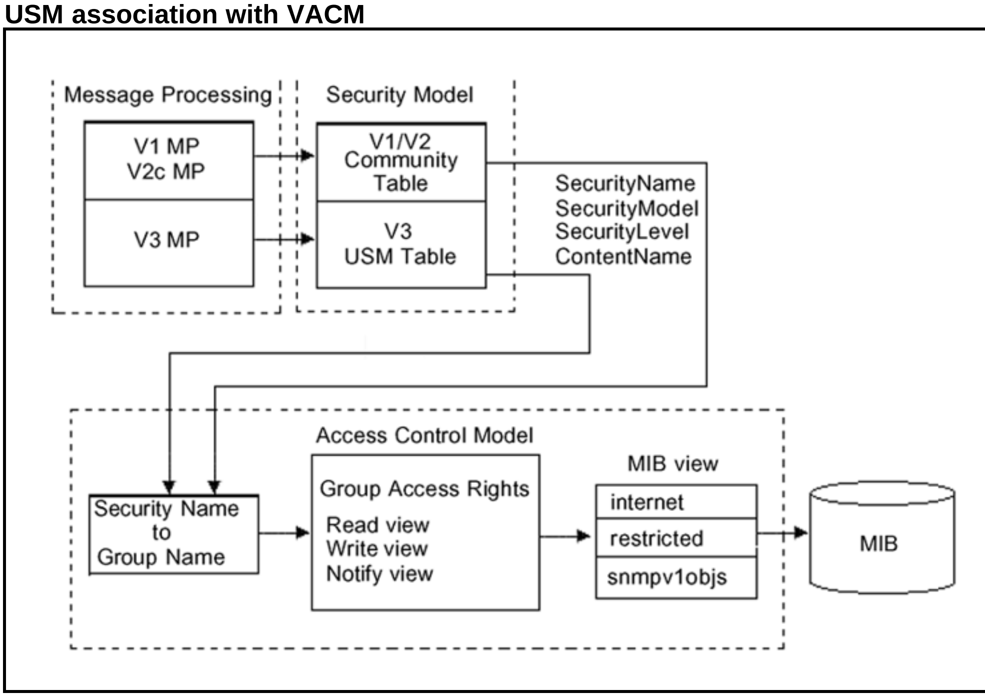
In a user-based security model (USM) system, the security model employs a defined set of user identities for any authorized user on an SNMP engine. The users with authorization on one SNMP engine must have authorization on any SNMP engine with which the original SNMP engine communicates.

The USM security model provides the following levels of communication:

- NoAuthNoPriv: communication without authentication and privacy
- AuthNoPriv: communication with authentication and without privacy
- AuthPriv: communication with authentication and privacy

Figure 7 "USM association with VACM" (page 61) shows the relationship between USM and VACM.

Figure 7
USM association with VACM



View-based Access Control Model

The VACM provides groups access, group security levels, and context based on a predefined subset of management information base (MIB) objects. These MIB objects define a set of managed objects and instances.

VACM is the standard access control mechanism for SNMPv3 and provides:

- authorization service to control access to MIB objects at the power distribution unit (PDU) level
- alternative access control subsystems

The access is based on principal, security level, MIB context, object instance, and type of access requested (read/write). VACM MIB defines the policy and permits remote management.

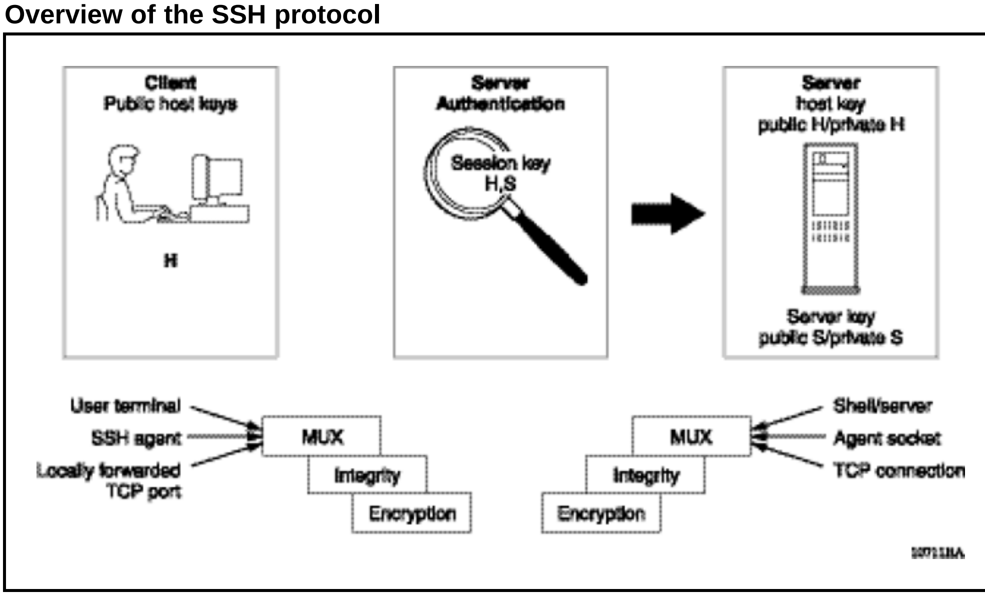
Secure Shell

Secure Shell (SSH) is a client/server protocol that specifies how to conduct secure communications over a network.

SSH supports a variety of the available public and private key encryption schemes. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key encrypts all traffic between the client and the server.

Figure 8 "Overview of the SSH protocol" (page 62) gives an overview of the SSH protocol.

Figure 8
Overview of the SSH protocol



By using a combination of host, server, and session keys, the SSH protocol provides strong authentication and secure communication over an unsecure network, offering protection from the following security risks:

- IP spoofing
- IP source routing
- DNS spoofing
- man-in-the-middle and TCP hijacking attacks
- eavesdropping and password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted, and the connection cannot be hijacked.

The secure channel of communication provided by SSH does not provide protection against break-in attempts or denial-of-service (DoS) attacks.

The SSH protocol supports the following security features:

- Authentication: identifies the SSH client. During logon, the SSH client is queried for a digital proof of identity.

  Supported authentications are RSA (SSH-1), DSA (SSH-2), and passwords (both SSH-1 and SSH-2).
- Encryption: scrambles data rendering it unintelligible except to the receiver.

  Supported encryptions are AES and 3DES.
- Integrity: guarantees that the data is transmitted from the sender to the receiver without alteration. If any third party captures and modifies the traffic, the SSH server detects this alteration.

ATTENTION
Currently, 3DES is the only supported encryption algorithm for the Nortel Ethernet Routing Switch 8600. Proper functioning requires the 3DES encryption image.

The implementation of the SSH server on the Nortel Ethernet Routing Switch 8600 enables the SSH client to securely connect to the Nortel Ethernet Routing Switch 8600 and supports commercially available SSH clients.

ATTENTION
You must use the CLI to initially configure SSH. You can use Enterprise Device Manager to change the SSH configuration parameters. Nortel recommends that you use the console port to configure the SSH parameters.

SSH version 2 (SSH-2)

SSH protocol, version 2 (SSH-2) is a complete upgrade of the SSH-1 protocol. While SSH-1 contains multiple functions in a single protocol, SSH-2 functions are divided among the following three protocols:

- SSH transport layer (SSH-TRANS)

  The SSH transport layer manages the server authentication and provides the initial connection between the client and the server. When a connection is established, the transport layer provides a secure, full-duplex connection between the client and the server.

- SSH authentication protocol (SSH-AUTH)

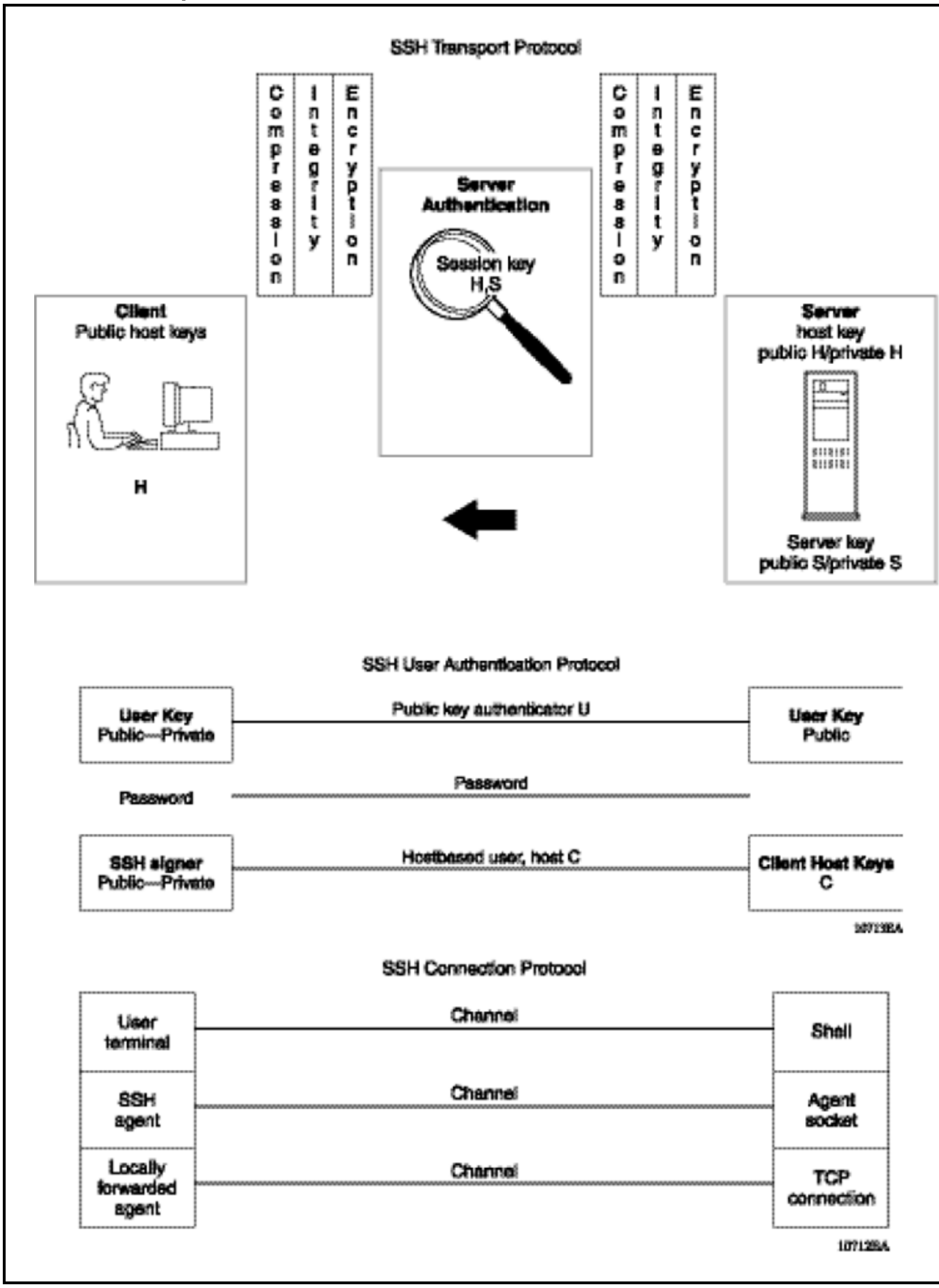
  The SSH authentication protocol runs on top of the SSH transport layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods: public key, host-based, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH connection protocol (SSH-CONN)

  The SSH connection protocol runs on top of the SSH transport layer and authentication protocols. SSH-CONN provides interactive logon sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These services multiplex into the single encrypted tunnel provided by the SSH transport layer.

Figure 9 "SSH version 2 protocols" (page 65) shows the SSH-2 protocols.

Figure 9
SSH version 2 protocols



The modular approach of SSH-2 improves on the security, performance, and portability of the SSH-1 protocol.

> **ATTENTION**
> The SSH-1 and SSH-2 protocols are not compatible. While the SSH implementation on the Nortel Ethernet Routing Switch 8600 supports both versions of SSH, Nortel recommends the more secure version, the SSH-2 protocol.

Access policy extensions

The access policy feature controls the admittance of the incoming connections though various applications such as HTTP, SNMPv3, Telnet and SSH. The access is controlled at two levels:

- the source IP address (IPv4 or IPv6)
- the logon access level, that is, read-only (ro), read-write (rw), read-write-all (rwa), and, in the case of SNMP, extra configuration for groups

The first check, performed at the PDU level, determines if an action is allowed based on the access configuration.

For SNMP, version 3 provides a group option in the access policy. See "SNMP version 3" (page 59).

Any modifications in the access policy entry can affect the existing application session.

The following modifications result in changes to established TCP-based connections:

- Disallowing connections from the host or network for the entry in the access policy table
- Deleting an entry
- Reducing the access level; that is; ro/rw/rwa.

  This results in a session logoff to clear the cached entry and forces the user to log on again. The new logon information is verified according to the configuration.
- Increasing the access level

Multicast link discovery

IPv6 routers use multicast link discovery (MLD) to discover

- the presence of multicast listeners on directly attached links
- multicast addresses required by neighboring nodes

MLD is an asymmetric protocol. It specifies separate behaviors for multicast address listeners (that is, hosts or routers that listen to multicast packets) and multicast routers. Each multicast router learns, for each directly attached link, which multicast addresses and which sources have listeners on that link. The information that MLD gathers is provided to the multicast routing protocols that the router uses. This information ensures that multicast packets arrive at all links where listeners require such packets.

A multicast router can itself be a listener of one or more multicast addresses. That is, the router performs both the multicast router role and the multicast address listener part of the protocol. The router collects the multicast listener information needed by the multicast routing protocol and informs itself and other neighboring multicast routers of the listening state.

MLD versions 1 and 2

The purpose of the MLD protocol in the IPv6 multicast architecture is to allow an IPv6 router to discover the presence of multicast listeners on directly attached links and to discover which multicast addresses are of interest to neighboring nodes. MLD is the direct IPv6 replacement for the IGMP protocol used in IPv4. The MLD implementation described in this document is based on the MLDv2 standard, which is a backward-compatible update to the MLDv1 standard.

QoS and IPv6 filters

Use filtering to block unwanted traffic from entering a switch or to prioritize required traffic. Filtering is critical to efficient bandwidth management and network protection. You determine which packets receive special handling based on information in the packet headers.

Traffic filters instruct an interface to selectively handle specified traffic. Using traffic filters, you can reduce network congestion and control access to network resources by blocking, forwarding, or prioritizing specified traffic on an interface. You can apply multiple traffic filters to a single interface.

If you configure IPv6 attributes for an access control template (ACT), you must configure an access control list (ACL) of type IPv6. If you configure only Ethernet attributes for an ACT, you can configure two ACLs: one of type IPv4 and one of type IPv6.

For additional information about QoS and IP filters, see *Nortel Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for R and RS Modules* (NN46205-507).

License information

The IPv6 feature requires an Advanced License. For more information about licenses, see *Administration* (NN46205-605).

IPv6 DHCP Relay

The Dynamic Host Configuration Protocol (DHCP) for IPv6 (RFC 3315) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCP supports automatic allocation of reusable network addresses and of additional configuration parameters.

To request the assignment of one or more IPv6 addresses, a client first locates a DHCP server and then requests the assignment of addresses and other configuration information from the server. The client sends a Solicit message to the All_DHCP_Relay_Agents_and_Servers (FF02::1:2) multicast address to find available DHCP servers. Any server that can meet the client's requirements responds with an Advertise message. The client then chooses one of the servers and sends a Request message to the server asking for confirmed assignment of addresses and other configuration information. The server responds with a Reply message that contains the confirmed addresses and configuration.

IPv6 DHCP clients use link-local addresses to send and receive DHCP messages. To allow a DHCP client to send a message to a DHCP server that is not attached to the same link, you must configure a DHCP relay agent on the client's link to relay messages between the client and server. The operation of the relay agent is transparent to the client.

A relay agent relays messages from clients and messages from other relay agents.

Remote ID

IPv6 DHCP Relay supports the Remote ID parameter (RFC 4649). When you enable Remote ID on the switch, the relay agent adds information about the client to DHCPv6 messages before relaying the messages to the DHCP server. The server can use the supplied information in the process of assigning the addresses, delegated prefixes and configuration parameters that the client is to receive.

The remote ID option contains two fields:

- enterprise-number
- remote-id

On the Ethernet Routing Switch 8600, the enterprise-number (vendor ID) used is 1584 and the remote-id field is filled with the unique MAC address of the client.

IPv6 VRRP

For IPv6 hosts on a LAN to learn about one or more default routers, IPv6-enabled routers send Router Advertisements using the IPv6 Neighbor Discovery (ND) protocol. The routers multicast these Router Advertisements every few minutes.

The ND protocol includes a mechanism called Neighbor Unreachability Detection to detect the failure of a neighbor node (router or host) or the failure of the forwarding path to a neighbor. Nodes can monitor the health of a forwarding path by sending unicast ND Neighbor Solicitation messages to the neighbor node. To reduce traffic, nodes only send Neighbor Solicitations to neighbors to which they are actively sending traffic and only after the node receives no positive indication that the neighbors are up for a period of time. Using the default ND parameters, it takes a host approximately 38 seconds to learn that a router is unreachable before it switches to another default router. This delay is very noticeable to users and causes some transport protocol implementations to timeout.

While you can decrease the ND unreachability detection period by modifying the ND parameters, the current lower limit that can be achieved is five seconds, with the added downside of significantly increasing ND traffic. This is especially so when there are many hosts all trying to determine the reachability of one of more routers.

To provide fast failover of a default router for IPv6 LAN hosts, the Ethernet Routing Switch 8600 supports the Virtual Router Redundancy Protocol (VRRP v3) for IPv6 (defined in draft-ietf-vrrp-ipv6-spec-08.txt).

VRRPv3 for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol. With VRRPv3, a backup router can take over for a failed default router in approximately three seconds (using VRRPv3 default parameters). This is accomplished without any interaction with the hosts and with a minimum amount of VRRPv3 traffic.

The operation of Nortel's IPv6 VRRP implementation is similar to the existing IPv4 VRRP operation, including support for hold-down timer, critical IP, fast advertisements, and backup master. With backup master enabled, the backup switch routes all traffic according to its routing table. It does not Layer 2-switch the traffic to the VRRP master.

New to the IPv6 implementation of VRRP, you must specify a link-local address to associate with the virtual router. Optionally, you can also assign global unicast IPv6 addresses to associate with the virtual router. Network prefixes for the virtual router are derived from the global IPv6 addresses assigned to the virtual router.

With the current implementation of VRRP, one active master switch exists for each IPv6 network prefix. All other VRRP interfaces in a network are in backup mode.

On an Ethernet Routing Switch 8600, you cannot directly check or set the virtual IP address on the standby CPU module. To check or set the virtual IP address on the standby CPU, you must configure the virtual IP address on the master CPU, save it to the config.cfg file, and then copy that file to the standby CPU module.

VRRPv3 operation

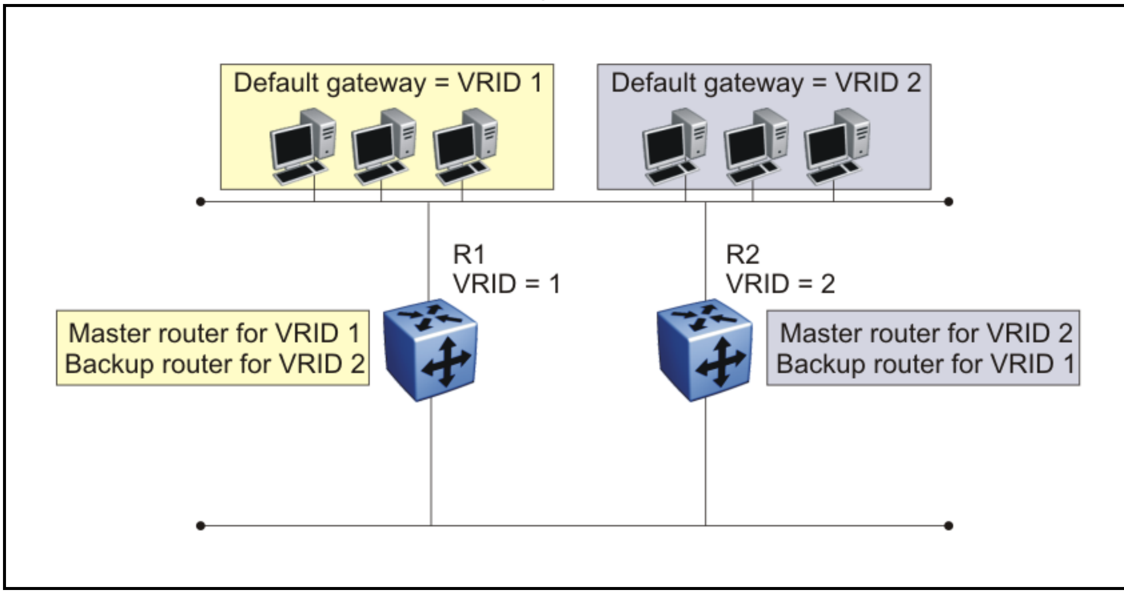
VRRP makes use of a virtual IP address (transparent to users) shared between two or more routers connecting the common network prefix to the enterprise network. With the virtual IP address as the default gateway on end hosts, VRRP provides dynamic default gateway redundancy in the event of failover.

VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP addresses associated with a virtual router is called the Master router. The Master router forwards packets sent to the virtual router IP addresses. The election process provides dynamic failover in the forwarding responsibility if the Master becomes unavailable.

In the following figure, the first three hosts install a default route to the R1 (virtual router 1) IP address and the other three hosts install a default route to the R2 (virtual router 2) IP address. For VRID 1, R1 is the master and R2 is the backup. For VRID 2, R2 is the master and R1 is the backup.

This configuration not only shares the load of the outgoing traffic, but it also provides full redundancy. If either router fails, the other router assumes responsibility for both addresses.

Figure 10
Virtual Router Redundancy Protocol configuration



When a VRRP router is initialized, if it is the IP address owner, it asserts itself as the master router with a priority of 255 and it sends a VRRP advertisement. The VRRP router also sends unsolicited ND Neighbor Advertisements and ND Router Advertisements containing the virtual router MAC address for each IP address associated with the virtual router. The VRRP router then transitions to the controlling state.

In the controlling state, the VRRP router functions as the forwarding router for the IP addresses associated with the virtual router. It responds to ND Neighbor Solicitation and ND Router Solicitation messages for these IP addresses, forwards packets with a destination MAC address equal to the virtual router MAC address, and accepts only packets addressed to IP addresses associated with the virtual router if it is the IP address owner.

If the VRRP router is initialized and the priority is not 255, the router transitions to the backup state to ensure that all Layer 2 switches in the down path relearn the new origin of the VRRP MAC addresses.

In the backup state, a VRRP router monitors the availability and state of the master router. It does not respond to ND Neighbor Solicitation and ND Router Solicitation messages for virtual router IP addresses and discards packets with a MAC address equal to the virtual router MAC address. It does not accept packets addressed to IP addresses associated with the virtual router. If a shutdown occurs, it transitions back to the initialize state. If the master router goes down, the backup router sends the VRRP advertisement and unsolicited ND Neighbor Advertisements and ND Router Advertisements described in the preceding paragraphs and transitions to the controlling state.

VRRP advertisements and master router failover

When a VRRP router is initialized, if it is the IP address owner, its priority is 255 and it sends a VRRP advertisement. The master router then continues to send advertisement messages at the advertisement interval period.

The other VRRP routers transition to the backup state in the following situations:

- if the priority in the received advertisement is greater than the local priority
- if the priority in the received advertisement is the same as the local priority and the primary IP address of the sender is greater than the local primary IP address

The backup routers use the advertisements from the master router as a keepalive to monitor the health of the master router. If the backup router does not receive an advertisement during the master downtime interval, calculated as 3 * advertisement interval, then the master router is declared down.

If a shutdown occurs, the master router sends a VRRP advertisement with a priority of 0 and transitions to the initialize state.

The priority value 0 indicates that the master router has stopped participating in VRRP. This triggers the backup router to transition to the master state without waiting for the current master to time out.

VRRP terms

The following terms are specific to VRRP:

- VRRP router—a router running the VRRP protocol
- Virtual router—an abstract object acting as the default router for one or more hosts, consisting of a virtual router ID and a set of addresses
- IP address owner—the VRRP router that has virtual router IP addresses as real interface addresses (the router that responds to packets sent to this IP address.)
- Primary IP address—an IP address selected from the real addresses and used as the source address of packets sent from the router interface (The virtual router master sends VRRP advertisements using this IP address as the source.)

- Virtual router master—the router assuming responsibility for forwarding packets sent to the IP address associated with the virtual router and answering ARP requests for these IP addresses
- Virtual router backup—the virtual router that becomes the master router if the current master router fails

Scaling

The Ethernet Routing Switch 8600 supports 255 VRRP interfaces for each switch.

Critical IP address

Within a VRRP VLAN, one link can go down while the remaining links in the VLAN remain operational. Because the VRRP VLAN continues to function, a virtual router associated with that VLAN does not register a master router failure.

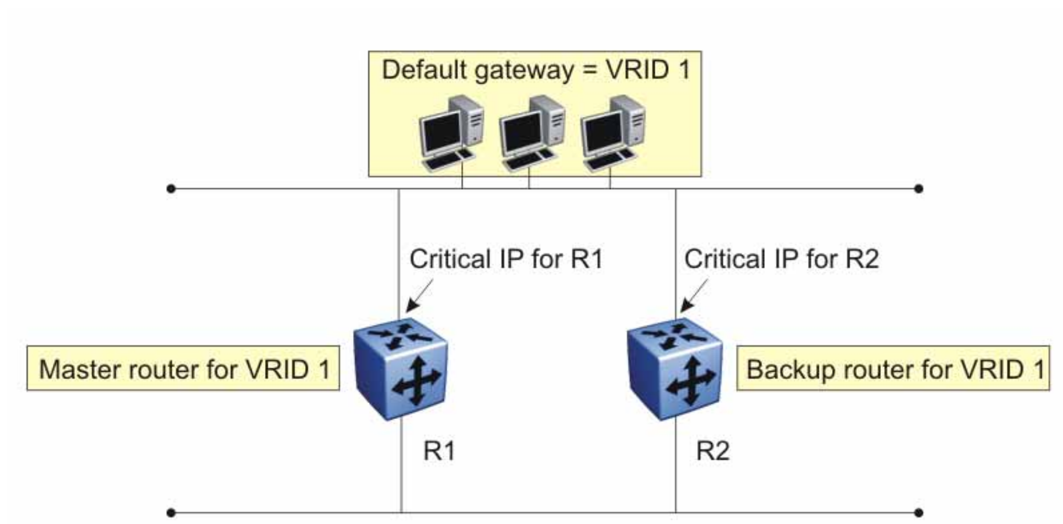
As a result, if the local router IP interface connecting the virtual router to the external network fails, this does not automatically trigger a master router failover.

The critical IP address resolves this issue. If the critical IP address fails, it triggers a failover of the master router.

You can specify the local router IP interface uplink from the VRRP router to the network as the critical IP address. This ensures that, if the local uplink interface fails, VRRP initiates a master router failover to one of the backup routers.

In the following figure, the local network uplink interface on R1 is shown as the critical IP address for R1. As well, the similar network uplink is shown as the critical IP address for R2. R2 also requires a critical IP address for cases in which it assumes the role of the master router.

Figure 11
VRRP with critical IP



The critical address can be any one of the global unicast IPv6 addresses assigned to any local IPv6 interfaces.

Hold-down timer

The hold-down timer is a proprietary Nortel enhancement to VRRP. When a master router transitions to a backup router after a critical IP failure, one of the backup routers is elected as the master router. When the critical IP of the original master router (now a backup router) is restored, that router remains in the backup state for a period which can be specified by the hold-down timer. The hold-down timer allows the master router enough time to detect and update the dynamic routes. The timer delays the preemption of the master over the backup, when the master becomes available. If the hold-timer is configured to 0, it becomes the master router immediately. Otherwise, it transitions to the master state only after the hold-down timer times out.

Note that the hold-down timer is not employed during failovers caused by the VRRP router priority change. It is only for failovers caused by a critical IP failure.

In addition, you can manually force the preemption of the master over the backup before the delay timer expires.

Nortel recommends that you set all of your routers to the identical number of seconds for the hold-down timer. The hold-down timer has a default value of 0 seconds.

Accept mode

With IPv6 VRRP, the accept mode controls whether a master router accepts packets addressed to the address owner’s IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.

This parameter is not applicable for VRRP over IPv4.

VRRP backup master with triangular SMLT

The standard implementation of VRRP supports only one active master switch for each IPv6 network prefix. All other VRRP interfaces in a network are in backup mode.

A deficiency occurs when VRRP-enabled switches use Split MultiLink Trunking (SMLT). If VRRP switches are aggregated into two Split MultiLink Trunk switches, the end host traffic is load-shared on all uplinks to the aggregation switches (based on the Multilink Trunk [MLT] traffic distribution algorithm).

However, VRRP usually has only one active routing interface enabled. All other VRRP routers are in backup mode. Therefore, all traffic that reaches the backup VRRP router is forwarded over the interswitch trunk (IST) link toward the master VRRP router. In this case, the IST link potentially does not have enough bandwidth to carry all the aggregated traffic.

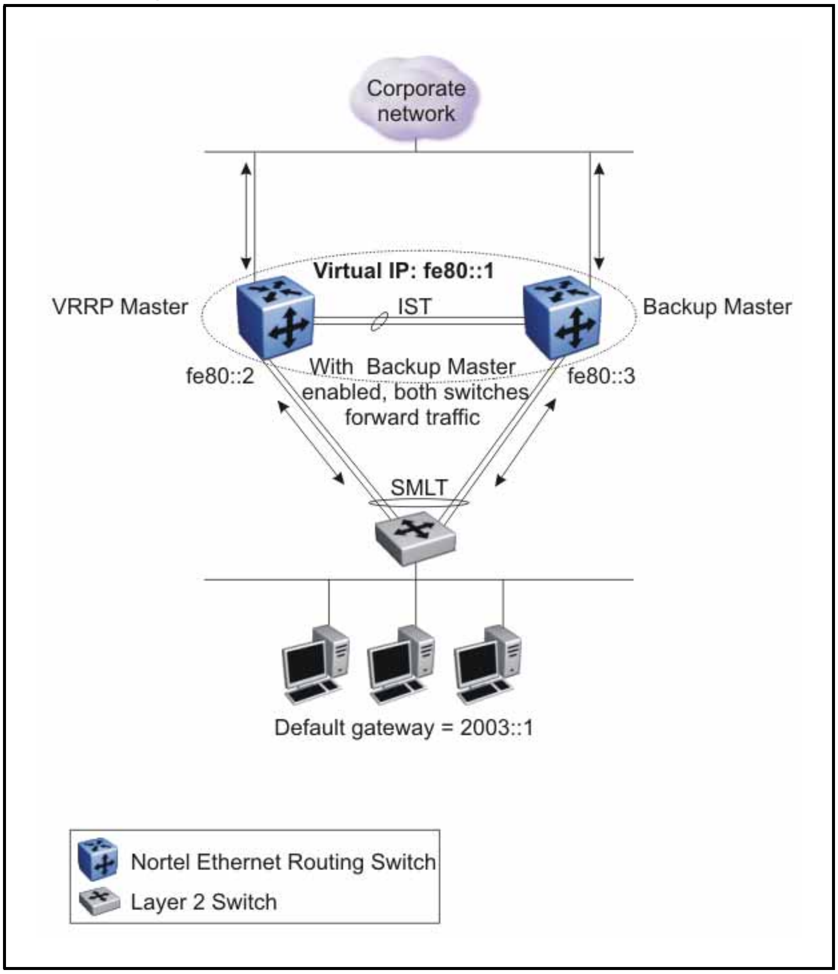
To resolve this issue, assign the backup router as the backup master router. The backup master router can actively load-share the routing traffic with a master router.

Because there is an exchange of MAC address tables between the two VRRP peer nodes, the VRRP backup master can forward traffic directly on behalf of the master router. The switch in the backup master state routes all traffic received on the backup master IP interface according to its routing table. It does not Layer 2-switch the traffic to the master router.

As a result, when the backup master router is enabled with SMLT, the incoming host traffic is forwarded over the SMLT links as usual.

The following figure shows a sample VRRP configuration with SMLT. Because the backup router is configured as the backup master, routing traffic is load-shared between the two devices.

Figure 12
VRRP configuration with SMLT



The backup master feature only supports the triangular SMLT topology.

> **ATTENTION**
> Do not use VRRP backup master and critical IP at the same time. Use one or the other.

VRRP fast advertisment interval

With the current implementation of VRRP, you can set the advertisement time interval (in seconds) between sending advertisement messages. This permits faster network convergence with standardized VRRP failover. However, losing connections to servers for more than a second can result in missing critical failures. Customer network uptime in many cases requires faster network convergence, which means network problems must be detected within hundreds of milliseconds.

To meet these requirements, Nortel provides the fast advertisement interval.

The fast advertisement interval is similar to the advertisement interval parameter except for the unit of measure and the range. The fast advertisement interval is expressed in milliseconds and the range is from 200 to 1000 milliseconds. (This unit of measure must be in multiples of 200 milliseconds.)

To configure fast advertisement, you must specify a fast advertisement interval and explicitly enable the fast advertisement feature. When the fast advertisement feature is enabled, the fast advertisement interval is used instead of the advertisement interval.

When the fast advertisement feature is enabled, VRRP can only communicate with other Ethernet Routing Switches with the same settings.

VRRP considerations with IPv6

In an IPv6 VRRP network with SMLT, if you delete the VRRP peers on the aggregation switches, the VRRP addresses on the access switch are not immediately removed from the IPv6 neighbor table. Instead, the access switch initially displays the IPv6 neighbor states as Incomplete.

In accordance with the ND RFC, neighbor addresses are aged out 30 minutes after the traffic is stopped from a neighbor. In this case, the access switch removes the virtual addresses 30 minutes after the VRRP virtual routers are deleted from the two aggregation switches.

IPv6 VRRP and ICMP redirects

In IPv6 networks, do not enable ICMP redirects on VRRP VLANs. If you enable this option (using the **`config ipv6 icmp redirect-msg`** command), VRRP cannot function. The option is disabled by default.

IPv6 RSMLT

In many cases, core network convergence time depends on the length of time a routing protocol requires to successfully converge. Depending on the specific routing protocol, this convergence time can cause network interruptions ranging from seconds to minutes.

Nortel Routed Split MultiLink Trunking (RSMLT) permits rapid failover for core topologies by providing an active-active router concept to core Split MultiLink Trunking (SMLT) networks. In the event of core router failures, RSMLT manages packet forwarding, thus minimizing dropped packets during the routing protocol convergence.

While Nortel’s Routed Split Multilink Trunk (RSMLT) functionality originally provided sub-second failover for IPv4 forwarding only, the Ethernet Routing Switch 8600 extends RSMLT functionality to IPv6. The overall model for IPv6 RSMLT is essentially identical to that of IPv4 RSMLT. In short, RSMLT peers exchange their IPv6 configuration and track each other's state by means of IST messages. An RSMLT node always performs IPv6 forwarding on the IPv6 packets destined to the peer's MAC addresses. When an RSMLT node detects that its RSMLT peer is down, the node also begins terminating IPv6 traffic destined to the peer's IPv6 addresses.

With RSMLT enabled, an SMLT switch performs IP forwarding on behalf of its SMLT peer – thus preventing IP traffic from being sent over the IST.

IPv6 RSMLT supports the full set of topologies and features supported by IPv4 RSMLT, including SMLT triangles, squares, and SMLT full-mesh topologies, with routing enabled on the core VLANs.

With IPv6, you must configure the RSMLT peers using the same set of IPv6 prefixes.

Supported routing protocols include the following:

- IPv6 Static Routes
- OSPFv3

IPv4 IST with IPv6 RSMLT

Ethernet Routing Switch 8600 does not support the configuration of an IST over IPv6. IST is supported over IPv4 only.

Enabling RSMLT for IPv4 and IPv6

To enable IPv6 RSMLT, you must use the same configuration commands provided for IPv4 RSMLT. As none of the RSMLT configuration parameters depend on IP-specific information, the configuration commands remain unchanged.

RSMLT configuration is a property of a VLAN. If you enable RSMLT on a VLAN and IPv4 and IPv6 are enabled on the VLAN, then the RSMLT configuration is in effect for both protocols. No additional or separate configuration parameters are available for configuring IPv6 RSMLT.

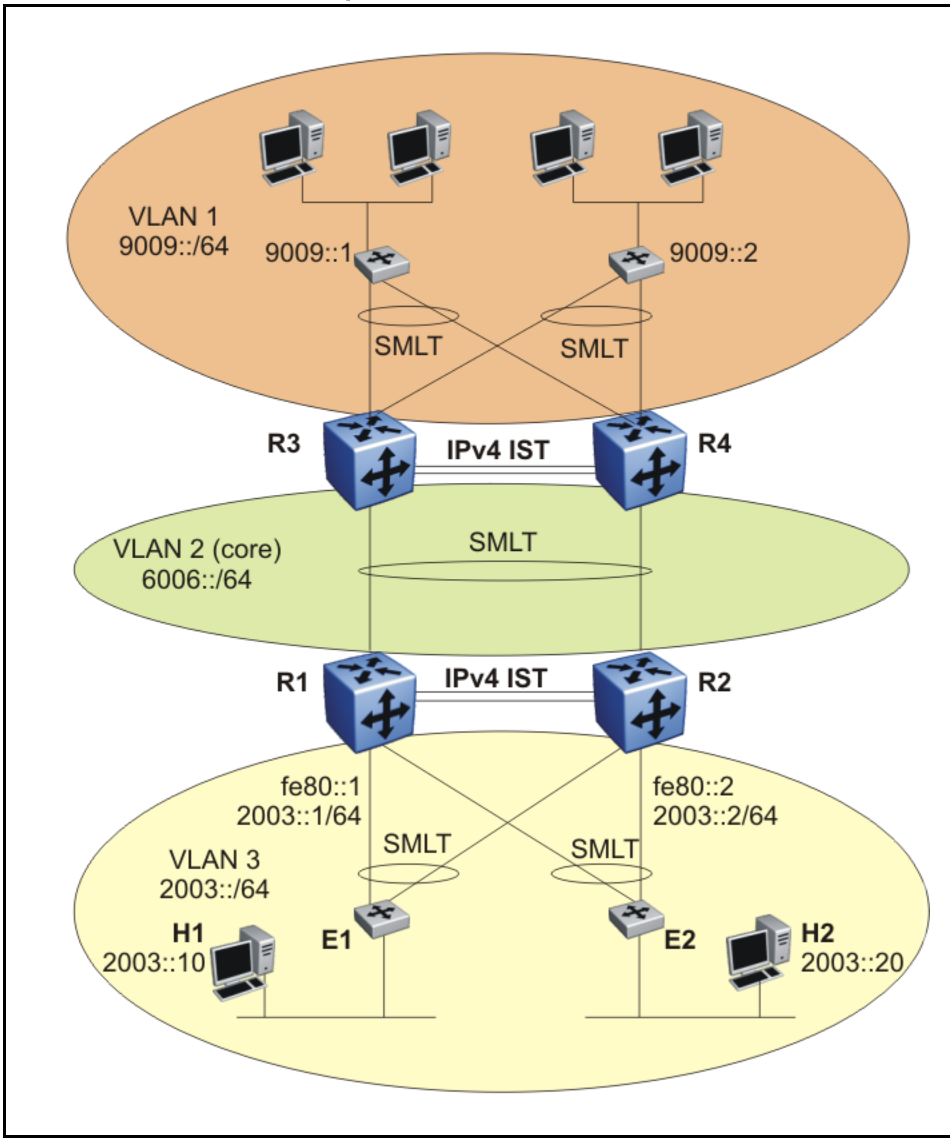
It is not possible to selectively enable or disable RSMLT for IPv4 only or IPv6 only.

Example network

The following figure shows a sample IPv6 RSMLT topology. It shows a typical redundant network example with user aggregation, core, and server access layers. To minimize the creation of many IPv6 prefixes, one VLAN (VLAN 1, IP prefix A) spans all wiring closets.

RSMLT provides the loop-free topology. The aggregation layer switches are configured with routing enabled and provide active-active default gateway functionality through RSMLT.

Figure 13
IPv6 RSMLT network example



In the VLAN 3 portion of the network shown in the preceding figure, routers R1 and R2 provide RSMLT-enabled IPv6 service to hosts H1 and H2. Router R1 can be configured as the default IPv6 router for H1 and R2 can be the default router for H2. R1 is configured with the link-local address of fe80::1, the global unicast address 2003::1, and the routing prefix of 2003::/64 (as a shorthand, the last two items are referred to as 2003::1/64). R2 is configured with fe80::2 and 2003::2/64.

Host H1 sends its IPv6 traffic destined to VLAN 1 to R1's MAC address (after resolving the default router address fe80::1 to R1's MAC). H2 sends its traffic to R2's MAC. When an IPv6 packet destined to R1's MAC address is received at R2 on its SMLT links (which is the expected MLT behavior), R2 performs IPv6 forwarding on the packet and does not bridge it over the IST. The same behavior occurs on R1.

At startup, R1 and R2 use the IST link to exchange full configuration information including MAC address for the IPv6 interfaces residing on SMLT VLAN 3.

When R2 detects that the RSMLT in R1 transitions to the DOWN state (for example, if R1 itself is down, or its SMLT links are down, or the IST link is down) R2 takes over IPv6 termination and IPv6 Neighbor Discovery functionality on behalf or R1's IPv6 SMLT interface. Specifically:

- When the above event is detected, R2 transmits an unsolicited IPv6 Neighbor Advertisement for each IPv6 address configured on R1's SMLT link using R1's MAC address (fe80::1 and 2003::1 in this example).
- R2 also transmits an unsolicited Router Advertisement for each of R1's routing prefixes (unless R1's prefixes are configured as "not advertised").
- R2 responds to Neighbor Solicitations and (if configuration allows) Router Advertisements on behalf of R1
- R2 terminates IPv6 traffic (such as pings) destined to R1's SMLT IPv6 addresses

When R1's RSMLT transitions back into the UP state and the HoldDown timer expires it resumes IPv6 forwarding and R2 ceases to terminate IPv6 traffic on R1's behalf.

Note that IPv6 allows a rich set of configuration options for advertising IPv6 routing prefixes (equivalent to IPv4 subnets) and configuring hosts on a link. A prefix can be configured to be or not to be advertised, to carry various flags or lifetime. These parameters affect how hosts can (auto)configure their IPv6 addresses and select their default routers. Most relevant from the RSMLT perspective is that an RSMLT node fully impersonates its peer's IPv6 configuration and behavior on the SMLT link – whatever its configuration happens to be. The above network example illustrates one of the many possible deployment schemes for IPv6 routers and hosts on a VLAN.

RSMLT provides both router failover and link failover. For example, if the Split MultiLink Trunk link between R2 and R4 is broken, the traffic fails over to R1 as well.

Router R1 recovery

After R1 reboots after a failure, it becomes active as a VLAN bridge first. Packets destined to R1 are switched, using the bridging forwarding table, to R2. R1 operates as a VLAN bridge for a period defined by the hold-down timer.

After the hold-down time expires and the routing tables converge, R1 starts routing packets for itself and also for R2. Therefore, it does not matter which of the two routers is used as the next hop from R3 and R4 to reach IPv6 prefix 2003::/64.

When an IPV6 RSMLT peer recovers, the peer installs a temporary default route in the IPv6 routing table to point all the IPv6 traffic to the IST peer IP address for the hold down time. (This is the same behavior as in IPv4 RSMLT.)

Hold-up timer

When both RSMLT peers are active, both peers forward traffic for each other. When a router detects that its peer is down, it begins terminating IPv6 traffic destined to the peer's IPv6 addresses (including, for example, responding to pings and router solicitations). The router continues to forward and terminate traffic for its peer for a duration defined by the hold-up timer. If the peer is not restored and the hold-up timer expires, the router stops forwarding and terminating traffic for the peer.

You can set the hold-up timer (in the preceding example, the amount of time R2 routes for R1 in a failure) for a time period greater than the routing protocol convergence. You can also set it as infinite (that is, the members of the pair always route for each other).

Nortel recommends that you use an infinite (9999) hold-up timer value for applications that use RSMLT at the edge instead of VRRP.

RSMLT or VRRP

For VLAN 1, VRRP with a backup master can provide the same functionality as RSMLT, as long as no additional router is connected to IPv6 prefix 2003::/64.

RSMLT provides superior router redundancy in core networks (IPv6 prefix B), where OSPFv3 is used for the routing protocol. Routers R1 and R2 provide router backup for each other, not only for the edge IP Prefix 2003::/64, but also for the core IPv6 prefix B. Similarly routers R3 and R4 provide router redundancy for IPv6 prefix C and also for core IPv6 prefix B.

Nortel does not recommend that you both VRRP and RSMLT on the same VLAN. Use one or the other.

Coexistence with IPv4 RSMLT

The IPv6 RSMLT feature introduces no changes to the existing IPv4 RSMLT state machine including RSMLT configuration, definitions of events, logic of state transitions, or timer operations. A single instance of state and configuration parameter set controls both IPv4 and IPv6 RSMLT logic. With the introduction of this feature, RSMLT is best thought of as a property of the VLAN layer as opposed to the IP (v4 or v6) layer above it. RSMLT configuration and states affect IPv4 and IPv6 operation simultaneously.

For a given SMLT VLAN RSMLT is supported for any of the following scenarios:

- IPv4 Only: IPv4 is configured on the VLAN and IPv6 is not. RSMLT operation and logic remains unchanged from the current implementation.
- IPv6 Only: IPv6 is configured on the VLAN and IPv4 is not. IPv6 RSMLT operation follows that of IPv4 as described in this document.
- IPv4 and IPv6: Both IPv4 and IPv6 are configured on the VLAN. IPv4 RSMLT operation and logic remains unchanged from the current implementation and unaffected by IPv6. IPv6 operation follows that of IPv4 as described in this document.

RSMLT network design and configuration

Because RSMLT is based on SMLT, all SMLT configuration rules apply. In addition, RSMLT is enabled on the SMLT aggregation switches for each VLAN. The VLAN must be a member of SMLT links and the IST trunk. For more information about configuring SMLT in a Layer 2 environment, see *Nortel Ethernet Routing Switch 8600 Configuration – Link Aggregation, MLT and SMLT* (NN46205-518).

The VLAN also must be routable (IP address configured) and an Interior Routing Protocol (IGP) such as OSPFv3 must be configured on all four routers, although it is independent of RSMLT. You can use any supported routing protocol, even static routes, with RSMLT.

RSMLT pair switches provide backup for each other. As long as one of the two routers of an IST pair is active, traffic forwarding is available for both next hops R1/R2 and R3/R4.

> **ATTENTION**
> Do not enable ICMP redirects on RSMLT VLANs. If you enable this option (using the **`config ipv6 icmp redirect-msg`** command), RSMLT cannot function. The option is disabled by default.

RSMLT-edge

RSMLT-edge stores the RSMLT peer MAC/IPv6 address pair in its local configuration file and restores the configuration if the peer does not restore after a simultaneous reboot of both RSMLT-peer switches.

The RSMLT-edge feature simply adds an enhancement whereby the peer's MAC (for the IP on the VLAN) gets committed to the config.cfg file after a save config; that way if you power off both switches, and then power up only 1 of them, that single switch can still take ownership of its peer's IP on that VLAN even if it has not yet even seen that peer switch since it booted; this is necessary as you might have configured the peer (the switch which is still down) IP as the default gateway in end stations.

If you enable RSMLT-edge, you must also ensure that the hold-up timer for RSMLT on those edge VLANs is set to infinity (9999). This is to ensure that if one cluster switch fails, the remaining cluster switch maintains ownership of its failed peer IPs indefinitely.

It does not matter if that VLAN is tagged over SMLT links, single attached links, or more SMLT links; what is possible with VRRP, you can do with RSMLT-edge.

Be sure to save the configuration after you configure RSMLT-edge. This step is required in order the save the peer MAC address.

RSMLT considerations with OSPF

If you run OSPF with RSMLT in a square or mesh, and a node loses the IST connection to its peer, OSPF adjacencies can be lost. In this scenario, OSPF is not guaranteed to be in a consistent state.

IPv6 routing configuration

Configure IPv6 routing to take advantage of the additional benefits over IPv4 routing such as an increased number of possible addresses in your network.

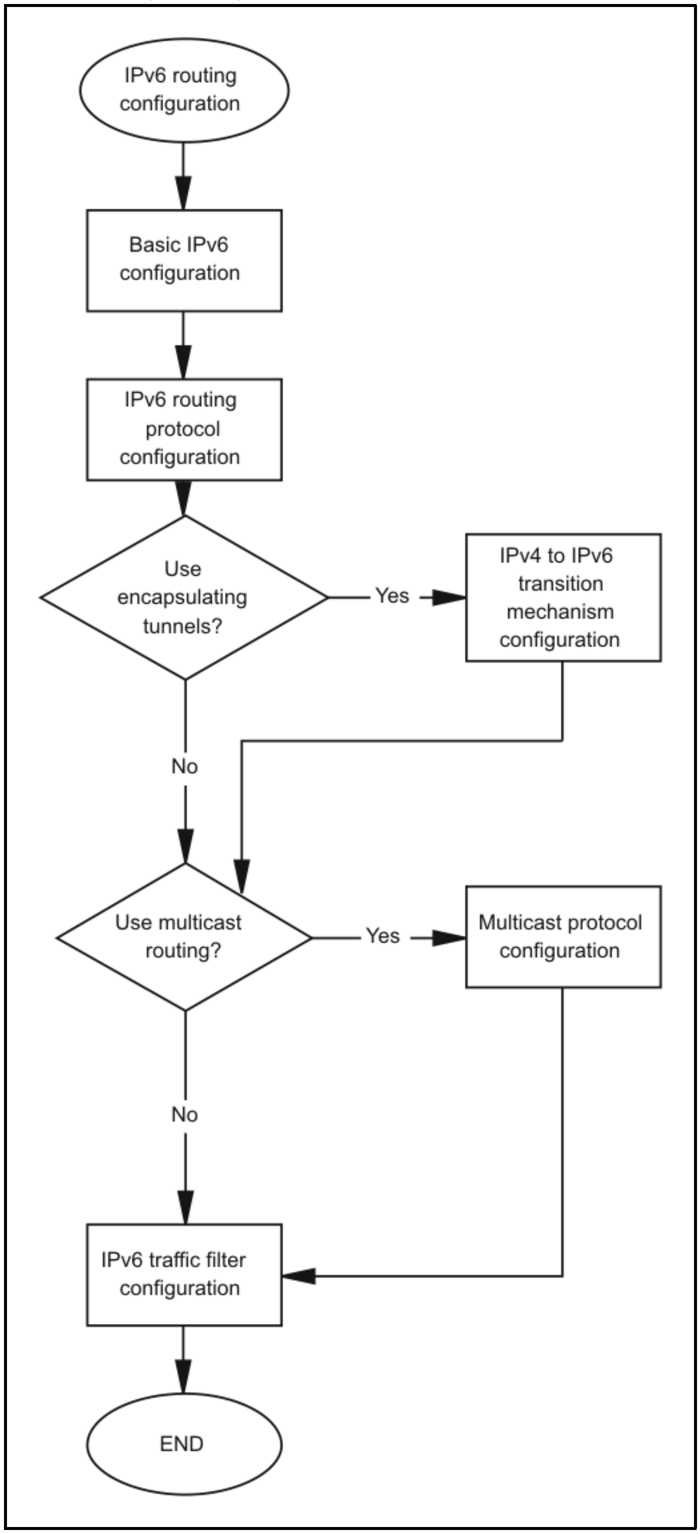
Prerequisites to IPv6 routing configuration

- You require R or RS modules for hardware forwarding.
- You must run Nortel Ethernet Routing Switch 8600 Release 4.1 software or later for IPv6 hardware-based forwarding.
- Assign an IPv6 address to the Ethernet SF/CPU port.

IPv6 routing configuration tasks

This work flow shows you the sequence of tasks you perform to configure IPv6 routing on the Nortel Ethernet Routing Switch 8600. To link to any task, go to “IPv6 routing configuration navigation” (page 87).

Figure 14
IPv6 routing configuration tasks



IPv6 routing configuration navigation

Basic IPv6 configuration using Enterprise Device Manager

This chapter describes Enterprise Device Manager procedures for enabling and configuring IPv6 routing functions on the Ethernet Routing Switch 8600. For conceptual information about Layer 3 routing functions, see "IPv6 routing fundamentals" (page 25).

Prerequisites to basic IPv6 configuration

- Hardware forwarding requires R or RS modules.
- An enterprise enhanced SF/CPU daughter card (SuperMezz) must be installed on your Ethernet Routing Switch 8600.
- At least one 8692SF/CPU module must be installed on your Ethernet Routing Switch 8600.
- Nortel Ethernet Routing Switch 8600 software Release 4.1 or later is required for IPv6 hardware-based forwarding.

Basic IPv6 configuration navigation

Configuring the management port interface

The management port provides switch connectivity and management. As with other ports, you can configure the management port for routing IPv6 and you can configure a number of IPv6 addresses on an interface. The switch does not advertise the management port address to the other ports.

Procedure steps

Step	Action
1	In the Device Physical View tab, select the management port.
2	In the navigation tree, open the following folders: **Configuration, Edit**.
3	Double-click **Mgmt Port**.
4	Click the **Mgmt Port-IPv6 Interface** tab.
5	Click **Insert**.
6	Edit the fields as required.
7	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the management port interface.

Variable	Value
Identifier	The IPv6 address interface identifier. This is a binary string of up to 8 octets in network byte-order.
IdentifierLength	The length of the interface identifier in bits. The range is 0-64.
Descr	A text string containing information about the interface. The network management system configures this string.

Variable	Value
ReasmMaxSize(MTU)	The MTU for this IPv6 interface. This value must be the same for all the IP addresses defined on this interface. The default value is 1500.
AdminStatus	The indication of whether IPv6 is enabled (true) or disabled (false) on this interface. This object does not affect the state of the interface itself, only its connection to an IPv6 stack. The default is false.
ReachableTime	The time (in milliseconds) a neighbor is considered reachable after receiving a reachability confirmation. The range is 0-3600000 milliseconds. The default value is 30000.
RetransmitTime	The time (in milliseconds) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. The range is 0-3600000 milliseconds. The default value is 1000.
MulticastAdminStatus	The indication of whether multicasting for IPv6 is enabled (up) or disabled (down) on this interface. The default is false.

Configuring management port addresses

Configure an IPv6 address on the port to use in IPv6 routing. The switch does not advertise the management port address to the other ports.

Procedure steps

Step	Action
1	In the Device Physical View tab, select the management port.
2	In the navigation tree, open the following folders: **Configuration, Edit**.
3	Double-click **Mgmt Port**.
4	Click the **Mgmt Port-IPv6 Addresses** tab.
5	Click **Insert**.
6	In the **Addr** box, type the required IPv6 address for the management port.
7	In the **AddrLen** box, type the number of bits from the IPv6 address to advertise.
8	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure management port IPv6 addresses.

Variable	Value
IfIndex	The index value that uniquely identifies the interface to which this entry applies.
Addr	The IPv6 address to which this addressing pertains. **ATTENTION** If the IPv6 address exceeds 116 octets, the object identifiers (OIDS) of instances of columns in this row are more than 128 subidentifiers and you cannot use SNMPv1, SNMPv2c, or SNMPv3 to access them.
AddrLen	The prefix length value for this address. You cannot change the address length after creation. You must provide this value to create an entry in this table. The range is 0-128.
Type	Unicast, the only supported type.
Type	The type of address: unicast or anycast. The default is unicast.
Origin	A read-only value indicating the origin of the address. The origin of the address is other, manual, dhcp, linklayer, or random.
Status	A read-only value indicating the status of the address, describing whether the address is used for communication. The status is preferred (default), deprecated, invalid, inaccessible, unknown, tentative, or duplicate.
Created	A read-only value indicating the value of sysUpTime at the time this entry was created. If this entry was created prior to the last reinitialization of the local network management subsystem, the object contains a zero value.
LastChanged	A read-only value indicating the value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last reinitialization of the local network management subsystem, this object contains a zero value.

Configuring the CPU IPv6 route table

Edit the management port CPU route table to specify network and gateway IP addresses used to remotely manage the device.

Procedure steps

Step	Action
1	In the Device Physical View tab, select the management port.

2 In the navigation tree, open the following folders: **Configuration, Edit**.

3 Double-click **Mgmt Port**.

4 Click the **CPU IPv6 Route Table** tab.

5 Click **Insert**.

6 Edit the fields as required.

7 Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the CPU IPv6 route table.

Variable	Value
Network	The IPv6 destination address.
PrefixLength	The number of address bits to advertise. The range is 0-128.
Gateway	The IPv6 address of the management port.

Configuring a virtual IPv6 address

Configure a virtual IPv6 address to make the switch accessible in failover situations.

Procedure steps

Step	Action
1	In the Device Physical View tab, select the chassis.
2	In the navigation tree, open the following folders: **Configuration, Edit**.
3	Double-click **Chassis**.
	The Chassis tab appears with the System tab selected.
4	In the **VirtualIPv6Addr** box, type the IPv6 address to configure as the virtual IPv6 address.
5	In the **VirtualIPv6PrefixLength** box, type the number of bits from the virtual IPv6 address to advertise.

--End--

Adding an IPv6 interface ID to a brouter port or VLAN

You must configure an IPv6 interface for a VLAN or brouter port before you can assign an IPv6 address to the interface.

Prerequisites

- You must configure a VLAN before you can give the VLAN an interface identifier or an IPv6 address. The Ethernet Routing Switch 8600 supports port-based, protocol-based, and MAC-source-based VLANs. For information about configuring VLANs, see *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517) and *Nortel Ethernet Routing Switch 8600 Configuration — Link Aggregation, MLT, and SMLT* (NN46205-518).

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**. **ATTENTION** Enterprise Device Manager provides multiple paths to configure IPv6 interfaces and addresses. In addition to selecting Configuration, IPv6, IPv6, you can select Configuration, VLAN, VLANs, (select a VLAN), IPv6, Insert or Configuration, Edit, Port, IPv6, Insert.
3	Click the **Interfaces** tab.
4	Click **Insert**.
5	In the **IfIndex** box, click **Port** or **VLAN**, and select a port number or VLAN.
6	You must select the **AdminStatus** check box before the interface takes effect.
7	Edit the remaining fields.
8	Click **Insert**.
9	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure IPv6 interfaces.

Variable	Value
IfIndex	A unique value to identify a physical interface or a logical interface (VLAN). For the brouter port, it is the ifindex of the port, and for a VLAN it is the ifindex of the VLAN.
Identifier	The IPv6 address interface identifier. This is a binary string of up to 8 octets in network byte order.
IdentifierLength	The length of the interface identifier in bits.
Descr	A text string containing information about the interface. The network management system also configures this string.
VlanId	A value that uniquely identifies the Virtual LAN associated with the entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	The type of interface.
ReasmMaxSize(MTU)	The MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1500.
PhysAddress	The media-dependent physical address. For Ethernet, this is a MAC address.
AdminStatus	The indication of whether IPv6 is enabled (true) or disabled (false) on this interface. This object does not affect the state of the interface itself, only the connection to an IPv6 stack. The default is false.
OperStatus	The current operational status of the interface.
ReachableTime	The time (in milliseconds) a neighbor is considered reachable after receiving a reachability confirmation message. The default is 30000.
RetransmitTime	The time (in milliseconds) between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. The default is 1000.
MulticastAdminStatus	The indication of whether multicasting for IPv6 is enabled (up) or disabled (down) on this interface. The default is false.

Assigning IPv6 addresses to a brouter port or VLAN

Assign IPv6 addresses to interfaces to configure IPv6 routing for the interface.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.

2 Double-click **IPv6**.

3 Click the **Addresses** tab.

4 Click **Insert**.

5 In the **IfIndex** box, click **Port** or **VLAN**, and select a port number or VLAN.

6 Edit the remaining fields.

7 Click **Insert**.

8 Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the IPv6 addresses for a brouter port or VLAN.

Variable	Value
IfIndex	The index value that uniquely identifies the interface to which this entry applies.
Addr	The IPv6 address to which this entry addressing information pertains. **ATTENTION** if the IPv6 address exceeds 116 octets, the object identifiers (OIDS) of instances of columns in this row are more than 128 subidentifiers and you cannot use SNMPv1, SNMPv2c, or SNMPv3 to access them.
AddrLen	The prefix length value for this address. You cannot change the address length after you create it. You must provide this value to create an entry in this table.
Type	The type of address: unicast or anycast. The default is unicast.
Origin	A read-only value indicating the origin of the address. The origin of the address is other, manual, dhcp, linklayer, or random.
Status	A read-only value indicating the status of the address, describing whether the address is used for communication. The status is preferred (default), deprecated, invalid, inaccessible, unknown, tentative, or duplicate.

Variable	Value
Created	A read-only value indicating the value of sysUpTime at the time this entry was created. If this entry was created prior to the last reinitialization of the local network management subsystem, the object contains a zero value.
LastChanged	A read-only value indicating the value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last reinitialization of the local network management subsystem, this object contains a zero value.

Configuring route advertisement

Configure route advertisement in IPv6 for neighbor discovery (ND). IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Route Advertisement** tab.
4	Edit the fields as required.
5	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure IPv6 route advertisement.

Variable	Value
IfIndex	A unique value to identify a physical interface or a logical interface (VLAN). For the brouter port, the value is the ifindex of the port, and for the VLAN, the value is the ifindex of the VLAN.
SendAdverts	Indicates whether the router sends periodic router advertisements and responds to router solicitations on this interface. The default is True.
UseDefaultVal	Select one included value to use the default value, or use all bits to configure all options to their default value.

Variable	Value
MaxInterval	Configure the maximum interval (in seconds) at which the transmission of route advertisements occurs on this interface. This must be no less than 4 seconds and no greater than 1800 seconds. The default is 600.
MinInterval	Configure the minimum interval (in seconds) at which the transmission of route advertisements can occur on this interface. The value must be no less than 3 seconds and no greater than .75 x max-interval. The default is 200.
ReachableTime	The value (in milliseconds) placed in the router advertisement message sent by the router. The value zero means unspecified (by this router). Configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event. The default is 30000.
RetransmitTimer	The value (in milliseconds) placed in the retransmit timer field in the router advertisement message sent from this interface. The value zero means unspecified (by this router). The value configures the amount of time that router waits for the transmission to occur. The default is 1000.
DefaultLifeTime	The value placed in the router lifetime field of router advertisements sent from this interface. This value must be either 0 or between rcIpv6RouterAdvertMaxInterval and 9000 seconds. A value of zero indicates that the router is not a default router. The default is 3 times the value of rcIpv6RouterAdvertMaxInterval or 1800.
CurHopLimit	The default value placed in the current hop limit field in router advertisements sent from this interface. The value must be the current diameter of the Internet. A value of zero in the router advertisement indicates that the advertisement is not specifying a value for curHopLimit. The value must be the value specified in the IANA Web pages (www.iana.org). The default is 30.
ManagedFlag	If enabled, the ManagedFlag configures the M-bit or the managed address configuration in the router advertisement. The default is false.
OtherConfigFlag	If set to true, then the O-bit (Other stateful configuration) in the router advertisement is set. Reference RFC2461 Section 6.2.1. The default value is false.
DadNSNum	The number of neighbor solicitation messages for duplicate address detection (DAD). A value of 0 disables the DAD process on this interface. A value of 1 sends one advertisement without retransmissions.
LinkMTU	The value placed in MTU options sent by the router on this interface. A value of zero indicates that the router sends no MTU options.

Configuring the neighbor cache

Neighbor cache in IPv6 is similar to the IPv4 Address Resolution Protocol (ARP) table. The neighbor cache is a set of entries for individual neighbors to which traffic was sent recently. You make entries on the neighbor on-link unicast IP address, including information such as the link-layer address. A neighbor cache entry contains information used by the Neighbor Unreachability Detection algorithm, including the reachability state, the number of unanswered probes, and the time the next Neighbor Unreachability Detection event is scheduled.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Neighbors** tab.
4	Click **Insert**.
5	In the **IfIndex** box, click **Port** or **VLAN**, and select a port number or VLAN.
6	Edit the remaining fields.
7	Click **Insert**.
8	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the IPv6 neighbor cache.

Variable	Value
IfIndex	A unique value to identify a physical interface or a logical interface (VLAN). For the brouter port, the value is the ifindex of the port, and for the VLAN, the value is the ifindex of the vlan.
NetAddress	The IP address corresponding to the media-dependent physical address.
PhyAddress	The media-dependent physical address. The range is 0–65535. For Ethernet, this is a MAC address.
Interface	Either a physical port ID or the MLT port ID. This entry is associated either with a port or with the MLT in a VLAN/brouter port.

Variable	Value
LastUpdated	The value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last reinitialization of the local network management subsystem, this object contains a zero value.
Type	The mapping type is as follows: • Dynamic type: indicates that the IP address to the physical address mapping was dynamically resolved using, for example, IPv4 ARP or the IPv6 Neighbor Discovery Protocol. • Static type: indicates that the mapping was statically configured. • Local type: indicates that the mapping is provided for the interface address. The default is static.
State	The Neighbor Unreachability Detection state for the interface when the address mapping in this entry is used. If Neighbor Unreachability Detection is not in use (for example, for IPv4), this object is always unknown. Options include the following: • reachable: confirmed reachability • stale: unconfirmed reachability • delay: waiting for reachability confirmation before entering the probe state • probe: actively probing • invalid: an invalidated mapping • unknown: state cannot be determined • incomplete: address resolution is being performed

Adding a static neighbor to the cache

Add a static neighbor to create an entry for the neighbor route.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Neighbors** tab.

4 Click **Insert**.

5 In the **IfIndex** box, click **Port** or **VLAN**, and select a port number or VLAN.

6 In the **Type** list, select **static**.

7 Edit the remaining fields as required.

8 Click **Insert**.

--End--

Configuring IPv6 routing and ICMP

Enable IPv6 routing to route IPv6 traffic on the switch.

IPv6 packets transport Internet Control Message Protocol (ICMP) error and information messages. Configure the rate, in milliseconds, at which ICMP sends messages to conserve system resources.

To view a list of ICMP messages, see "ICMPv6 type and code" (page 439).

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	To enable IPv6 routing, in the **Forwarding** box, select **forwarding**.
4	Configure the routing and ICMP parameters as required.
5	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure IPv6 global properties.

Variable	Value
Forwarding	Configures whether this entity is an IPv6 router with respect to the forwarding of datagrams received by, but not addressed to, this entity. Select forwarding to act as a router. Select notForwarding to not act as a router. The default is notForwarding.
DefaultHopLimit	Configures the hop limit. The default is 30.

Variable	Value
Interfaces	A read-only value indicating the number of interfaces.
IfTableLastChange	A read-only value indicating the date of the last interface table change.
IcmpNetUnreach	If selected, enables the ICMP network unreachable feature. The default is disabled.
IcmpRedirectMsg	If selected, enables the ICMP redirect message feature. The default is disabled.
IcmpErrorInterval	Configures the interval (in milliseconds) for sending ICMPv6 error messages. The default is 1000 milliseconds. An entry of 0 seconds results in no sent ICMPv6 error messages.
IcmpErrorQuota	The number of ICMP error messages that can be sent during the ICMP error interval. A value of zero specifies not to send any. The default value is 50.
MulticastAdminStatus	If selected, enables multicasting. The default is false.

Configuring an IPv6 discovery prefix

The IPv6 discovery prefix determines the source of an IP address or set of IP addresses. The discovery prefix also permits other tables to share the information through a pointer rather than by copying. For example, when the node configures both a unicast and anycast address for a prefix, the ipAddressPrefix objects for those addresses point to a single row in the table.

You can use IPv4 addresses in IPv6. IPv4 prefixes use default values. You can override each value if an object is meaningful to the node.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Discovery Prefix** tab.
4	Click **Insert**.
5	In the **IfIndex** box, click **Port** or **VLAN**, and select a port number or VLAN.
6	Edit the remaining fields.
7	Click **Insert**.

8 Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the discovery prefix.

Variable	Value
IfIndex	A read-only value indicating the unique value to identify an IPv6 interface. For the brouter port, it is the ifindex of the port and, in the case of the VLAN, it is the ifindex of the VLAN.
Prefix	Configures the prefix to create an IPv6 address in the IPv6 interface table.
PrefixLen	Configures the mask to create an IPv6 prefix entry as either advertised or suppressed.
VlanId	Specifies the VLAN ID of the IPv6 interface.
UseDefaultVal	Select one of the values to set its value to default value. This is a bitmask field, setting all the bits means that all the options will be reverted to default values.
ValidLife	Configures the valid lifetime in seconds that indicates the length of time this prefix is advertised. The default is 2592000.
PreferredLife	Configures the preferred lifetime in seconds that indicates the length of time this prefix is advertised. The default value is 604800.
Infinite	Configures the prefix valid lifetime so it never expires. The default is false.
OnLinkFlag	Configures the prefix for use when determining if a node is onlink. This value is placed in the L-bit field in the prefix information option. It is a 1-bit flag. The default is true.
AutoFlag	Configures the prefix for use as the autonomous address configuration. This value is placed in the autoflag field in the prefix information option. It is a 1-bit flag. The default is true.
AddressEui	Configures the EUI address. Use an EUI-64 interface ID in the low-order 64-bits of the address when the ID is not specified in the address field. If enabled, use EUI, or use EUI-64 and the complement Universal/Local (U/L) bit. This operation provides for both global and link-local addresses. After you create the entry, you cannot modify this value. This value is valid for use only when the PrefixLength is 64 or less. The default is eui-not-used.
NoAdvertise	Select true to not include the prefix in the neighbor advertisement. The default is false.

Deleting an IPv6 address

Delete an IPv6 address from an interface to stop IPv6 routing on the interface.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Addresses** tab.
4	Select the address you want to delete.
5	Click **Delete**.

--End--

Deleting an IPv6 interface

Delete an IPv6 VLAN or brouter port to remove the IPv6 interface from the current configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Interfaces** tab
4	Select the interface you want to delete.
5	Click **Delete**.

--End--

Deleting an IPv6 discovery prefix

Delete an IPv6 discovery prefix to remove it from the current configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.

2 Double-click **IPv6**.

3 Click the **Discovery Prefix** tab.

4 Select the prefix you want to delete.

5 Click **Delete**.

--End--

Removing an entry from the neighbor cache

Remove entries from the neighbor cache to remove the route from the table.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Neighbors** tab.
4	Select the neighbor you want to remove.
5	Click **Delete**.

--End--

Basic IPv6 configuration using the CLI

This chapter describes how to use the command line interface (CLI) to perform basic IPv6 connectivity configuration.

Basic IPv6 configuration navigation

Job aid: Roadmap of basic IPv6 CLI commands

The following table lists the commands and parameters that you use to perform the procedures in this chapter.

Table 7
Job aid: Roadmap of basic IPv6 CLI commands

Command	Parameter
config ethernet slot/port ipv6 nd-prefix <prefix/prefix length> create	create
	default
	delete
	infinite
	info
	no-advertise
	pref-life
	valid-life
config ipv6 icmp-error-interval <0 through 2147483647>	--
config sys dns	--
config sys net6-mgmt ipv6 add <IPv6 address/prefix length> cpu-slot <slot-id>	--
config sys net6-mgmt ipv6 del <IPv6 address/prefix length> cpu-slot <slot-id>	--
config sys net6-mgmt route add <network IPv6 address> <network gateway>	--
config sys net6-mgmt route del <network IPv6 address> <network gateway>	--
config sys set mgmt-virtual-ipv6 <ipv6address/prefixlen>	--
config sys set snmp	--

Table 7
Job aid: Roadmap of basic IPv6 CLI commands (cont'd.)

Command	Parameter
`config vlan <vlan ID> ipv6 create`	`link-local`
	`descr`
	`addr`
	`addr-type`
	`delete`
	`admin`
	`mcast`
	`mtu`
	`reachable-time`
	`retransmit-time`
`config vlan <vlan id> ipv6 nd`	`dad-ns`
	`default`
	`hop-limit`
	`info`
	`life-time`
	`managed-flag`
	`other-stateful`
	`route-advertisement`
	`rtr-advert`

Assigning an IPv6 address to the management port

The Nortel Ethernet Routing Switch 8600 switch contains an Ethernet port in the SF/CPU slot. You can assign IPv6 addresses to this port to manage the device.

Perform duplicate address detection (DAD) for the management IPv6 address.

> **ATTENTION**
> Do not advertise the management route to the regular routing domain (OSPFv3) or advertise the prefix information for the management interface in router advertisement.

Procedure steps

Step	Action
1	Assign an IPv6 address to the management port: **`config sys net6-mgmt ipv6 add <IPv6 address/prefix length> cpu-slot <slot-id>`**

--End--

Variable definitions

Use the data in the following table to use the **`config sys net6-mgmt ipv6 add`** command.

Variable	Value
`IPv6 address/prefix length`	Specifies the IPv6 address and prefix length to assign to the port.
`slot-id`	Specifies the slot number where the port is located. If a slot ID is not specified, the address is configured for the current SF/CPU.

Configuring a management route

Configure a management route to establish communication between networks.

Procedure steps

Step	Action
1	Configure the management route by using the following command: **`config sys net6-mgmt route add <network IPv6 address> <network gateway>`**

--End--

Variable definitions

Use the data in the following table to use the **`config sys net6-mgmt route add`** command.

Variable	Value
network gateway	Specifies the IPv6 address of the gateway.
network IPv6 address	Specifies the IPv6 address of the network to add.

Configuring a management virtual IPv6 address

Configure a system virtual IPv6 address to manage of the SF/CPU Ethernet port in failover situations.

Procedure steps

Step	Action
1	Configure a virtual IPv6 address by using the following command: `config sys set mgmt-virtual-ipv6 <ipv6address/prefixlen>`

--End--

Variable definitions

Use the data in the following table to use the `config sys set mgmt-virtual-ipv6` command.

Variable	Value
ipv6address/prefixlen	Specifies the IPv6 address and prefix length to add to the port. The default value is 0:0:0:0:0:0:0:0/0.

Creating a VLAN

You must create a VLAN before you can configure it as an IPv6 VLAN. The Nortel Ethernet Routing Switch 8600 supports three types of VLANs:

- port-based VLANs
- protocol-based VLANs
- MAC-source-based VLANs

Specify the type of VLAN and assign an IP address to the VLAN. VLAN 1 is the default VLAN.

Procedure steps

Step	Action
1	Create a VLAN by using the following command: `config vlan <vid> create`

--End--

Variable definitions

Use the data in the following table to use the **config vlan create** command.

Variable	Value
byport <sid> [name <value>] [color <value>]	Creates a port-based VLAN. • **sid** is the spanning tree group ID from 1-64 characters. • **name <value>** is the name of the VLAN from 0-64 characters. • **color <value>** is the color of the VLAN (0-32). The color attribute is used by Optivity software to display the VLAN.
byprotocol <sid> <ip|appleTalk|declat|decOther|sna802dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp|PPPoE> [<pid>] [name <value>] [color <value>] [encap <value>]	Creates a protocol-based VLAN. • **sid** is the spanning tree ID 1-64. • **ip|appleTalk|decLat|decOther|sna802dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp| PPPoE** specifies the protocol. • **pid** is a user-defined protocol ID number in hexadecimal format (0 to 65535). • **name <value>** is the name of the VLAN from 0-64 characters. • **color <value>** is the color of the VLAN (0-32). The color attribute is used by Optivity software to display the VLAN. • **encap <value>** is the frame encapsulation method.

Variable	Value
`bysrcmac <sid> [name <value> ] [color <value>]`	Creates a VLAN by MAC-source address. • `sid` is the spanning tree ID 1-64. • `name <value>` is the name of the VLAN from 0-64 characters. • `color <value>` is the color of the VLAN (0-32). The color attribute is used by Optivity software to display the VLAN. This command is available only for the Nortel Ethernet Routing Switch 8600.
`info`	Shows information about the specified VLAN.
`vid`	Specifies the VLAN ID (from 1-4094).

Configuring the VLAN as an IPv6 VLAN

Configure a VLAN as an IPv6 VLAN to use IPv6 routing on the VLAN.

Prerequisites

- You must create the VLAN before you configure it as an IPv6 VLAN.

Procedure steps

Step	Action
1	Configure the VLAN by using the following command: **`config vlan <vlan ID> ipv6 create`**

--End--

Variable definitions

Use the data in the following table to use the **`config vlan ipv6 create`** command.

Variable	Value
`addr`	Specifies the IPv6 address and prefix length in the format address and prefix length.
`addr-type`	1—unicast, 2—anycast. The default values is 1—unicast.

Variable	Value
`admin`	Enables or disables the administrative state of the interface.
`delete`	Deletes one of the following: • addr <value> • all • interface
`descr`	Views or updates the description for the interface.
`info`	Displays information about the configuration.
`link-local`	Specifies a numeric identifier for the interface.
`mcast`	Enables or disables MLD. The default value is disable.
`mtu`	Configures the maximum transmission unit for the interface. The default value is 1500.
`reachable-time`	Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation. The default value is 30000.
`retransmit-time`	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. The default value is 1000.
`vlan id`	Specifies the VLAN ID, from 1-4094.

Assigning an IPv6 address to the VLAN

Assign an IPv6 address to the VLAN to enable IPv6 routing on the VLAN.

Procedure steps

Step	Action
1	Assign an IPv6 address by using the following command: `config vlan <vlan id> ipv6 create addr <ipv6 address>`

--End--

Variable definitions

Use the data in the following table to use the **config vlan ipv6 create addr** command.

Variable	Value
ipv6 address	Specifies the IPv6 address to add to the VLAN.
vlan id	Specifies the ID of the VLAN, from 1-4094.

Example of assigning an IPv6 address to a VLAN

Procedure steps

Step	Action
1	Assign an IPv6 address: ERS-8610:5#**config vlan 13 ipv6 create addr 8888:0:0:0:0:0:0:1/96**

--End--

Configuring the administrative status for the VLAN

Configure the administrative status to enable the IPv6 VLAN.

Procedure steps

Step	Action
1	Configure the administrative status by using the following command: **config vlan <vlan id> ipv6 admin enable**

--End--

Variable definitions

Use the data in the following table to use the **config vlan ipv6 admin enable** command.

Variable	Value
vlan id	Specifies the ID of the VLAN, from 1 to 4094.

Assigning an IPv6 address to the brouter port

Assign an IPv6 address to a brouter port on a VLAN to customize the IPv6 VLAN configuration.

Procedure steps

Step	Action
1	Assign an IPv6 address by using the following command: **`config ethernet <slot/port> ipv6 create addr <ipv6 address> vlan <vlan id>`**

--End--

Variable definitions

Use the data in the following table to use the **`config ethernet ipv6 create addr vlan`** command.

Table 8
Variable defintions

Variable	Value
`ipv6 address`	Specifies the IPv6 address to add to the port.
`slot/port`	Identifies the slot and port location.
`vlan id`	Specifies the ID of the VLAN, from 1-4094.

Setting the administrative status on a brouter port

Enable the brouter port by setting the administrative status.

Procedure steps

Step	Action
1	Configure the administrative status by using the following command: **`config ethernet <slot/port> ipv6 admin enable`**

--End--

Variable definitions

Use the data in the following table to use the **`config ethernet ipv6 admin enable`** command.

Variable	Value
`slot/port`	Specifies the slot and port location for the port.

Configuring IPv6 ICMP

Configure Internet Control Message Protocol (ICMP) to transport error and information messages within IPv6 packets.

To view a list of ICMP messages, see “ICMPv6 type and code” (page 439).

Procedure steps

Step	Action
1	Configure the ICMP rate by using the following command: **`config ipv6 icmp-error-interval <0 through 2147483647>`**

--End--

Configuring neighbor discovery prefixes

IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

Procedure steps

Step	Action
1	Configure discovery prefixes for a brouter port by using the following command: **`config ethernet <slot/port> ipv6 nd-prefix <prefix/prefix length> create`**
2	Configure discovery prefixes for a VLAN by using the following command: **`config vlan <vlan id> ipv6 nd-prefix <prefix/prefix length> create`**

--End--

Variable definitions

Use the data in the following table to use the **config ethernet ipv6 nd-prefix create** and **config vlan ipv6 nd-prefix create** commands.

Variable	Value
create	Creates discovery prefixes and configures the following options: • on-link-flag: if assigned, onlink determination uses the prefix. This value is placed in the L-bit field in the prefix information option. It is a 1-bit flag. The default value is true. • auto-flag: if assigned, the prefix is used for autonomous address configuration. The default value is true. • eui: (1) Extended Unique Identifier (EUI) not used, (2) EUI with Universal/Local bit (U/L) complement enabled, (3) EUI used without U/L. The default value is (EUI) not used. • no-advertise: if true, the prefix is not advertised. If false, the prefix is advertised. The default value is false.
default	Select one of the values to use as the default value. This is a bitmask field; using all the bits means that all the options revert to default values: • (0) valid-life • (1) preferred-life • (3) no-advertise
delete	Deletes the prefix.
infinite	If assigned, the prefix does not expire. The default value is false.
info	Subcontext commands.
no-advertise	Modify whether the prefix is advertised. The true setting prevents prefix advertisement. The default value is false.
pref-life	The number of seconds that the prefix can accept and use new connections. The default value is 604800.
prefix/prefix length	Specifies the IP address and prefix.

Variable	Value
slot/port	Specifies the slot and port location of the brouter port.
valid-life	The number of seconds that the prefix advertised in the neighbor advertisement is valid. During the valid lifetime, existing connections can be used. New connections cannot be opened. The default value is 2592000.
vlan id	Specifies the ID of the VLAN from 1-4094.

Example of configuring neighbor discovery prefixes

Procedure steps

Step	Action
1	Configure brouter port 4/18 with an IPv6 address of 4040::1/96. `ERS-8610:5#`**`config ethernet 4/18 ipv6 nd-prefix 4040::0/96 create`**
2	Configure VLAN 13 with an IPv6 address of 8888::1/96. `ERS-8610:5#`**`config vlan 13 ipv6 nd-prefix 8888::1/96 create`**

--End--

Configuring route advertisement

Use route advertisement to discover potential default routers in a network and to discover link information.

Procedure steps

Step	Action
1	Configure route advertisement on a brouter port by using the following command: **`config ethernet <slot/port> ipv6 nd`**
2	Configure route advertisement on a VLAN by using the following command: **`config vlan<vlan id> ipv6 nd`**

--End--

Variable definitions

Use the data in the following table to use the **config ethernet ipv6 nd** and **config vlan ipv6 nd** commands.

Variable	Value
dad-ns	The number of neighbor solicitation messages from duplicate address detection. The acceptable range is 0-600. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. The default value is 1.
default	Select one or multiple entries to configure the default value. • max-interval • min-interval • life-time • hop-limit • managed-flag • other-config-flag • dad-ns-num • all
hop-limit	Configures the maximum number of hops before packets drop. The default value is 30.
info	Display subcontext commands.
life-time	Enter the router lifetime included in router advertisement. Other devices use this information to determine if the router can be reached.
managed-flag	Configure to true to enable M-bit (managed address configuration) on the router. The default value is false.
other-stateful	Configure to true to enable the O-bit (other stateful configuration) in the router advertisement. Other stateful configuration autoconfigures received information without addresses. The default value is false.

Variable	Value
route-advertisement	Enable or disable periodic router advertisement messages. The default value is true.
rtr-advert	min <value>: The minimum time allowed between sending unsolicited multicast router advertisements. The default value is 200. max <value>: The maximum time allowed between sending unsolicited multicast router advertisements from the interface, in seconds. (3-200 seconds). The default value is 600.

Adding static entries to the neighbor cache

The neighbor cache is populated with information about IPv6 neighbors to which the IPv6 device sends traffic. You can add neighbors to the cache manually.

Procedure steps

Step	Action
1	Add a neighbor by using the following command: **config ipv6 neighbor add ports <slot/port> ipv6addr <ipv6 address> mac <mac address> vlanid <vlan id>**

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 neighbor add ports** command.

Variable	Value
ipv6 address	Specifies the IPv6 address in hexadecimal colon format {string length 0..128}
mac address	Specifies the MAC address in the following format: {0x00:0x00:0x00:0x00:0x00:0x00}

Variable	Value
slot/port	Specifies the slot and port location to add a neighbor for a brouter port.
vlan id	Specifies the ID of the VLAN to add a neighbor for a VLAN.

Example of adding static entries to the neighbor cache

Procedure steps

Step	Action
1	Add a VLAN static entry. ERS-8610:5#**config ipv6 neighbor add ports 4/17 ipv6addr 9999:0:0:0:0:0:0:1 mac 00:80:2d:c0:92:03 vlanid 14**
2	Add a brouter port static entry. ERS-8610:5#**config ipv6 neighbor add ports 4/18 ipv6addr 4040:0:0:0:0:0:0:1 mac 00:80:2d:c0:92:03**

--End--

Deleting an IPv6 address from the Ethernet SF/CPU slot

You can assign multiple addresses to the Ethernet SF/CPU slot on the Nortel Ethernet Routing Switch 8600. Delete an address to remove it from the configuration.

Procedure steps

Step	Action
1	Remove an IPv6 address from the Ethernet SF/CPU slot by using the following command: **config sys net6-mgmt ipv6 del <IPv6 address/prefix length> cpu-slot <slot-id>**

--End--

Variable definitions

Use the data in the following table to use the **config sys net6-mgmt ipv6 del** command.

Variable	Value
`IPv6 address/prefix length`	Specifies the IPv6 address and prefix length to delete from the port.
`slot-id`	Specifies the slot number where the port is located. If a slot ID is not specified, the address is deleted from the current SF/CPU.

Deleting an IPv6 address

Delete the IPv6 address to stop IPv6 routing.

Procedure steps

Step	Action
1	Delete the IPv6 address on a VLAN by using the following command: **`config vlan <vlan id> ipv6 delete addr <Ipv6 address>`**
2	Delete the IPv6 address on a brouter port by using the following command: **`config ethernet <slot/port> ipv6 delete addr <IPv6 address>`**

--End--

Variable definitions

Use the data in the following table to use the **`config vlan ipv6 delete addr`** and **`config ethernet ipv6 delete addr`** commands.

Variable	Value
`IPv6 address`	Specifies the IPv6 address to delete.
`slot/port`	Specifies the slot and port location of the brouter port from which to delete the IPv6 address.
`vlan id`	Specifies the ID of the VLAN from which to delete the IPv6 address.

Example of deleting an IPv6 address

Procedure steps

Step	Action
1	Delete the IPv6 address on a VLAN:

```
ERS-8610:5#config vlan 13 ipv6 delete addr 9898::1
```

2 Delete the IPv6 address on a brouter port:

```
ERS-8610:5#config ethernet 1/18 ipv6 delete addr
4040::1
```

--End--

Deleting an IPv6 interface

Delete an IPv6 interface to remove it from the configuration.

Procedure steps

Step	Action
1	Delete an IPv6 interface from a VLAN by using the following command: **config vlan <vlan id> ipv6 delete interface**
2	Delete an IPv6 interface from a brouter port by using the following command: **config ethernet <slot/port> ipv6 delete interface**

--End--

Variable definitions

Use the data in the following table to use the **config vlan ipv6 delete interface** and **config ethernet ipv6 delete interface** commands.

Variable	Value
slot/port	Specifies the slot and port location of the brouter port from which to delete the IPv6 interface.
vlan id	Specifies the ID of the VLAN from which to delete the IPv6 interface.

Example of deleting an IPv6 interface

Procedure steps

Step	Action
1	Delete the IPv6 interface on a VLAN: ERS-8610:5#**config vlan 13 ipv6 delete interface**

2 Delete the IPv6 interface on a brouter port:

```
ERS-8610:5#config ethernet 1/18 ipv6 delete
interface
```

--End--

Modifying interface parameters

Modify interface parameters to update configured settings for VLAN or brouter port parameters.

Procedure steps

Step	Action
1	Modify parameters for a VLAN by using the following command: `config vlan <vlan id> ipv6`
2	Modify parameters for a brouter port by using the following command: `config ethernet <slot/port> ipv6`

--End--

Variable definitions

Use the data in the following table to use the **config vlan ipv6** and **config ethernet ipv6** commands.

Variable	Value
admin	Enables or disables the interface.
create	Creates an interface and configures the following: • link-local • descr: modify the description for the interface. • addr: modify the IPv6 address for the interface. • addr-type: unicast or anycast The default value is unicast.
delete	Deletes one of the following: • addr • all • interface

Variable	Value
mcast	Enables or disables the multicast administrative status of the interface. The default value is disable.
mtu	Configures the maximum transmission unit in bytes for the interface. The default value is 1500.
reachable-time	Configures the time (in milliseconds) a neighbor is considered reachable after receiving a reachability confirmation. The default value is 30000.
retransmit-timer	Configures the time (in milliseconds) between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. The default value is 1000.
slot/port	Specifies the slot and port location of the brouter port.
vlan id	Specifies the ID of the VLAN from 1-4094.

Deleting a management route

Delete a management route to stop communication between networks.

Procedure steps

Step	Action
1	Delete a management route by using the following command: **config sys net6-mgmt route del <network IPv6 address> <network gateway>**

--End--

Variable definitions

Use the data in the following table to use the **config sys net6-mgmt route del** command.

Variable	Value
network gateway	Specifies the IPv6 address of the gateway.
network IPv6 address	Specifies the IPv6 address of the network to delete.

Deleting a neighbor discovery prefix

Delete a neighbor discovery prefix to remove it from the configuration.

Procedure steps

Step	Action
1	Delete a neighbor discovery prefix from a VLAN by using the following command: `config vlan <vlan id> ipv6 nd-prefix <prefix/length> delete`
2	Delete a neighbor discovery prefix from a brouter port by using the following command: `config ethernet <slot/port> ipv6 nd-prefix <prefix/length> delete`

--End--

Variable definitions

Use the data in the following table to use the **config vlan ipv6 nd-prefix delete** and **config ethernet ipv6 nd-prefix delete** command.

Variable	Value
prefix/length	Specifies the IP address and prefix.
slot/port	Specifies the slot and port location of the brouter port.
vlan id	Specifies the ID of the VLAN from 1-4094.

Example of deleting a neighbor discovery prefix

Procedure steps

Step	Action
1	Delete a neighbor discovery prefix from a VLAN: ERS-8610:5#**config vlan 13 ipv6 nd-prefix 9898::0/96 delete**
2	Delete a neighbor discovery prefix from a brouter port: ERS-8610:5#**config ethernet 1/18 ipv6 nd-prefix 4040::0/96 delete**

--End--

Removing an entry from the neighbor cache

Remove an entry from the neighbor cache to delete it from the static configuration.

Procedure steps

Step	Action
1	Remove an entry by using the following command: **config ipv6 neighbor delete <ipv6 address> port <slot/port> vlanid <vlan id>**

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 neighbor delete** command.

Variable	Value
ipv6 address	Specifies the IPv6 address in hexadecimal colon format (string length 0-128).
slot/port	Specifies the slot and port location to remove a neighbor for a brouter port.
vlan id	Specifies the ID of the VLAN to remove a neighbor for a VLAN.

Example of removing an entry from the neighbor cache

Procedure steps

Step	Action
1	Remove a VLAN entry from the neighbor cache: ERS-8610:5#**config ipv6 neighbor delete 8888:0:0:0:0:0:0:1 vlanid 13**

--End--

Basic IPv6 configuration using the NNCLI

This section describes how to use the Nortel command line interface (NNCLI) to perform basic IPv6 connectivity configuration.

Basic IPv6 configuration navigation

Job aid: Roadmap of basic IPv6 NNCLI commands

The following table lists the commands and parameters that you use to perform the procedures in this section.

Table 9
Job aid: Roadmap of basic IPv6 NNCLI commands

Command	Parameter
Global Configuration mode	

Table 9
Job aid: Roadmap of basic IPv6 NNCLI commands (cont'd.)

Command	Parameter
`ipv6 icmp`	`error-interval <0 through 2147483647>`
	`redirect-msg`
	`unreach-msg`
`ipv6 mgmt-virtual <ipv6address/prefixlen>`	--
`ipv6 neighbor <ipv6 address>`	`port <slot/port> mac <mac address> vlan <vlan id>`
`net6-mgmt ipv6`	`<IPv6 address/prefix length>`
	`route <network IPv6 address>`
`vlan create <vid>`	`name <value>`
	`type <value>`
Interface Configuration mode	
`ipv6 interface`	`address-type <1-2>`
	`enable`
	`link-local <word>`
	`mtu <bytes>`
	`multicast-routing`
	`name`
	`reachable-time <ms>`
	`retransmit-time <ms>`
	`vlan <vlan id>`
`ipv6 interface address <ipv6 address>`	`address-type <1-2>`
	`link-local <word>`
	`mtu <bytes>`
	`multicast-routing`
	`reachable-time <ms>`
	`retransmit-time <ms>`

Table 9
Job aid: Roadmap of basic IPv6 NNCLI commands (cont'd.)

Command	Parameter
`ipv6 nd`	`dad-ns`
	`hop-limit`
	`managed-config-flag`
	`other-config-flag`
	`ra-lifetime`
	`rtr-advert-max-interval`
	`rtr-advert-min-interval`
	`send-ra`
`ipv6 nd prefix <prefix/prefix length>`	`infinite`
	`no-advertise`
	`preferred-life <seconds>`
	`valid-life <seconds>`
`ipv6 nd prefix-interface <Ipv6address-prefix>`	`no-autoconfig <false|true>`
	`eui <1-3>`
	`no-advertise`
	`no-onlink <false|true>`

Assigning an IPv6 address to the management port

The Nortel Ethernet Routing Switch 8600 switch contains an Ethernet port in the SF/CPU slot. You can assign IPv6 addresses to this port to manage the device.

Perform duplicate address detection (DAD) for the management IPv6 address.

> **ATTENTION**
> Do not advertise the management route to the regular routing domain (OSPFv3) or advertise the prefix information for the management interface in router advertisement.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Assign an IPv6 address to the management port by using the following command: **`net6-mgmt ipv6 <IPv6 address/prefix length>`**

--End--

Variable definitions

Use the data in the following table to use the **`net6-mgmt ipv6`** command.

Variable	Value
`IPv6 address/prefix length`	Specifies the IPv6 address and prefix length to assign to the management interface. The default value is none.

Configuring a management route

Configure a management route to establish communication between networks.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the management route by using the following command: **`net6-mgmt ipv6 route <network IPv6 address>`**

--End--

Variable definitions

Use the data in the following table to use the **`net6-mgmt ipv6 route`** command.

Variable	Value
`network IPv6 address`	Specifies the IPv6 address and prefix length of the network to add. The default value is none.

Configuring a management virtual IPv6 address

Configure a system virtual IPv6 address to manage of the SF/CPU Ethernet port in failover situations.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure a virtual IPv6 address by using the following command: `ipv6 mgmt-virtual <ipv6address/prefixlen>`

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 mgmt-virtual`** command.

Variable	Value
`ipv6address/prefixlen`	Specifies the IPv6 address and prefix length to add to the port. To configure this option to the default value, use the `default` operator with the command: `default ipv6 mgmt-virtual`. The default value is 0:0:0:0:0:0:0:0/0.

Creating a VLAN

You must create a VLAN before you can configure it as an IPv6 VLAN. Nortel Ethernet Routing Switch 8600 supports three types of VLANs:

- port-based VLANs
- protocol-based VLANs
- MAC-source-based VLANs

Specify the type of VLAN and assign the VLAN a name. VLAN 1 is the default VLAN.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create a VLAN by using the following command: **`vlan create <vid> name <value> type <value>`**

--End--

Variable definitions

Use the data in the following table to use the **`vlan create`** command.

Variable	Value
`name <value>`	Configures a name for the VLAN.
`type <value>`	Specifies the type of VLAN to create: • port [<stgId:1-16>|cist|msti <1-15>] • protocol-ApltkEther2Snap • protocol-decEther2 • protocol-decOtherEther2 • protocol-ipEther2 • protocol-ipv6Ether2 • protocol-Netbios • protocol-RarpEther2 • protocol-sna802.2 • protocol-snaEther2 • protocol-Userdef <4096-65534> • protocol-vinesEther2 • protocol-xnsEther2 • ipsubnet-mstprstp <1-63> <A.B.C.D/0-32> [color<1-32>] • port-mstprstp <1-63> <A.B.C.D/0-32> [color<1-32>] [naap-vlan] [firewall-vlan] [firewall-peering-vlan]

Variable	Value
	• protocol-mstprstp <1-63> ip|appleTalk|decLat|decOther|sna802dot2|snaEthernet2|netBios|xns|vines|ipV6|usrDefined|rarp|PPPoE [<pid>] [color <1-32>] [encap <value>] • srcmac-mstprstp <1-63> [color <1-32>] • svlan-mstprstp <1-63> [color <1-32>] • ids-mstprstp <1-63> [color <1-32>] • ipsubnet <1-63> <A.B.C.D/mask> [color <1-32>] • srcmac <1-63> [color <1-32>] • svlan <1-63> [color <1-32>] • ids <1-63> [color <1-32>] stgId is the spanning tree group ID. color <value> is the color of the VLAN. Optivity software uses the color attribute to display the VLAN. pid is a user-defined protocol ID number in hexadecimal format (0–65535). encap <value> is the frame encapsulation method. **ATTENTION** The mstprstp options are available for the Nortel Ethernet Routing Switch 8600 only.
`vid`	Specifies the VLAN ID (from 1–4094).

Configuring an interface as an IPv6 interface

Configure an interface as an IPv6 interface to use IPv6 routing on the interface.

Prerequisites

- You must log on to the Interfaces configuration mode in NNCLI for the required port or port list.

Procedure steps

Step	Action
1	Configure the IP address by using the following command: **`ipv6 interface address <ipv6 address> vlan <vlan id>`**

2 Configure additional parameters for the port by using the following command:

```
ipv6 interface [address-type <1-2>] [mtu <bytes>]
[muticast-routing] [reachacble-time <ms>]
[retransmit-time <ms>] [vlan <vlan id>]
```

--End--

Variable definitions

Use the data in the following table to use the **ipv6 interface** and **ipv6 interface address** commands.

Variable	Value
address <ipv6 address>	Configures the IPv6 address and prefix length in the format address and prefix length. The default value is none.
address-type <1-2>	1—unicast, 2—anycast. The default value is 1—unicast.
mtu <bytes>	Configures the maximum transmission unit for the interface. The default value is 1500.
multicast-routing	Enables or disables MLD. The default value is disable.
reachable-time <ms>	Configures the time, in milliseconds, that a neighbor is considered reachable after receiving a reachability confirmation. The default value is 30000.
retransmit-time <ms>	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. The default value is 1000.
vlan <vlan id>	Specifies the VLAN ID.

Configuring the VLAN as an IPv6 VLAN

Configure a VLAN as an IPv6 VLAN to use IPv6 routing on the VLAN.

Prerequisites

- You must log on to the VLAN Interfaces configuration mode in NNCLI for the required VLAN ID.
- You must create the VLAN before you configure it as an IPv6 VLAN.

Procedure steps

Step	Action
1	Configure the IP address by using the following command: **`ipv6 interface address <ipv6 address>`**
2	Configure additional parameters for the VLAN by using the following command: **`ipv6 interface [address-type <1-2>] [mtu <bytes>] [muticast-routing] [reachacble-time <ms>] [retransmit-time <ms>]`**

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 interface`** and **`ipv6 interface address`** commands.

Variable	Value
`address <ipv6 address>`	Configures the IPv6 address/prefix length. The default value is none.
`address-type <1-2>`	1—unicast, 2—anycast. The default value is 1—unicast.
`mtu <bytes>`	Configures the maximum transmission unit for the interface. The default value is 1500.
`multicast-routing`	Enables or disables MLD. The default value is disable.
`reachable-time <ms>`	Configures the time, in milliseconds, a neighbor is considered reachable after receiving a reachability confirmation. The default value is 30000.
`retransmit-time <ms>`	Configures the time, in milliseconds, between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. The default value is 1000.

Configuring IPv6 ICMP

Configure Internet Control Message Protocol (ICMP) to transport error and information messages within IPv6 packets.

To view a list of ICMP messages, see "ICMPv6 type and code" (page 439).

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the ICMP rate by using the following command: **`ipv6 icmp error-interval <0 through 2147483647>`**
2	Set the status for redirect messages by using the following command: **`ipv6 icmp redirect-msg`**
3	Configure the status for unreachable messages by using the following command: **`ipv6 icmp unreach-msg`**

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 icmp`**command.

Variable	Value
`error-interval <0 through 2147483647>`	Configures the error interval in milliseconds. The interval is the time between transmission of error messages. To configure this option to the default value, use the **`default`** operator with the command. The default value is 1000.

Variable	Value
redirect-msg	Configures the administrative status for ICMP redirect messages. Use the **no** operator to remove this configuration. To configure this option to the default value, use the **default** operator with the command. The default value is disable.
unreach-msg	Configures the administrative status for ICMP unreachable messages. Use the **no** operator to remove this configuration. To configure this option to the default value, use the **default** operator with the command. The default value is disable.

Configuring neighbor discovery prefixes

IPv6 nodes on the same link use ND to discover link-layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided by Address Resolution Protocol (ARP) and router discovery for IPv4. IPv6 router advertisement includes discovery prefixes.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure discovery prefixes by using the following command: **ipv6 nd prefix-interface < Ipv6address-prefix> [no-autoconfig <false|true>] [eui <1-3>] [no-advertise] [no-onlink <false|true>]**
2	Configure neighbor discovery prefix parameters by using the following command: **ipv6 nd prefix <prefix/prefix length> [infinite] [no-advertise] [preferred-life <seconds>] [valid-life <seconds>]**

--End--

Variable definitions

Use the data in the following table to use the **ipv6 nd prefix** and **ipv6 nd prefix-interface** commands.

Variable	Value
no-autoconfig <false|true>	If true, the prefix is used for autonomous address configuration. The default value is true.
eui <1-3>	(1) eui (extended unique identifier) not used, (2) eui with U/L (Universal/Local bit) complement enabled, (3) eui used without u/l. The default value is eui not used.
infinite	Configures the prefix as infinite. The default value is disable.
no-advertise	Removes the prefix from the neighbor advertisement. Use the **no** operator to remove this option. Use the **default** operator to configure this value to the default setting. The default value is disable.
no-onlink <false|true>	If true, onlink determination uses the prefix. This value is placed in the L-bit field in the prefix information option. It is a 1-bit flag. The default value is true.
preferred-life <seconds>	Configures the preferred life, in seconds. The valid range is 0–3600000. Use the **default** operator to configure this value to the default setting. The default value is 604800.
prefix/prefix length	Specifies the IP address and prefix.
valid-life <seconds>	Configures the valid life, in seconds. The valid range is 0–3600000. Use the **default** operator to configure this value to the default setting. The default value is 2592000.

Configuring route advertisement

Use route advertisement to discover potential default routers in a network and to discover link information.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure route advertisement on a brouter port by using the following command: **ipv6 nd [dad-ns <0-600>] [hop-limit <1-255>] [managed-config-flag] [other-config-flag] [ra-lifetime <0|4-9000>] [rtr-advert-max-interval <4-1800>] [rtr-advert-min-interval <3-1350>] [send-ra]**

--End--

Variable definitions

Use the data in the following table to use the **ipv6 nd** command.

Variable	Value
dad-ns	The number of neighbor solicitation messages from duplicate address detection. The acceptable range is 0-600. A value of 0 disables duplicate address detection on the specified interface. A value of 1 configures a single transmission without follow-up transmissions. Use the **default** operator to configure this value to the default setting. The default value is 1.
hop-limit	Enter the maximum number of hops before packets drop. Use the **default** operator to configure this value to the default setting. The default value is 30.
managed-config-flag	Configure to true to enable M-bit (managed address configuration) on the router. Use the **no** operator to remove this option. Use the **default** operator to configure this value to the default setting. The default value is false.
other-config-flag	Configure to true to enable the O-bit (other stateful configuration) in the router advertisement. Other stateful configuration autoconfigures received information without addresses. Use the **no** operator to remove this option. Use the **default** operator to configure this value to the default setting. The default value is false.

Variable	Value
ra-lifetime	Enter the router lifetime included in router advertisement. Other devices use this information to determine if the router can be reached. The range is 0 or 4–9000. Use the **default** operator to configure this value to the default setting. The default value is 1800.
rtr-advert-max-interval	Configures the maximum time allowed between sending unsolicited multicast router advertisements. The default value is 600.
rtr-advert-min-interval	Configures the minimum time allowed, in seconds (3–1350), between sending unsolicited multicast router advertisements from the interface. Use the **default** operator to configure this value to the default setting. The default value is 200.
send-ra	Enable or disable periodic router advertisement messages. Use the **no** operator to remove this option. Use the **default** operator to configure this value to the default setting. The default value is true.

Adding static entries to the neighbor cache

The neighbor cache contains information about IPv6 neighbors to which the IPv6 device sends traffic. You can manually add neighbors to the cache.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Add a neighbor by using the following command:

ipv6 neighbor <ipv6 address> port <slot/port> mac <mac address> vlan <vlan id>

--End--

Variable definitions

Use the data in the following table to use the **ipv6 neighbor** command.

Variable	Value
ipv6 address	Specifies the IPv6 address in hexadecimal colon format {string length 0..128}. The default value is none.
mac address	Specifies the MAC address in the following format: {0x00:0x00:0x00:0x00:0x00:0x00}
slot/port	Specifies the slot and port location to add a neighbor for a brouter port.
vlan id	Specifies the ID of the VLAN to add a neighbor for a VLAN.

Example of adding static entries to the neighbor cache

Procedure steps

Step	Action
1	Add a VLAN static entry: `ERS-8606:5(config)#`**`ipv6 neighbor 9999:0:0:0:0:0:0:1 port 4/1 mac 00:80:2d:c0:92:03 vlan 4`**

--End--

IPv6 routing configuration using Enterprise Device Manager

This chapter describes Enterprise Device Manager procedures to configure IPv6 static routes and the Open Shortest Path First version 3 (OSPFv3) protocol in the Ethernet Routing Switch 8600. Routers exchange network topology information with the Open Shortest Path First (OSPF) protocol. For conceptual information relating to static routes and OSPF, see "IPv6 routing fundamentals" (page 25).

IPv6 routing configuration navigation

Creating IPv6 static routes

To improve the static route management, you can change static routes directly with the IPv6 static routing table manager. The static routing table is separate from the system routing table, which the router uses to control forwarding. Although the tables are separate, entries in the static routing table manager automatically change in the system routing table if the next-hop address in the static route is reachable and the static route is enabled.

Use static routes to manually configure routes to destination IPv6 address prefixes.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Static Routes** tab.
4	Click **Insert**.
5	In the **Dest** box, type the IPv6 address.
6	In the **PrefixLength** box, type the length of the prefix for the IPv6 address.
7	In the **NextHop** box, type the IPv6 address of the router through which the specified route is accessible.
8	In the **IfIndex** box, click **Port**, **VLAN**, or **Tunnel** and select an option.
9	In the **Cost** box, type a number for the distance.
10	Select the **Enable** check box.
11	In the **Preference** box, type the route preference.
12	Click **Insert**.
	The new route appears in the Static Routes tab.

--End--

Variable definitions

Use the data in the following table to configure the static route.

Variable	Value
Dest	Configures the IPv6 destination network address. The prefix value must match the PrefixLength.
PrefixLength	Configures the number of leading one bits that form the mask as a logical value. The prefix value must match the value in the Dest box. The range is 0–128.
NextHop	Configures the next hop IPv6 address.

<table>
<tr><th>Variable</th><th>Value</th></tr>
<tr><td>IfIndex</td><td>Select the required VLAN, port, or tunnel.</td></tr>
<tr><td>Cost</td><td>Configures the cost or distance ratio to reach the destination for this node. The range is 1–65535.
The default value is 1.</td></tr>
<tr><td>Enable</td><td>Configures whether the configured static route is available on the port. The default is enable.

ATTENTION
If a static route is disabled, you must enable it before you can add the route to the system routing table.</td></tr>
<tr><td>Status</td><td>Indicates the current status of this entry.</td></tr>
<tr><td>Preference</td><td>Configures the routing preference of the destination IPv6 address. The range is 1-255.
The default value is 5.</td></tr>
</table>

Creating a static default route

You can statically configure the routing switches with the default route statically, or routing switches can learn the default route through a dynamic routing protocol (RFC1812).

> **ATTENTION**
> You must configure the destination address and subnet mask for the default static route to 0::0.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Static Routes** tab.
4	Click **Insert**.
5	In the**Dest** box, type **0::0**.
6	In the **PrefixLength** box, type **0**.
7	In the **NextHop** box, select the router that leads to the specified route.
8	In the **IfIndex** box, click **Port** or **VLAN** and select an option.
9	Click **Insert**.

The default route record is created in the static routing table.

--End--

Enabling OSPF on a router

When you configure an interface for the OSPF protocol, you must first enable OSPF globally on the router and then assign an IPv6 address.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **OSPF**.
3	In the **AdminStat** option box, select **enabled** to activate OSPF, or select **disabled** to deactivate OSPF.
4	Click **Apply**.
	The OSPF protocol is enabled (or disabled) on this router.
5	Click Yes to confirm the forced SPF run.
	The router performs the SPF run and the OSPF link state database is updated.

ATTENTION
After initiating an SPF run, wait 10 seconds before you initiate another SPF run.

--End--

Variable definitions

Use the data in the following table to configure OSPF.

Variable	Value
RouterID	Identifies the router independent of other routers in the OSPF domain. The IPv6 Router ID uses the same format as an IPv4 address.
AdminStat	The administrative status of OSPF in the router. The value enabled activates OSPF on at least one interface; disabled deactivates OSPF on all interfaces. The default is disabled.
VersionNumber	Current version number of OSPF.

Variable	Value
AreaBdrRtrStatus	A read-only flag identifying this router as an area border router (ABR). **ATTENTION** The AreaBdrRtrStatus value must be true to create a virtual router interface.
ASBdrRtrStatus	When you select the ASBdrRtrStatus option, the router is configured as an autonomous system boundary router (ASBR). The default is false.
AsScopeLsaCount	A read-only field displaying the number of external (LS type 5) link-state advertisements in the link-state database.
AsScopeLsaCksumSum	A read-only field displaying the 32-bit unsigned sum of the LS checksums of the external link-state advertisements in the link-state database. This sum determines changes and compares the link-state databases of two routers.
OriginateNewLsas	A read-only field displaying the number of new link-state advertisements. The number is incremented each time the router originates a new LSA.
RxNewLsas	A read-only field displaying the number of new link-state advertisements received. This number does not include new instantiations of self-originated link-state advertisements.
ExtLsaCount	A read-only field displaying the number of external LSAs (LS type 0x4005) in the link-state database.
ExtAreaLsdLimit	The maximum number of nondefault AS-external LSAs entries stored in the link-state database (LSDB). If the value is -1,no limit exists. The default is -1. You must configure the ExtAreaLsdbLimit to the same value for all routers attached to the OSPFv3 backbone or any regular OSPFv3 area (that is, exclude OSPFv3 stub areas and NSSAs).

Variable	Value
MulticastExtentions	A bit mask indicating whether the router is forwarding IPv6 multicast datagrams based on the algorithms defined in the multicast extensions to OSPF. Possible forwarding includes: • intraAreaMulticast forwards to directly attached areas (called intra-area multicast routing) • interAreaMulticast forwards between OSPFv3 areas (called inter-area multicast routing) • interAsMulticast forwards between autonomous systems (called inter-AS multicast routing) By default, all bits are cleared.
ExitOverflowInterval	The number of seconds after entering the overflow state, that a router attempts to leave the overflow state. The router resends nondefault AS-external-LSAs. When the value is configured to 0, the router does not leave the overflow state until the router restarts. The default value is 4294967295.
DemandExtentions	The router support for demand routing. The default value is disabled.
TrafficEngineeringSupport	The router support for traffic engineering extensions. The default value is disabled.
ReferenceBandwidth	The reference bandwidth in kilobits per second for calculating default interface metrics. The default value is 100 000 Kbps (100 Mb/s).
RestartSupport	The router support for OSPF hitless restart. Options include no restart support, only planned restarts, or both planned and unplanned restarts. Options include: • none (default) • plannedOnly • plannedAndUnplanned
RestartStatus	A read-only field indicating the current status of OSPF hitless restart: • notRestarting (default) • plannedRestart • unplannedRestart

Variable	Value
RestartInterval	The configured OSPF hitless restart timeout interval in the range 1–1800 seconds. The default is 1800.
RestartAge	A read-only field indicating the remaining time in the current OSPF hitless restart interval in seconds. The range is 1–1800.
RestartExitReason	A read-only field indicating the outcome of the last attempt at a hitless restart. Options include the following: • none indicates no restart was attempted. • inProgress indicates a restart attempt is currently underway. • completed indicates a completed restart. • timedout indicates a timed-out restart. • topologyChanged indicates a cancelled restart due to topology change. The default is none.

Creating OSPF port interfaces

You configure an OSPF interface, or link, on an IP interface. In the Nortel Ethernet Routing Switch 8600, an IP interface is either a single link (brouter port) or a logical interface configured on a VLAN (multiple ports). The underlying lower level protocols and the routing protocol itself obtain the state information associated with the interface.

When you enable an OSPF interface, you designate the interface as one of the following types:

- broadcast (active)
- nonbroadcast multiaccess (NBMA)
- point-to-point
- point-to-multipoint

> **ATTENTION**
> When you enable an OSPF interface, you cannot change the interface type. You must first disable the interface. After you disable the interface, you can change the type and reenable it. On NMBA interfaces, you must also delete all manually configured neighbors before you change the type.

Prerequisites

- Before you can configure the OSPF protocol on a router interface, you must first enable OSPF globally on the router and assign an IPv6 address to the interface.

Procedure steps

Step	Action
1	In the Device Physical View tab, select the port to configure.
2	In the navigation tree, open the following folders: **Configuration, Edit, Port**.
3	Double-click **IPv6**.
4	Select the **IPv6 OSPF Interface** tab.
5	Click **Insert**.
6	In the **AreaId** box, click the ellipsis (...) button to select the ID.
7	In the **Type** box, select the type of OSPF interface you want to create: **broadcast**, **nbma**, **pointToPoint** or **pointToMultipoint**.
8	In the **AdminState** box, select **enabled**.
9	In the **RtrPriority** box, modify the value if required.
10	In the **TransitDelay**, **RetransitInterval**, **HelloInterval**, **RtrDeadInterval**, and **PollInterval** boxes, modify values as required.
11	In the **Metric Value** box, type the metric value for a demand for an instance.
12	In the **InstId** box, type the instance ID.
13	Click **Insert**.
14	On the Interfaces tab, click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure an OSPF port interface.

Variable	Value
Index	The interface index of this OSPFv3 interface. The index corresponds to the interface index of the IPv6 interface where OSPFv3 is configured.

Variable	Value
AreaId	Dotted decimal value to designate the OSPF area name. VLANs maintaining the default area setting on the interface cause the LSDB to be inconsistent. **ATTENTION** The area name is not related to an IPv6 address. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).
Type	Type of OSPF interface (broadcast, nbma, point-to-point, or point-to-multipoint).
AdminStat	Current administrative state of the OSPF interface (enabled or disabled).
Rtrpriority	OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become the designated router or the backup. The priority is used only during election of the designated router and backup designated router. The range is 0–255. The default is 1.
TransitDelay	Length of time, in seconds (1–1800), required to transmit an LSA update packet over the interface. The default value is 1.
RetransInterval	Length of time, in seconds (1–1800), required between LSA retransmissions. The default value is 5.
HelloInterval	Length of time, in seconds, between hello packets. This value must be the same for all routers attached to a common network. The default is 10 seconds. **ATTENTION** When you change the Hello interval values, you must save the configuration file and reboot the switch for the values to be restored and checked for consistency.

Variable	Value
RtrDeadInterval	Adjacent routers use this interval to determine if the router is removed from the network. The interval must be identical on all routers on the subnet and a minimum of four times the hello interval. To avoid interpretability issues, the RtrDeadInterval value for the OSPF interface must match the RtrDeadInterval value for the OSPF virtual interface. The default is 40 seconds.
PollInterval	Length of time, in seconds, between hello packets sent to an inactive OSPF router. The default value is 120.
State	A read-only field indicating the OSPFv3 interface state. Options include: • down • loopback • waiting • pointToPoint • designatedRouter • backupDesignatedRouter • otherDesignatedRouter
DesignatedRouter	A read-only field indicating the router ID of the designated router.
BackupDesignatedRouter	A read-only field indicating the router ID of the backup designated router.
Events	A read-only field indicating the number of times this OSPF interface changed state or an error occurred.
MetricValue	The metric assigned to this interface. The default metric value is the reference bandwidth or ifSpeed. The value of the reference bandwidth is configured by the rcOspfv3ReferenceBandwidth object.
LinkScopeLsaCount	A read-only field indicating the number of Link-Scope link-state advertisements in the link-state database.
LinkLsaChksumSum	A read-only field indicating the 32-bit unsigned sum of the Link-Scope link-state advertisement LS checksums in the link-state database. The sum determines a change in the router link-state database and compares the link-state database of two routers.

Creating OSPF VLAN interfaces

You configure an OSPF interface, or link, on an IP interface. In the Nortel Ethernet Routing Switch 8600, an IP interface is either a single link (brouter port) or a logical interface configured on a VLAN (multiple ports). The underlying low level protocols and the routing protocol itself obtain the state information associated with the interface.

When you enable an OSPF interface, you designate the interface as one of the following types:

- broadcast (active)
- nonbroadcast multiaccess (NBMA)
- point-to-point
- point-to-multipoint

> **ATTENTION**
> When you enable an OSPF interface, you cannot change the interface type. You must first disable the interface. After you disable the interface, you can change the type and reenable it. On NMBA interfaces, you must also delete all manually configured neighbors before you change the type.

Prerequisites

- Before you can configure the OSPF protocol on a router interface, you must first enable OSPF globally on the router and assign an IPv6 address to the interface.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, VLAN**.
2	Double-click **VLANs**.
3	In the Basic tab, select the VLAN for which to configure an OSPF interface.
4	Click **IPv6**.
5	Click the **IPv6 OSPF Interface** tab.
6	Click **Insert**.
7	In the **AreaId** box, click the ellipsis (...) button to select the ID.
8	In the **Type** box, select the type of OSPF interface to create: **broadcast**, **nbma**, **pointToPoint**, or **pointToMultipoint**.
9	In the **AdminState** box, select **enabled**.
10	In the **RtrPriority** box, modify the value if required.

11 In the **TransitDelay**, **RetransitInterval**, **HelloInterval**, **RtrDeadInterval**, and **PollInterval** boxes, modify values as required.

12 In the **Metric Value** box, type the metric value for a demand for an instance.

13 In the **InstId** box, type the instance ID.

14 Click **Insert**.

15 On the Interfaces tab, click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure an OSPF VLAN interface.

Variable	Value
Index	The interface index of this OSPFv3 interface. The index corresponds to the interface index of the IPv6 interface where OSPFv3 is configured.
AreaId	Dotted decimal value to designate the OSPF area name. VLANs maintaining the default area setting on the interface cause the LSDB to be inconsistent. **ATTENTION** The area name is not related to an IPv6 address. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).
Type	Type of OSPF interface (broadcast, nbma, point-to-point, or point-to-multipoint).
AdminStat	Current administrative state of the OSPF interface (enabled or disabled).
Rtrpriority	OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become the designated router or the backup. The priority is used only during election of the designated router and backup designated router. The range is 0—255. The default is 1.

Variable	Value
TransitDelay	Length of time, in seconds (1—1800), required to transmit an LSA update packet over the interface. The default value is 1.
RetransInterval	Length of time, in seconds (1—1800), required between LSA retransmissions. The default value is 5.
HelloInterval	Length of time, in seconds, between hello packets. This value must be the same for all routers attached to a common network. The default is 10 seconds. **ATTENTION** When you change the Hello interval values, you must save the configuration file and reboot the switch for the values to be restored and checked for consistency.
RtrDeadInterval	Adjacent routers use this interval to determine if the router is removed from the network. The interval must be identical on all routers on the subnet and a minimum of four times the Hello Interval. To avoid interpretability issues, the RtrDeadInterval value for the OSPF interface must match with the RtrDeadInterval value for the OSPF virtual interface. The default is 40 seconds.
PollInterval	Length of time, in seconds, between hello packets sent to an inactive OSPF router. The default value is 120.
State	A read-only field indicating the OSPFv3 interface state: • down • loopback • waiting • pointToPoint • designatedRouter • backupDesignatedRouter • otherDesignatedRouter
DesignatedRouter	A read-only field indicating the router ID of the designated router.
BackupDesignatedRouter	A read-only field indicating the router ID of the backup designated router.

Variable	Value
Events	A read-only field indicating the number of times this OSPF interface changed state or an error occurred.
MetricValue	The metric assigned to this interface. The default value of the metric is the reference bandwidth or ifSpeed. The value of the reference bandwidth is configured by the rcOspfv3ReferenceBandwidth object.
LinkScopeLsaCount	A read-only field indicating the number of Link-Scope link-state advertisements in the link-state database.
LinkLsaChksumSum	A read-only field indicating the 32-bit unsigned sum of the Link-Scope link-state advertisement LS checksums in the link-state database. The sum determines a change in the router link-state database and compares the link-state database of two routers.
InstId	Enables multiple instances of OSPFv3 over a single link. The switch assigns each protocol instance a separate ID. This ID is significant for local links only. The default is 0.

Adding NBMA neighbors

In contrast to a broadcast network where switches multicast (send to AllSPFRouters and AllDRouters) certain OSPF protocol packets, switches replicate and send NBMA packets to each neighboring router as unicast. NBMA networks drop all OSPF packets with destination addresses AllSPFRouters and AllDRouters. Because the NBMA network does not broadcast, you must manually configure a list of neighbors and priorities for all routers in the network that can become the designated router (DR). Potential DRs use a positive nonzero router priority.

An NMBA interface with a positive nonzero router priority is eligible to become the DR for the NBMA network and is configured with the identification of all attached routers, IPv6 addresses, and router priorities.

Prerequisites

- Before you begin this configuration, identify the following:
  - — specific interfaces to include in the NBMA network
  - — the IPv6 address for each interface
  - — the router priority for each interface
  - — the HelloInterval for the network

— the RtrDeadInterval for the network

— the PollInterval for the network

After you gather the information, you can configure the interfaces and add neighbors for each interface that is eligible to become the DR.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Interfaces** tab.
4	Select an NBMA interface with a positive nonzero router priority.
5	Click the **NBMA Neighbors** tab.
6	Click **Insert**.
7	In the **IfIndex** box, click **Port** or **VLAN**, and select the required interface.
8	In the **Address** box, type the IPv6 address for the first neighbor.
9	In the **Priority** box, type the priority for the neighbor.
10	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure an OSPF NBMA neighbor.

Variable	Value
IfIndex	The local link ID of the link over which the neighbor can be reached
Address	The IPv6 address of the neighbor associated with the local link.
Priority	The priority of this neighbor in the designated router election algorithm. The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network.

Variable	Value
RtrId	A 32-bit integer (represented as a type IpAddress) uniquely identifying the neighboring router in the Autonomous System. A value of 0.0.0.0 is returned until a Hello is received from the configured neighbor.
State	The State of the relationship with this Neighbor.

Creating OSPF areas

A stub area does not receive advertisements for external routes, which reduces the size of the link-state database. A stub area uses only one area border router. Any packets destined for outside the area are routed to the area border exit point, examined by the area border router, and forwarded to a destination.

A not so stubby area (NSSA) prevents the flooding of AS-External link-state advertisements into the area by replacing them with a default route. NSSAs also import small stub (non-OSPF) routing domains into OSPF.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Areas** tab.
4	Click **Insert**.
5	Type the required values.
6	Click **Insert**.
7	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the OSPF area.

Variable	Value
Id	A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone. VLANs with the default area setting on the interface cause LSDB inconsistency.
ImportAsExtern	The area support for importing AS-external link-state advertisements. Options include importExternal (default), importNotExternal, or importNssa (not so stubby area).
SpfRuns	Indicates the number of SPF calculations OSPF performs.
BdrRtrCount	The number of area border routers reachable within this area. The switch calculates the value, initially zero, in each SPF pass.
AsBdrRtrCount	The number of autonomous system border routers reachable within this area. The switch calculates the value, initially zero, in each SPF pass.
ScopeLsaCount	The number of link-state advertisements in the area link-state database, excluding AS External LSAs.
ScopeLsaCksumSum	The 32-bit unsigned sum of the link-state advertisements. This sum excludes external (LS type-5) link-state advertisements. The sum determines changes in a router link-state database and compares the link-state databases of two routers.
Summary	The area support for summary advertisements in a stub area. The default value is sendAreaSummary.
StubMetric	The number of active interfaces in this area. The default value is 10.
NssaTranslatorRole	Indicates an NSSA border router ability to translate NSSA type-7 LSAs into type-5 LSAs: • always (default) • candidate

Variable	Value
NssaTranslatorState	Indicates if and how an NSSA border router translates NSSA type-7 LSAs into type-5 LSAs: • enabled indicates the NSSA border router translator role is configured to always. • elected indicates a candidate NSSA border router is translating type-7 LSAs into type-5. • disabled indicates a candidate NSSA border router is not translating type-7 LSAs into type-5.
NssaTranslatorStabilityInterval	The number of seconds after an elected translator determines translation is not required that it resumes translation duties. The default value is 40.
NssaTranslatorEvents	A read-only field indicating the number of translator state changes since the last startup.
StubMetricType	Configures the type of metric advertised as a default route: • ospfv3Metric indicates the OSPF metric • comparableCost indicates an external type 1 • nonComparable indicates and external type 2 The default value is ospfv3Metric.

Creating a virtual link

When you use OSPF, an Ethernet Routing Switch 8600 that functions as an ABR must connect directly to the backbone. If the switch does not directly connect, it requires a virtual link. In an Ethernet Routing Switch 8600, you can automatically create virtual links or you can manually configure a virtual link.

Virtual linking is similar to backup redundancy. With virtual linking configured, the switch creates a virtual link for vital traffic paths in your OSPF configuration if traffic is interrupted, such as when an interface cable providing connection to the backbone (either directly or indirectly) is disconnected from the switch. Automatic virtual linking ensures that a link is created by using another switch.

If automatic virtual linking requires more resources than you want to expend, create manual virtual links. Manual virtual links conserve resources and provide specific control over virtual link placement in your OSPF configuration.

OSPF behavior is modified according to OSPF standards so that OSPF routes cannot be learned through an ABR unless it connects to the backbone or through a virtual link.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Virtual If** tab.
4	Click **Insert**.
5	In the **AreaId** box, specify the area ID for the transit area. The transit area is the common area between two ABRs.
6	In the **Neighbor** box, specify the neighbor ID. The neighbor ID is the IP router ID of the ABR through which the other ABR must route traffic destined for the backbone.
7	Click **Insert**.
8	To verify that the virtual link is active, refresh the Virtual If tab and check the **State** column. If the state is point-to-point, the virtual link is active. If the state is down, the virtual link is configured incorrectly.

--End--

Variable definitions

Use the data in the following table to configure the virtual link.

Variable	Value
AreaId	A read-only field indicating the transit area ID that the virtual link traverses.
Neighbor	A read-only field indicating the router ID of the virtual neighbor.
TransitDelay	The estimated number of seconds required to transmit a link-state update packet over this interface. The range is 1–1800 and the default is 1 second.

Variable	Value
RetransInterval	The number of seconds between link-state advertisement, and retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting the database description and the link-state request packets. This value must exceed the expected round- trip time. The range is 1–1800 and the default is 5 seconds.
HelloInterval	The length of time, in seconds, between the hello packets that the router sends on the interface. This value must be the same for the virtual neighbor. The default value is 10 seconds.
RtrDeadInterval	The number of seconds during which router hello packets are not received before neighbors declare the router down. Use a multiple of the hello interval. You must configure this same value on the virtual neighbor. The default value is 60 seconds.
State	OSPF virtual interface states.
Events	The number of state changes or error events on this virtual link
LinkScopeLsaCount	The total number of Link-Scope link-state advertisements in this virtual link's link-state database.
LinkLsaCksumSum	The 32-bit unsigned sum of the Link-Scope link-state advertisements' LS checksums contained in this virtual link's link-state database. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers.

Specifying ASBRs

Autonomous system boundary routers (ASBR) advertise non-OSPF routes into OSPF domains, communicating routes throughout the OSPF routing domain. A router can function as an ASBR if you connect one or more interfaces to a non-OSPF network (for example, RIP or BGP).

To conserve resources, or to specifically control which routers perform as ASBRs, you can limit the number of ASBRs on your network.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **OSPF**.

3 Select the **ASBdrRtrStatus** box to designate the router as an ASBR.

OR

Clear the box to remove ASBR status from the router.

4 Click **Apply**.

--End--

Inserting OSPF area aggregate ranges

Configure an area address range on the OSPF router to reduce the number of ABR advertisements into other OSPF areas. An area address range is an implied contiguous range of area network addresses for which the ABR advertises a single summary route.

You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Area Aggregate** tab.
4	Click **Insert**.
5	In the **AreaId** box, click the ellipsis button (**...**) to select the required area ID of the aggregate address.
6	In the **AreaLsdbType** box, select the required option: • interAreaPrefixLsa: to generate an aggregated summary • nssaExternalLink: to generate an NSSA link summary
7	In the **Prefix** box, type the prefix of the area IPv6 address.
8	In the **Prefix Length** box, type the number of bits you want to advertise from the IPv6 address.
9	In the **Effect** box, select the required option: • advertiseMatching: to advertise the aggregate summary LSA with the same link-state ID • doNotAdvertiseMatching: to suppress all networks that fall within the entire range

10 In the **AdvertiseMetric** box, type a cost value (in the range 0 to 65535) to advertise for the OSPF area range.

11 Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the IPv6 OSPF area aggregate.

Variable	Value
AreaID	Specifies the address of an OSPF area. Use dotted decimal notation to specify the area name.
AreaLsdbType	Specifies the LSA type.
Prefix	Specifies the IPv6 address range of an OSPF area.
PrefixLength	Specifies the prefix length value for this address.
Effect	Specifies the area range advertise mode as advertise or no-advertise. The default value is advertiseMatching.
AdvertiseMetric	Specifies the advertise metric value in the range 0 to 65535.

Configuring route redistribution

You can configure a redistribute entry for OSPF to announce routes of a certain source type, such as static, RIP, or direct. If you do not configure a route policy field for a redistribute entry, the switch uses the default action on the basis of metric, metric-type, and subnet. The default action is called basic redistribution. Otherwise, the specified route policy performs detailed redistribution. If you do not configure a redistribution entry, the switch generates no external LSA for non-OSPF routes.

ATTENTION
Changing OSPF redistribute contexts is a process-oriented operation that can affect system performance and network reachability. Nortel recommends that you change default preferences for an OSPF redistribute context before you enable the protocols.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Redistribute** tab. The Redistribute tab appears.
4	Click **Insert**.
5	Modify options as required.
6	Click **Insert**.
7	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the route redistribution.

Variable	Value
DstVrfId	Specifies the ID of the destination virtual router and forwarder (VRF).
Protocol	Specifies any one of the dynamic routing protocols, which is interested in receiving the external routing info.
SrcVrfId	Specifies the ID of the source VRF.
RouteSource	Select the route source protocol for the redistribution entry.
Enable	Enable (or disable) an OSPF redistribution entry for a specified source type. You can also enable or disable this feature in the OSPF Redistribute tab of the Policy dialog box by clicking in the field and selecting enable or disable from the menu.

IPv6 routing configuration using the CLI

This chapter contains procedures to configure IPv6 static routes and the Open Shortest Path First version 3 (OSPFv3) protocol.

IPv6 routing configuration navigation

Job aid: Roadmap of IPv6 static route and OSPFv3 CLI commands

The following table lists the commands and parameters that you use to perform the procedures in this section.

Table 10
Job aid: Roadmap of IPv6 static route and OSPFv3 CLI commands

<table>
<tr><th>Command</th><th>Parameter</th></tr>
<tr><td rowspan="11">config ethernet <ports> ipv6 ospf</td><td>info</td></tr>
<tr><td>admin-status <enable|disable></td></tr>
<tr><td>create <area> {priority <value>] [metric <value>] [retransmit-interval <value>] [transit-delay <value>] [hello-interval <value>] [dead-interval <value>] [type <value>]</td></tr>
<tr><td>delete</td></tr>
<tr><td>hello-interval <seconds></td></tr>
<tr><td>dead-interval <seconds></td></tr>
<tr><td>poll-interval <seconds></td></tr>
<tr><td>metric <metric></td></tr>
<tr><td>priority <priority></td></tr>
<tr><td>retransmit-interval <seconds></td></tr>
<tr><td>transit-delay <seconds></td></tr>
<tr><td rowspan="4">config ethernet <ports> ipv6 ospf nbma-nbr <ipv6address></td><td>info</td></tr>
<tr><td>create <priority></td></tr>
<tr><td>delete</td></tr>
<tr><td>priority <priority></td></tr>
<tr><td rowspan="5">config ipv6 ospf</td><td>info</td></tr>
<tr><td>disable</td></tr>
<tr><td>enable</td></tr>
<tr><td>as-boundary-router <enable|disable></td></tr>
<tr><td>router-id <RTR_ADDR></td></tr>
<tr><td rowspan="7">config ipv6 ospf area <ipaddr></td><td>info</td></tr>
<tr><td>create [<type>] [stub-metric <value>] [translator-role <value>]</td></tr>
<tr><td>delete</td></tr>
<tr><td>import-summaries <true|false></td></tr>
<tr><td>nssa <true|false></td></tr>
<tr><td>stub <true|false></td></tr>
<tr><td>stub-metric <cost></td></tr>
</table>

Table 10
Job aid: Roadmap of IPv6 static route and OSPFv3 CLI commands (cont'd.)

Command	Parameter
`config ipv6 ospf area <ipaddr> range <ipv6addr-prefix>`	`info`
	`advertise-metric <cost> lsa-type <value>`
	`advertise-mode <advertise|no-advertise>`
	`delete lsa-type <value>`
	`create advertise-mode <value> lsa-type <value> [advertise-metric <value>]`
`config ip ospf area <ipv6addr> virtual-interface <ipv6addr>`	`info`
	`create`
	`dead-interval <seconds>`
	`delete`
	`hello-interval <seconds>`
	`retransmit-interval <seconds>`
	`transit-delay <seconds>`
`config ipv6 ospf redistribute direct`	`info`
	`disable`
	`enable`
`config ipv6 ospf redistribute static`	`info`
	`disable`
	`enable`
`config ipv6 static-route`	`info`
	`create <ipv6addr-prefix> cost <value> [next-hop <value>] port <value> [vlan <value>] [tunnel <value>] [preference <value>]`
	`delete <ipv6addr-prefix> [next-hop <value>] [port <value>] [vlan <value>] [tunnel <value>]`
	`disable <ipv6addr-prefix> [next-hop <value>] [port <value>] [vlan <value>] [tunnel <value>]`
	`enable <ipv6addr-prefix> [next-hop <value>] [port <value>] [vlan <value>] [tunnel <value>]`

Table 10
Job aid: Roadmap of IPv6 static route and OSPFv3 CLI commands (cont'd.)

Command	Parameter
	preference <preference> <ipv6addr-prefix> [next-hop <value>] [port <value>] [vlan <value>] [tunnel <value>]
config vlan <vid> ipv6 ospf	info
	admin-status <enable|disable>
	create <area> [priority <value>] [metric <value>] [retransmit-interval <value>] [transit-delay <value>]
	delete
	hello-interval <seconds>
	dead-interval <seconds>
	poll-interval <seconds>
	metric <metric>
	priority <priority>
	retransmit-interval <seconds>
	transit-delay <seconds>
config vlan <vid> ipv6 ospf nbma-nbr <ipv6address>	info
	create <priority>
	delete
	priority <priority>

Configuring IPv6 static routes

Configure IPv6 static routes to change static routes directly with the IPv6 static routing table manager. Create a new static route or modify existing static route parameters.

Procedure steps

Step	Action
1	Configure static routes by using the following command:

```
config ipv6 static-route
```

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 static-route** command.

Variable	Value
`create <ipv6addr-prefix> cost <value> [next-hop <value> ] port <value> [vlan <value> ] [tunnel <value> ] [preference <value> ]`	Adds a static or default route to the switch. • **ipv6addr-prefix** is the IP address and prefix for the route destination as a string 0–46 characters. • **cost <value>** is the metric of the route in the range of 1–65535. • **next-hop <value>** is the IP address of the next-hop router; the next router at which packets must arrive on this route. The string length is 0–46 characters. • **port <value>** is the slot/port number. • **vlan <value>** is the VLAN ID in the range of 1–4094. • **tunnel <value>** configures the tunnel ID in the range of 1–2147477248. • **preference <value>** configures the preference value in the range of 1–255.
`delete <ipv6addr-prefix> [next-hop <value> ] [port <value> ] [vlan <value> ] [tunnel <value> ]`	Deletes a static route. • **ipv6addr-prefix** is the IP address and prefix for the route destination as a string 0–46 characters. • **next-hop <value>** is the IP address of the next-hop router-- the next router at which packets must arrive on this route. The string length is 0–46 characters. • **port <value>** is the slot/port number. • **vlan <value>** is the VLAN ID in the range of 1–4094. • **tunnel <value>** is the tunnel ID value in the range 1–2147477248. When you select a tunnel, you must provide the VLAN, port, and next hop. You must configure an IPv6 tunnel before entering this value.

Variable	Value
disable <ipv6addr-prefix> [next-hop <value>] [port <value>] [vlan <value>] [tunnel <value>]	Disables a static route. • **ipv6addr-prefix** is the IP address and prefix for the route destination as a string 0–46 characters. • **next-hop <value>** is the IP address of the next hop router; the next router at which packets must arrive on this route. The string length is 0–46 characters. • **port <value>** is the slot/port number. • **vlan <value>** is the VLAN ID in the range of 1–4094. • **tunnel <value>** is the tunnel ID value in the range of 1-5000. When you select a tunnel, you must provide the VLAN, port, and next hop. You must configure an IPv6 tunnel first.
enable <ipv6addr-prefix> [next-hop <value>] [port <value>] [vlan <value>] [tunnel <value>]	Enables a static route. • **ipv6addr-prefix** is the IP address and prefix for the route destination as a string 0–46 characters. • **next-hop <value>** is the IP address of the next-hop router–the next router at which packets must arrive on this route. The string length is 0–46 characters. • **port <value>** is the slot/port number. • **vlan <value>** is the VLAN ID in the range of 1–4094. • **tunnel <value>** is the tunnel ID value in the range of 1–2147477248. When you select a tunnel, you must provide the VLAN, port, and next hop. You must configure an IPv6 tunnel first.

Variable	Value
`info`	Displays characteristics of the created static route.
`preference <preference> <ipv6addr-prefix> [next-hop <value> ] [port <value> ] [vlan <value> ] [tunnel <value> ]`	Modifies static route preference. • **`preference`** configures the route preference in the range of 1–255. • **`ipv6addr-prefix`** is the IP address and prefix for the route destination as a string 0–46 characters. • **`next-hop <value>`** is the IP address of the next-hop router–the next router at which packets must arrive on this route. The string length is 0–46 characters. • **`port <value>`** is the slot/port number. • **`vlan <value>`** is the VLAN ID in the range of 1–4094. • **`tunnel <value>`** is the tunnel ID value in the range of 1-5000. When you select a tunnel, you must provide the VLAN, port, and next hop. You must configure an IPv6 tunnel before you enter this value. **ATTENTION** A black hole route is a route with an invalid next hop, so the switch drops data packets destined to this network. When you specify a route preference, be sure that you configure the preference value appropriately so that when the black hole route is used, it is elected as the best route.

Configuring OSPF global parameters

Configure Open Shortest Path First (OSPF) version 3 global parameters to affect OSPF routing on the entire switch. Routers use the OSPFv3 protocol to exchange network topology information, providing each router with a map of the network.

Procedure steps

Step	Action
1	Configure OSPFv3 by using the following command:

```
config ipv6 ospf
```

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 ospf** command.

Variable	Value
as-boundary-router <enable|disable>	Enables or disables the OSPF Autonomous System boundary router. The default is disable.
disable	Globally disables OSPF on the switch.
enable	Globally enables OSPF on the switch.
info	Displays the current OSPF configuration on the switch.
router-id <RTR_ADDR>	Configures the OSPF router ID IPv4 address. **<RTR_ADDR>** is the IPv4 address in dotted decimal format {a.b.c.d}.

Configuring OSPF areas

OSPF supports hierarchical routing by dividing the Autonomous System into different areas. When two or more areas exist, the backbone area (area 0.0.0.0) must always be present.

You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).

Procedure steps

Step	Action
1	Configure an OSPF area by using the following command: **config ipv6 ospf area <ipaddr>**

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 ospf area** command.

Variable	Value
create [<type>] [stub-metric <value>] [translator-role <value>]	Creates an OSPF area. • **type** is the type of area (**stub** or **nssa**). • **stub-metric <value>** is the cost from 0–16777215. This is the metric value applied at the indicated type of service. • **translator-role <value>** is either 1 for always or 2 for candidate.
delete	Deletes an OSPF area.
import-summaries <true|false>	Configures the area support for importing summary advertisements into a stub area. Use this entry only if the stub area is configured to true.
info	Displays OSPF area characteristics.
ipaddr	Specifies the address of an OSPF area. Use dotted decimal notation to specify the area name.
nssa <true|false>	Configures a not so stubby area (true or false). An NSSA prevents flooding of normal route advertisements into the area by replacing them with a default route.
stub <true|false>	Configures the import external option for this area to be stub or not {true|false}. A stub area uses only one exit point (router interface) out of the area.
stub-metric <cost>	Stub default metric for this stub area. **cost** is the range from 0–16777215. This is the metric value applied at the indicated type of service.

Configuring OSPF area ranges

Configure an area address range on the OSPF router to reduce the number of ABR advertisements into other OSPF areas. An area address range is an implied contiguous range of area network addresses for which the ABR advertises a single summary route.

You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).

Procedure steps

Step	Action
1	Configure an OSPF area range by using the following command: **config ipv6 ospf area <ipaddr> range <ipv6addr-prefix>**

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 ospf area range** command.

Variable	Value
advertise-metric <cost> lsa-type <value>	Specifies the advertise metric value and LSA type. • **cost** is the advertise metric vlaue in the range 0–65535. • **value** is the LSA type as either **inter-area-prefix-link** or **nssa-extlink**.
advertise-mode <advertise|no-advertise>	Specifies the area range advertise mode as **advertise** or **no-advertise**.
delete lsa-type <value>	Deletes an LSA type. • **value** is the LSA type as either **inter-area-prefix-link** or **nssa-link**.
create advertise-mode <value> lsa-type <value> [advertise-metric <value>]	Creates an advertise mode for a range of IPv6 area addresses. • **create advertise-mode <value>** is **advertise** or **no-advertise**. • **lsa-type <value> value** is the LSA type as either **inter-area-prefix-link** or **nssa-extlink**. • **advertise-metric <value>** is the advertise metric 0–65535.
info	Displays OSPF range characteristics.

Variable	Value
ipaddr	Specifies the address of an OSPF area. Use dotted decimal notation to specify the area name.
ipv6addr-prefix	Configures the IPv6 address range of an OSPF area. The string length is 0–255 characters.

Configuring OSPF area virtual interfaces

If a remote OSPF ABR uses no connection to the backbone area but needs to be part of the same routing domain (AS) in which the switch resides, configure an OSPFv3 virtual interface to the ABR.

You can use any value for the OSPFv3 area name (for example, 1.1.1.1 or 200.200.200.200).

> **ATTENTION**
> OSPFv3 behavior is modified according to OSPFv3 standards so that OSPFv3 routes cannot be learned through an area border router (ABR) unless the router connects to the backbone or through a virtual link.

Procedure steps

Step	Action
1	Configure an OSPFv3 area virtual interface by using the following command: **config ipv6 ospf area <ipaddr> virtual-interface <ipaddr>**

--End--

Variable definitions

Use the data in the following table to use the **config ip ospf area virtual-interface** command.

Variable	Value
create	Creates a virtual interface for an area.
dead-interval <seconds>	Specifies the dead interval, in seconds, as a range 1–4095.
delete	Deletes a virtual interface for an area.

Variable	Value
hello-interval <seconds>	Specifies the hello interval, in seconds, at which hello packets send between switches for a virtual interface in an OSPF area. The range is 1–65535.
info	Displays OSPF virtual interface characteristics.
ipaddr	Specifies the address of an OSPF area. Use dotted decimal notation to specify the area name.
retransmit-interval <seconds>	Configures the retransmit interval for the OSPF interface, the number of seconds between link-state advertisement retransmissions. **seconds** is an integer between 1–1800.
transit-delay <seconds>	Configures the transit delay time for the OSPF interface, the estimated time in seconds it takes to transmit a link-state update packet over the interface. **seconds** is an integer between 1–1800.

Configuring OSPF direct redistribution

Enable or disable direct redistribution to obtain information about redistributing IPv6 direct routes into an OSPFv3 routing domain.

Procedure steps

Step	Action
1	Configure OSPF direct redistribution by using the following command: **config ipv6 ospf redistribute direct**

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 ospf redistribute direct** command.

Variable	Value
`disable`	Disables an OSPF direct redistribution policy. The default value is disable.
`enable`	Enables an OSPF direct redistribution policy.
`info`	Displays information about the OSPF direct redistribution policy settings.

Configuring OSPF static redistribution

Enable or disable static redistribution to obtain information about redistributing IPv6 static routes into an OSPFv3 routing domain.

Procedure steps

Step	Action
1	Configure OSPF static redistribution by using the following command: **`config ipv6 ospf redistribute static`**

--End--

Variable definitions

Use the data in the following table to use the **`config ipv6 ospf redistribute static`** command.

Variable	Value
`disable`	Disables an OSPF static redistribution policy. The default value is disable.
`enable`	Enables an OSPF static redistribution policy.
`info`	Displays information about the OSPF static redistribution policy settings.

Configuring port-based OSPF parameters

Configure port-based OSPFv3 parameters to customize your OSPF IPv6 configuration.

ATTENTION
Both sides of the OSPF connection must use the same authentication type and key.

Procedure steps

Step	Action
1	Configure port-based OSPF by using the following command: **`config ethernet <ports> ipv6 ospf`**

--End--

Variable definitions

Use the data in the following table to use the **`config ethernet ipv6 ospf`** command.

Variable	Value
`admin-status <enable|disable>`	Configures the state (enabled or disabled) of the OSPF interface.
`create <area> [priority <value> ] [metric <value> ] [retransmit-interval <value> ] [transit-delay <value> ] [hello-interval <value> ] [dead-interval <value> ] [type <value> ]`	Creates an OSPF interface. • **`<area>`** is the area ID (0–2147483647) or area IP address (0.0.0.0 to 255.255.255.255) {a.b.c.d}. • **`priority <value>`** is the priority in the range 0–255. • **`metric <value>`** is the metric in the range 0–65535. • **`retransmit-interval <value>`** is the retransmit interval in the range 1–1800 seconds. • **`transit-delay <value>`** is the transit delay in the range 1–1800 seconds. • **`hello-interval <value>`** is the hello interval in the range 1–65535 seconds. • **`dead-interval <value>`** is the dead interval in the range 0–4095 seconds. • **`type <st|nbma|p2p|p2mp>`** is the type of interface where 1 is ethernet, 2 is nbma, 3 is p2p, 4 is lookback, and 5 is p2mp.

Variable	Value
`dead-interval <seconds>`	Configures the OSPF dead interval for the interface. `seconds` is the number of seconds the switch OSPF neighbors wait before determining that this OSPF router is down. The range is from 1–4095. This value must be at least four times the Hello interval value. The default is 40.
`delete`	Deletes an OSPF interface.
`hello-interval <seconds>`	Configures the OSPF hello interval for the interface. `seconds` is the number of seconds between hello packets sent on this interface. The range is 1–65535. The default is 10. **ATTENTION** When you change the hello interval values, you must save the configuration file and restart the switch to restore the values and check for consistency.
`info`	Displays OSPF characteristics on the port.
`metric <metric>`	Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. `metric` is the range 0–65535.
`poll-interval <seconds>`	Configures the polling interval for the OSPF interface in seconds. `seconds` is 0–214783674.
`ports`	Specifies the port or range of ports you configure in the format slot/port.

Variable	Value
`priority <priority>`	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The range is 0–255. The default is 1.
`retransmit-interval <seconds>`	Configures the retransmit interval for the OSPF interface; the number of seconds between link-state advertisement retransmissions. `seconds` is an integer 1–1800.
`transit-delay <seconds>`	Configures the transit delay time for the OSPF interface, the estimated time, in seconds, required to transmit a link-state update packet over the interface. `seconds` is an integer 1–1800.

Configuring port-based OSPF neighbor parameters

Configure port-based OSPFv3 neighbor parameters for specified ports to customize your OSPF IPv6 configuration.

> **ATTENTION**
> Both sides of the OSPF connection must use the same authentication type and key.

Procedure steps

Step	Action
1	Configure port-base OSPF neighbor parameters by using the following command: **`config ethernet <ports> ipv6 ospf nbma-nbr <ipv6address>`**

ATTENTION
You must use an IPv6 link-local address as an NBMA neighbor.

--End--

Variable definitions

Use the data in the following table to use the **config ethernet ipv6 ospf nbma-nbr** command.

Variable	Value
create <priority>	Creates a neighbor priority. The range is 0–255. The default is 1.
delete	Deletes an OSPF NBMA neighbor.
info	Displays OSPF characteristics on the port.
ipv6address	Specifies the IPv6 address of the neighbor as a string of 0–43.
ports	Specifies the port or range of ports to configure in the format slot/port.
priority <priority>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The range is 0–255. The default is 1.

Configuring OSPF parameters for a VLAN

Configure OSPFv3 parameters for a specified VLAN to customize your OSPF IPv6 configuration.

Procedure steps

Step	Action
1	Configure OSPF parameters for a VLAN by using the following command: **config vlan <vid> ipv6 ospf**

--End--

Variable definitions

Use the data in the following table to use the **config vlan ipv6 ospf** command.

Variable	Value
admin-status <enable|disable>	Configures the state (enabled or disabled) of the OSPF interface.
create <area> [priority <value>] [metric <value>] [retransmit-interval <value>] [transit-delay <value>] [hello-interval <value>] [dead-interval <value>] [type <value>]	Creates an OSPF interface. • **<area>** is the area IP address (0.0.0.0 to 255.255.255.255) {a.b.c.d}. • **priority <value>** is the priority in the range 0–255. • **metric <value>** is the metric in the range 0–65535. • **retransmit-interval <value>** is the retransmit interval in the range 1–1800 seconds. • **transit-delay <value>** is the transit delay in the range 1–1800 seconds. • **hello-interval <value>** is the hello interval in the range 1–65535 seconds. • **dead-interval <value>** is the dead interval in the range 1–4095 seconds. • **type <st|nbma|p2p|p2mp>** is the type of interface where 1 is ethernet, 2 is nbma, 3 is p2p, 4 is lookback, and 5 is p2mp.
dead-interval <seconds>	Configures the OSPF dead interval for the interface. **seconds** is the number of seconds the switch OSPF neighbors wait before determining that this OSPF router is down. The range is 1–4095. This value must be at least four times the hello interval value. The default is 40.
delete	Deletes an OSPF interface.

Variable	Value
hello-interval <seconds>	Configures the OSPF hello interval for the interface. **seconds** is the number of seconds between hello packets sent on this interface. The range is 1–65535. The default is 10. **ATTENTION** When you change the hello interval values, you must save the configuration file and reboot the switch to restore the values and check for consistency.
info	Displays OSPF characteristics on the VLAN.
metric <metric>	Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. **metric** is the range 0–65535.
poll-interval <seconds>	Configures the polling interval for the OSPF interface in seconds. **seconds** is 0–2147483647.
priority <priority>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. **priority** is in the range 0–255. The default is 1.
retransmit-interval <seconds>	Configures the retransmit interval for the OSPF interface; the number of seconds between link-state advertisement retransmissions. **seconds** is an integer from 1–1800.

Variable	Value
`transit-delay <seconds>`	Configures the transit delay time for the OSPF interface, the estimated time, in seconds, required to transmit a link-state update packet over the interface. `seconds` is an integer from 1–1800.
`vid`	Specifies a unique integer value in the range 1–4094 that identifies the VLAN to configure.

Configuring OSPF neighbor parameters for a VLAN

Configure port-based OSPFv3 neighbor parameters for a VLAN to customize your OSPF IPv6 configuration.

> **ATTENTION**
> Both sides of the OSPF connection must use the same authentication type and key.

Procedure steps

Step	Action
1	Configure OSPF neighbor parameters for a VLAN by using the following command: **`config vlan <vid> ipv6 ospf nbma-nbr <ipv6address>`**

--End--

Variable definitions

Use the data in the following table to use the **`config vlan ipv6 ospf nbma-nbr`** command.

Variable	Value
`create <priority>`	Creates a neighbor priority. `priority` is in the range 0–255. The default is 1.
`delete`	Deletes an OSPF NBMA neighbor.
`info`	Displays OSPF characteristics on the port.
`ipv6address`	Specifies the IPv6 address of the neighbor as a string of 0–43 characters.

Variable	Value
priority <priority>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. **priority** is in the range 0–255. The default is 1.
vid	Specifies a unique integer value in the range 1–4094 that identifies the VLAN to configure.

IPv6 routing configuration using the NNCLI

This chapter contains procedures to configure IPv6 static routes and the Open Shortest Path First version 3 (OSPFv3) protocol.

IPv6 routing configuration navigation

Job aid: Roadmap of IPv6 static route and OSPFv3 NNCLI commands

The following table lists the commands and parameters that you use to perform the procedures in this section.

Table 11
Job aid: Roadmap of IPv6 static route and OSPFv3 NNCLI commands

Command	Parameter
Global Configuration mode	
`ipv6 route <Ipv6 address/prefix>`	`enable [next-hop <Ipv6 address/prefix>] [port <slot/port>] [tunnel <tunnel-id>] [vlan <vlan id>]`
	`cost <1-65535>`
	`preference <1-255>`
`router ospf ipv6-enable`	
Interface Configuration mode	
`ipv6 ospf`	`area <A.B.C.D> enable`
	`cost <metric>`
	`dead-interval <seconds>`
	`hello-interval <seconds>`
	`poll-interval <seconds>`
	`priority <value>`
	`retransmit-interval <seconds>`
	`transmit-delay <seconds>`
`ipv6 ospf nbma-nbr <Ipv6address/prefix-len> priority <priority>`	
OSPF Router Configuration mode	
`ipv6`	`as-boundary-router enable`
	`router-id <A.B.C.D>`
`ipv6 area <A.B.C.D>`	`default-cost <cost>`
	`import <value>`
	`import-summaries enable`
	`translator-role <value>`
	`type <nssa|stub>`
`ipv6 ipv6 area range <Ipv6 address/prefix> <A.B.C.D>`	`inter-area-prefix-link advertise-mode <advertise|not-advertise> advertise-mode <advertise|not-advertise> advertise-metric <0–65535>`
	`nssa-extlink advertise-metric <0-65535>`

Table 11
Job aid: Roadmap of IPv6 static route and OSPFv3 NNCLI commands (cont'd.)

Command	Parameter
ipv6 area virtual-link <area IP address> <virtual link IP address>	dead-interval <seconds>
	hello-interval <seconds>
	retransmit-interval <seconds>
	transit-delay <seconds>
ipv6 redistribute	direct enable
	static enable

Configuring IPv6 static routes

Configure IPv6 static routes to change static routes directly with the IPv6 static routing table manager. Create a new static route or modify existing static route parameters.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create the static route by using the following command: **ipv6 route <Ipv6 address/prefix> enable [next-hop <Ipv6 address/prefix>] [port <slot/port>] [tunnel <tunnel-id>] [vlan <vlan id>]**
2	Assign the cost by using the following command: **ipv6 route <Ipv6 address/prefix> cost <1-65535>**
3	Configure the preference by using the following command: **ipv6 route <Ipv6 address/prefix> preference <1-255>**

--End--

Variable definitions

Use the data in the following table to use the **ipv6 route** command.

Variable	Value
cost <1-65535>	cost <value> is the metric of the route in the range of 1–65535.

Variable	Value
enable [next-hop <Ipv6 address/prefix>] [port <slot/port>] [tunnel <tunnel-id>] [vlan <vlan id>]	Adds a static or default route to the switch. • **ipv6address/prefix** is the IP address and prefix for the route destination as a string of 0–46 characters. • **next-hop <value>** is the IP address of the next-hop router—the next router at which packets must arrive on this route. The string length is 0–46 characters. When creating a black hole static route, set this field to 255.255.255.255 as the IP address of the router through which the specified route is accessible. • **port <value>** is the slot/port number. • **vlan <value>** is the VLAN ID in the range of 1–4094. • **tunnel <value>** configures the tunnel ID in the range of 1-5000.
preference <preference> <ipv6addr-prefix> [next-hop <value>] [port <value>] [vlan <value>] [tunnel <value>]	Modifies static route preference. • **preference** configures the route preference in the range of 1–255. The default value is 0. • **ipv6addr-prefix** is the IP address and prefix for the route destination as a string 0–46 characters. • **next-hop <value>** is the IP address of the next-hop router—the next router at which packets must arrive on this route. The string length is 0–46 characters. • **port <value>** is the slot/port number. • **vlan <value>** is the VLAN ID in the range of 1–4094. • **tunnel <value>** is the tunnel ID value in the range of 1-5000. When you select a tunnel, you must provide the VLAN, port, and next hop. You must configure an IPv6 tunnel before you enter this value. **ATTENTION** A black hole route is a route with an invalid next hop, so the switch drops data packets destined to this network. When you specify a route preference, be sure that you configure the preference value appropriately so that

Variable	Value
	when you use the black-hole route, it is elected as the best route.

Configuring OSPF global parameters

Configure Open Shortest Path First (OSPF) global parameters to affect OSPF routing on the entire switch. Routers use the OSPF protocol to exchange network topology information, providing each router with a map of the network.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Enable OSPF for IPv6 by using the following command: `router ospf ipv6-enable`
2	Log on to the OSPF Router configuration mode by using the following command: `router ospf`
3	Enable the OSPF autonomous system boundary router by using the following command: `ipv6 as-boundary-router enable`
4	Configure the OSPF router ID by using the following command: `ipv6 router-id <A.B.C.D>`

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 router-id`** command.

Variable	Value
`router-id <A.B.C.D>`	Configures the OSPF router ID IPv6 address.

Configuring OSPF areas

OSPF supports hierarchical routing by dividing the Autonomous System into different areas. When two or more areas exist, the backbone area (area 0.0.0.0) must always be present.

You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).

Prerequisites

- You must log on to the OSPF Router Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create and configure an OSPF area by using the following command: **`ipv6 area <A.B.C.D> default-cost <cost> import <value> [import-summaries enable] translator-role <value> type <nssa|stub>`**

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 area`** command.

Variable	Value
`default-cost <cost>`	Stub default metric for this stub area. **`cost`** is the range from 0 to 16777215. This is the metric value applied at the indicated type of service. To configure this option to the default value, use the **`default`** operator with the command. The default value is 10.

Variable	Value
import <value>	Configures the area support for importing advertisements. The options are: • external—Stub and nssa are both false • noexternal—Configure the area as stub area • nssa—Configure the area as nssa To configure this option to the default value, use the **default** operator with the command. The default value is external.
import-summaries enable	Configures the area support for importing summary advertisements into a stub area. Use this entry only for a stub area. To configure this option to the default value, use the **default** operator with the command. The default value is true.
translator-role <value>	Indicates an NSSA Border router ability to perform translation of type-7 LSAs into type-5 LSAs. Valid values are 1 (always) or 2 (candidate). Default value is 1 (always).
type <nssa|stub>	Configures the type of area. An NSSA prevents flooding of normal route advertisements into the area by replacing them with a default route. A stub area uses only one exit point (router interface) from the area. By default, the area is neither a stub area or an NSSA.

Configuring OSPF area ranges

Configure an area address range on the OSPF router to reduce the number of ABR advertisements into other OSPF areas. An area address range is an implied contiguous range of area network addresses for which the ABR advertises a single summary route.

Configure the area by using one of the two LSA types: inter-area-prefix -link or nssa-extlink.

You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).

Prerequisites

- You must log on to the OSPF Router Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure an OSPF area range by using the following command: **`ipv6 area range <A.B.C.D> <Ipv6 address/prefix> <inter-area-prefix-link|nssa-extlink> advertise-mode <advertise|not-advertise>] advertise-metric <0-65535>`**

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 area range`** command.

Variable	Value
`A.B.C.D`	Specifies the IP address of the area.
`advertise-metric <0-65535>`	Specifies the advertise metric value and LSA type. The default value is 0.
`advertise-mode <advertise|no-advertise>`	Specifies the area range advertise mode as **`advertise`** or **`no-advertise`**. The default value is advertise.
`ipv6addrress/prefix`	Configures the IPv6 address range of an OSPF area. The string length is 0–255 characters.

Configuring OSPF area virtual interfaces

If a remote OSPF ABR uses no connection to the backbone area but needs to be part of the same routing domain (AS) in which the switch resides, configure an OSPF virtual interface to the ABR.

You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200).

> **ATTENTION**
> OSPF behavior is modified according to OSPF standards so that OSPF routes cannot be learned through an area border router (ABR) unless the router connects to the backbone or through a virtual link.

Prerequisites

- You must log on to the OSPF Router Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure an OSPF area virtual interface by using the following command: **`ipv6 area virtual-link <area IP address> <virtual link IP address> dead-interval <seconds> hello-interval <seconds> retransmit-interval <seconds> transit-delay <seconds>`**

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 area virtual-link`** command.

Variable	Value
`dead-interval <seconds>`	Specifies the dead interval, in seconds, as a range 1–4 095. To configure this option to the default value, use the **`default`** operator with the command. The default value is 60.
`hello-interval <seconds>`	Specifies the Hello interval, in seconds, sent between switches for a virtual interface in an OSPF area. The range is 1–65535. To configure this option to the default value, use the **`default`** operator with the command. The default value is 10.

Variable	Value
retransmit-interval <seconds>	Specifies the retransmit interval, in seconds, sent between switches for a virtual interface in an OSPF area. The range is 1–1800. To configure this option to the default value, use the **default** operator with the command. The default value is 5.
transit-delay <seconds>	Specifies the transit delay interval, in seconds, sent between switches for a virtual interface in an OSPF area. The range is 1–1800. To configure this option to the default value, use the **default** operator with the command. The default value is 1.

Configuring an OSPF interface

Configure an OSPF interface for designated router (DR) and backup designated router (BDR) election to reduce the amount of routing traffic.

Prerequisites

- Before you can configure OSPF parameters on an interface, you must first configure IP on the interface.
- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Associate the interface with an OSPF area with the following command: **ipv6 ospf area <A.B.C.D>**
2	Enable OSPF on the interface by using the following command: **ipv6 ospf enable**
3	Configure the OSPF area by using the following command: **ipv6 ospf area <A.B.C.D> cost <metric> [dead-interval <seconds>] [hello-interval <seconds>] [network <value>] [priority <value>] [retransmit-interval <seconds>] [transit-delay <seconds>]**
4	Enable an OSPF area on an interface by using the following command: **ipv6 ospf area <A.B.C.D>**

5 Configure the interface by using the following command:

`ipv6 ospf cost <metric> [priority <value>]`

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 ospf`** command.

Variable	Value
`area <A.B.C.D>`	Specifies the area IP address (0.0.0.0 to 255.255.255.255) {a.b.c.d}.
`cost <metric>`	Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. **`metric`** is the range 0–65535. To configure this option to the default value, use the **`default`** operator with the command. The default value is 1.
`dead-interval <seconds>`	Configures the OSPF dead interval for the interface. **`seconds`** is the number of seconds the switch OSPF neighbors wait before determining that this OSPF router is down. The range is from 1-4095. This value must be at least four times the Hello interval value. The default is 40. To configure this option to the default value, use the **`default`** operator with the command.
`hello-interval <seconds>`	Configures the OSPF hello interval for the interface. **`seconds`** is the number of seconds between hello packets sent on this interface. The range is 1–65535. The default is 10. **ATTENTION** When you change the hello interval values, you must save the configuration file and

Variable	Value
	reboot the switch for the values to be restored and checked for consistency. To configure this option to the default value, use the **default** operator with the command.
network <value>	Configures the type of interface: • eth: broadcast • nbma: NBMA • p2mp: point-to-multipoint • p2p: point-to-point
poll-interval <seconds>	Configures the polling interval for the OSPF interface in seconds. **seconds** is 0–2147483647. To configure this option to the default value, use the **default** operator with the command. The default value is 120.
priority <value>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. **value** is in the range 0–255. The default is 1. To set this option to the default value, use the **default** operator with the command.
retransmit-interval <seconds>	Configures the retransmit interval for the OSPF interface; the number of seconds between link-state advertisement retransmissions. **seconds** is an integer from 1–1 800. To configure this option to the default value, use the **default** operator with the command.

Variable	Value
	The default value is 5.
transit-delay <seconds>	Configures the transit delay time for the OSPF interface, the estimated time in seconds it takes to transmit a link-state update packet over the interface. **seconds** is an integer from 1–1 800. To configure this option to the default value, use the **default** operator with the command. The default value is 1.

Configuring OSPF direct redistribution

Enable or disable direct redistribution to redistribute IPv6 direct routes into an OSPFv3 routing domain.

Prerequisites

- You must log on to the OSPF Router Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure OSPF direct redistribution by using the following command: **ipv6 redistribute direct enable**

--End--

Configuring OSPF static redistribution

Enable or disable static redistribution to redistribute IPv6 static routes into an OSPFv3 routing domain.

Prerequisites

- You must log on to the OSPF Router Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure OSPF static redistribution by using the following command: **ipv6 redistribute static enable**

--End--

Configuring port-based OSPF neighbor parameters

Configure port-based OSPFv3 neighbor parameters for specified ports to customize your OSPF IPv6 configuration.

> **ATTENTION**
> Both sides of the OSPF connection must use the same authentication type and key.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure port-based OSPF neighbor parameters by using the following command: **ipv6 ospf nbma-nbr <Ipv6address/prefix-len> priority <priority>** **ATTENTION** You must use an IPv6 link-local address as an NBMA neighbor.

--End--

Variable definitions

Use the data in the following table to use the **ipv6 ospf nbma-nbr** command.

Variable	Value
Ipv6address/prefix-len	Specifies the IPv6 address of the neighbor as a string of 0–43 characters.
priority <priority>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. The range is 0 to 255. The default is 1. To configure this option to the default value, use the **default** operator with the command.

Configuring OSPF parameters for a VLAN

Configure OSPFv3 parameters for a specified VLAN to customize your OSPF IPv6 configuration.

Prerequisites

- You must log on to the VLAN Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Associate the OSPF area with an interface by using the following command: **ipv6 ospf area <A.B.C.D>**
2	Enable OSPF on the interface with the following command: **ipv6 ospf enable**
3	Configure the area by using the following command: **ipv6 ospf area <A.B.C.D> cost <metric> [dead-interval <seconds>] [hello-interval <seconds>] [network <value>] [priority <value>] [retransmit-interval <seconds>] [transmit-delay <seconds>]**
4	Configure the interface by using the following command:

ipv6 ospf cost <metric> [priority <value>]

--End--

Variable definitions

Use the data in the following table to use the **ipv6 ospf** command.

Variable	Value
area <A.B.C.D>	Specifies the area IP address (0.0.0.0 to 255.255.255.255) {a.b.c.d}.
cost <metric>	Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements. **metric** is the range 0–65535. To configure this option to the default value, use the **default** operator with the command. The default value is 1.
dead-interval <seconds>	Configures the OSPF dead interval for the interface. **seconds** is the number of seconds the switch OSPF neighbors wait before determining that this OSPF router is down. The range is from 1-4095. This value must be at least four times the Hello interval value. The default is 40. To configure this option to the default value, use the **default** operator with the command.
hello-interval <seconds>	Configures the OSPF hello interval for the interface. **seconds** is the number of seconds between hello packets sent on this interface. The range is 1–65 535. The default is 10. **ATTENTION** When you change the hello interval values, you must save the configuration file and restart the switch to restore the values and check for consistency. To configure this option to the default value, use the **default** operator with the command.

Variable	Value
network <value>	Configures the type of interface: • eth—broadcast • nbma—NBMA • p2mp—point-to-multipoint • p2p—point-to-point
poll-interval <seconds>	Configures the polling interval for the OSPF interface in seconds. **seconds** is from 0–2147483647. To configure this option to the default value, use the **default** operator with the command. The default value is 120.
priority <value>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. **value** is in the range 0–255. The default is 1. To configure this option to the default value, use the **default** operator with the command.
retransmit-interval <seconds>	Configures the retransmit interval for the OSPF interface; the number of seconds between link-state advertisement retransmissions. **seconds** is an integer from 1–1800. To configure this option to the default value, use the **default** operator with the command. The default value is 5.
transit-delay <seconds>	Configures the transit delay time for the OSPF interface, the estimated time in seconds it takes to transmit a link-state update packet over the interface. **seconds** is an integer from 1–1800.

Variable	Value
	To configure this option to the default value, use the **default** operator with the command. The default value is 1.

Configuring OSPF neighbor parameters for a VLAN

Configure port-based OSPFv3 neighbor parameters for a VLAN to customize your OSPF IPv6 configuration.

> **ATTENTION**
> Both sides of the OSPF connection must use the same authentication type and key.

Prerequisites

- You must log on to the VLAN Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure OSPF neighbor parameters for a VLAN by using the following command: **ipv6 ospf nbma-nbr <Ipv6address/prefix-len> priority <priority>**

--End--

Variable definitions

Use the data in the following table to use the **ipv6 ospf nbma-nbr** command.

Variable	Value
Ipv6address/prefix-len	Specifies the IPv6 address of the neighbor as a string of 0–43.
priority <priority>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the

Variable	Value
	designated router or a backup. The priority is used only during election of the designated router and backup designated router. The range is 0–255. The default is 1. To configure this option to the default value, use the **`default`** operator with the command.

IPv6 DHCP Relay configuration using Enterprise Device Manager

Use the Forward Path tab to configure the DHCP Relay forward path, and use the Interface tab to configure the related parameters (for example, max hops and remote ID).

DHCP configuration navigation

Configuring the DHCP relay forwarding path

Configure forwarding policies to indicate the relay agent and the DHCP server to which packets are forwarded.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **DHCP Relay**.
3	Click the **Forward Path** tab.
4	Click **Insert**.
5	In the **AgentAddr** box, type the agent address.
6	In the **ServerAddr** box, type the server address.
7	Click **Enabled** to enable DHCP relay. You can enable or disable each agent server forwarding path. The default is enabled.

8	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the DHCP Relay forward path.

Variable	Value
AgentAddr	The IP address of the input interface (agent) on which the DHCP request packets are received for forwarding. This address is the IP address of either a brouter port or a VLAN for which forwarding is enabled.
ServerAddr	This parameter is the IP address of the DHCP server. The request is unicast to the server address.
Enable	Enables DHCP relay on the routing switch.

Configuring DHCP relay interface parameters

Configure the DHCP relay behavior on the interface.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **DHCP Relay**.
3	In the Interface tab, click **Insert**.
4	Enter the appropriate values.
5	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the DCHP Relay interface parameters.

Variable	Value
IfIndex	A read-only value indicating the unique value to identify an IPv6 interface. For the brouter port, it is the ifindex of the port and, in the case of the VLAN, it is the ifindex of the VLAN.

Variable	Value
MaxHop	Specifies the maximum number of hops a DHCP packet can take from the DHCP client to the DHCP server.
RemoteIdEnabled	Enables or disables remote ID.
DhcpEnabled	Specifies whether DHCP is enabled or disabled on the interface.

Viewing DHCP Relay statistics

View DHCP Relay statistics to monitor network performance.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **DHCP Relay**.
3	In the Interface tab, select an interface and click **Statistics**.

--End--

Variable definitions

Use the data in the following table to use the DHCP Relay Statistics tab.

Variable	Value
NumRequests	The count of request messages.
NumReplies	The count of reply messages.

IPv6 DHCP Relay configuration using the CLI

Dynamic Host Configuration Protocol (DHCP) provides host configuration information to the workstations dynamically. Use the DHCP relay commands to set DHCP relay behavior on a port or on a VLAN.

This section describes the CLI commands for IPv6 DHCP Relay configuration functions in the Ethernet Routing Switch 8600.

To configure DHCP Relay, you can use the **`config ipv6 dhcp-relay`** command, which allows you to specify the IP address of the port or VLAN to use as a relay agent, or use the **`config {vlan <vid> | ethernet <ports>} ipv6 dhcp-relay`** command to explicitly specify the port or VLAN to use as the relay agent.

IPv6 DHCP relay configuration navigation

- "Job aid: Roadmap of IPv6 DHCP Relay CLI commands" (page 215)
- "Configuring an IPv6 DHCP relay interface" (page 216)
- "Configuring IPv6 DHCP relay on a port or VLAN" (page 218)
- "Showing IPv6 DHCP relay information" (page 219)
- "Showing IPv6 DHCP relay information for a port or VLAN" (page 220)

Job aid: Roadmap of IPv6 DHCP Relay CLI commands

The following table lists the IPv6 DHCP Relay commands and their parameters that you use to complete the procedures in this section.

Table 12
IPv6 DHCP Relay configuration commands

Command	Parameter
`config ipv6 dhcp-relay`	`info`

Table 12
IPv6 DHCP Relay configuration commands (cont'd.)

Command	Parameter
	`create-fwd-path agent <value> server <value> [state <value>]`
	`delete-fwd-path agent <value> server <value>`
	`disable-fwd-path agent <value> server <value>`
	`enable-fwd-path agent <value> server <value>`
`config {ethernet <ports> | vlan <vlan-id>} ipv6 dhcp-relay`	`info`
	`create-fwd-path server <value> [state <value>]`
	`delete-fwd-path server <value>`
	`disable`
	`disable-fwd-path server <value>`
	`enable`
	`enable-fwd-path server <value>`
	`max-hop <max-hop>`
	`remote-id {enable|disable}`
`show ipv6 dhcp-relay fwd-path`	
`show ipv6 dhcp-relay counters`	
`show vlan info dhcp-relay`	
`show ports info dhcp-relay [vlan <vid>] [port <value>]`	

Configuring an IPv6 DHCP relay interface

Configure an IPv6 DHCP relay interface.

Procedure steps

Step	Action
1	Configure DHCP parameters globally with the following command: **`config ipv6 dhcp-relay`**

2 Confirm your configuration with the following command:
config ipv6 dhcp-relay info

--End--

Variable definitions

Use the data in the following table to use the following commands:

- **config ipv6 dhcp-relay**

Variable	Value
create-fwd-path agent <value> server <value> [state <value>]	Configures the forwarding path from the client to the server. • **agent <value>** is the IPv6 address configured on an interface (a locally configured IPv6 address) that must be configured to forward or relay DHCP messages. • **server <value>** is the IPv6 address of the DHCP server in the network. • **state <value>** enables or disables the forwarding path.
delete-fwd-path agent <value> server <value>	Deletes the forwarding path from the client to the server. • **agent <value>** is the IPv6 address configured on an interface (a locally configured IPv6 address). • **server <value>** is the IPv6 address of the DHCP server in the network.
disable-fwd-path agent <value> server <value>	Disables DHCP relaying on the path from the IP address to the server. This is the default. • **agent <value>** is the IPv6 address configured on an interface (a locally configured IPv6 address). • **server <value>** is the IPv6 address of the DHCP server in the network.

Variable	Value
enable-fwd-path agent <value> server <value>	Enables DHCP relaying on the path from the IPv6 address to the server. • **agent <value>** is the IPv6 address configured on an interface (a locally configured IPv6 address). • **server <value>** is the IPv6 address of the DHCP server in the network.
info	Displays the current DHCP global configuration on the switch.

Configuring IPv6 DHCP relay on a port or VLAN

You can configure DHCP parameters on specific ports or VLANs.

Procedure steps

Step	Action
1	Configure DHCP parameters on a specified port or VLAN by using the following command: **config {vlan <vid> | ethernet <ports>} ipv6 dhcp-relay**
2	Confirm your configuration by using the following command: **config {vlan| ethernet} ipv6 dhcp-relay info**

--End--

Variable definitions

Use the data in the following table to use the **config {vlan <vid> | ethernet <ports>} ipv6 dhcp-relay** command.

Variable	Value
create-fwd-path server <value> [state <value>]	Configures the forwarding path from the client (port or VLAN) to the server. • **<value>** is the IPv6 address of the DHCP server in the network. • **state <value>** enables or disables the forwarding path.
delete-fwd-path server <value>	Deletes the forwarding path to the specified server. • **value** is the IPv6 address in the format X:X::X:X.

Variable	Value
`disable`	Disables DHCP relay on the port. This is the default state.
`disable-fwd-path server <value>`	Disables the forwarding path to the specified server. • `value` is the IPv6 address in the format X:X::X:X.
`enable`	Enables DHCP relay on the port.
`enable-fwd-path server <value>`	Enables the forwarding path server to the specified server. • `value` is the IPv6 address in the form X:X::X:X.
`info`	Displays the current DHCP configuration on the port.
`max-hop <max-hop>`	Sets the maximum number of hops before a DHCP packet is discarded (1 to 32). The default is 32.
`remote-id {enable	disable}`	Enables or disables remote ID.

Showing IPv6 DHCP relay information

Display DHCP relay information to show forward paths and counters.

Procedure steps

Step	Action
1	Display information about the DHCP relay forward path with the following command: **`show ipv6 dhcp-relay fwd-path`**
2	Display information about DHCP relay counters by using the following command: **`show ipv6 dhcp-relay counters`**

--End--

Job aid

The following table shows the field descriptions for the **`show ipv6 dhcp-relay counters`** command.

Table 13
show ip dhcp-relay command

Parameter	Description
INTERFACE	Indicates the interface IPv6 address.
REQUEST	Indicates the total number of DHCP requests received on this interface.
REPLIES	Indicates the total number of DHCP replies received on this interface.

The following table shows the field descriptions for the **show ipv6 dhcp-relay fwd-path** command.

Table 14
show ip dhcp-relay command

Parameter	Description
INTERFACE	Indicates the interface IPv6 address.
SERVER	Indicates the DHCP server IPv6 address.
ENABLE	Indicates if DHCP is enabled on the interface.

Showing IPv6 DHCP relay information for a port or VLAN

You can display the IPv6 DHCP parameters for ports or VLANs.

Procedure steps

Step	Action
1	Display the DHCP parameters for VLANs by using the following command: **show ipv6 dhcp-relay interface ports <ports>**
2	Display the DHCP parameters for ports by using the following command: **show ipv6 dhcp-relay interface vlan <vid>**

--End--

Variable definitions

Use the data in the following table to use the **show ipv6 dhcp-relay interface** command.

Variable	Value
port <ports>	The port list {slot/port[-slot/port][,...]}.
vid	The VLAN ID, which is a value from 1 to 4094.

Job aid

The following table shows the field descriptions for the **show ipv6 dhcp-relay interface vlan <vid>** command.

Table 15
show ipv6 dhcp-relay interface vlan command

Parameter	Description
VLAN ID	Indicates the VLAN ID number.

Table 15
show ipv6 dhcp-relay interface vlan command (cont'd.)

Parameter	Description
IF INDEX	Indicates the interface index number. Numbers 1 to 256 are ports; numbers above 257 are VLANs.
MAX HOP	Indicates the maximum number of hops a DHCP packet can take from the source device (DHCP client) to the destination device (DHCP server).
DHCP-RELAY	Indicates whether DHCP Relay is enabled or disabled.
REMOTE ID	Indicates whether Remote ID is enabled or disabled.

The following table shows the field descriptions for the **`show ipv6 dhcp-relay interface ports <ports>`** command.

Table 16
show ipv6 dhcp-relay interface ports command

Parameter	Description
PORT_NUM	Indicates the port number.
IF INDEX	Indicates the interface index number. Numbers 1 to 256 are ports; numbers above 257 are VLANs.
MAX HOP	Indicates the maximum number of hops a DHCP packet can take from the source device (DHCP client) to the destination device (DHCP server).
DHCP-RELAY	Indicates whether DHCP Relay is enabled or disabled.
REMOTE ID	Indicates whether Remote ID is enabled or disabled.

IPv6 DHCP Relay configuration using the NNCLI

Dynamic Host Configuration Protocol (DHCP) provides host configuration information to workstations dynamically. Use the DHCP relay commands to set DHCP relay behavior on a port or on a VLAN.

This section describes the NNCLI commands for IPv6 DHCP Relay configuration functions on the Ethernet Routing Switch 8600.

To configure DHCP Relay, you can use the **ipv6 dhcp-relay** command in Global configuration mode, which allows you to specify the IP address of the port or VLAN to use as a relay agent, or use the **ipv6 dhcp-relay** in Interface Configuration mode to first select the port or VLAN to use as the relay agent, and then specify the DHCP server and related parameters.

IPv6 DHCP configuration navigation

Job aid: Roadmap of DHCP Relay NNCLI commands

The following table lists the commands and parameters that you use to complete the IPv6 DHCP Relay procedures in this section.

Table 17
Roadmap of IPv6 DHCP Relay commands

Command	Parameter
Global Configuration mode	

Table 17
Roadmap of IPv6 DHCP Relay commands (cont'd.)

Command	Parameter
`ipv6 dhcp-relay`	`fwd-path <agent-addr> <server-addr> [enable]`
Interface Configuration Mode	
`ipv6 dhcp-relay`	`fwd-path <server-addr> [enable]`
	`max-hop <1-32>`
	`remote-id {enable	disable}`
PrivExec	
`show ipv6 dhcp-relay counters`	
`show ipv6 dhcp-relay fwd-path`	
`show ip dhcp-relay interface`	`<interface-type> <interface-id>`

Configuring IPv6 DHCP relay in Global configuration mode

In Global configuration mode, you can configure the DHCP relay forwarding path, but you cannot configure related parameters (for example, max hops or remote ID).

Prerequisites

- Access Global configuration mode.

Procedure steps

Step	Action
1	Create the forwarding path from the client to the server by using the following command: **ipv6 dhcp-relay fwd-path <agent-addr> <server-addr>**
2	Enable the forwarding path by using the following command: **ipv6 dhcp-relay fwd-path <agent-addr> <server-addr> enable**

--End--

Variable definitions

Use the data in the following table to use the preceding commands.

Variable	Value
fwd-path <agent-addr> <server-addr> [enable]	Configures the forwarding path from the client to the server. • **<agent-addr>** is the IPv6 address configured on an interface (a locally configured IPv6 address) to forward or relay DHCP. • **<server-addr>** is the IPv6 address of the DHCP server in the network. Use the **enable** operator to enable the path. Use the **no** or **default** operators to delete the forwarding path: **no ipv6 dhcp-relay fwd-path <agent-addr> <server-addr>** **default ipv6 dhcp-relay fwd-path <agent-addr> <server-addr>**
{default|no} ipv6 dhcp-relay fwd-path <agent-addr> <server-addr> enable	To disable the specified path, use the **no** or **default** operators with the **enable** option.

Configuring IPv6 DHCP relay parameters on a port or VLAN

In Interface Configuration mode, you can configure the DHCP relay forwarding path and parameters for a specified port or VLAN.

Prerequisites

- Access Interface configuration mode.

Procedure steps

Step	Action
1	Configure DHCP relay parameters on the specified port or VLAN by using the following command: **ipv6 dhcp-relay**

--End--

Variable definitions

Use the data in the following table to use the **ipv6 dhcp-relay** command.

Variable	Value
fwd-path <server-addr> [enable]	Creates a DHCP relay forwarding path. • **<server-addr>** is the server IPv6 address. Use the enable option to enable a forward path. Use the **no** or **default** operators to delete a forward path **no ip dhcp-relay fwd-path <server-addr>** **default ip dhcp-relay fwd-path <server-addr>**
max-hop <1-32>	Sets the maximum number of hops before a DHCP packet is discarded (1 to 32). The default is 32. To set this option to the default value, use the **default** operator with this command.
remote-id {enable|disable}	Enables or disables remote ID.
{default|no} ipv6 dhcp-relay fwd-path <server-addr> enable	To disable the specified path, use the **no** or **default** operators with the **enable** option.

Showing IPv6 DHCP relay information

Display relay information about DHCP relay routes and counters.

Prerequisites

- Access privExec Configuration Mode.

Procedure steps

Step	Action
1	Display information about DHCP relay forward paths by using the following command: **show ipv6 dhcp-relay fwd-path**
2	Display information about DHCP relay counters by using the following command: **show ipv6 dhcp-relay counters**
3	Display information about DHCP relay interfaces by using the following command: **show ipv6 dhcp-relay interface <interface-type> <interface-id>**

--End--

IPv6 VRRP configuration using Enterprise Device Manager

To provide fast failover of a default router for IPv6 LAN hosts, the Ethernet Routing Switch 8600 supports the Virtual Router Redundancy Protocol (VRRP v3) for IPv6. VRRP supports a virtual IPv6 address shared between two or more routers connecting the common subnet to the enterprise network. VRRPv3 for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

To configure a VRRP interface, you can either configure the interface using the **Configuration, IPv6, VRRP** path from the navigation tree, or by first selecting a port or VLAN and selecting the **IPv6, VRRP** path from there.

ATTENTION
An Ethernet Routing Switch 8600 acting as a VRRP Master does not reply to SNMP Get requests to the VRRP virtual interface address. It will, however, respond to SNMP Get requests to its physical IP address.

Prerequisites to VRRP configuration

- Assign an IPv6 address to the interface.
- Enable routing globally.
- RSMLT is not configured on the VLAN.

Navigation

- "Configuring a VRRP interface" (page 228)
- "Configuring additional addresses on the VRRP interface" (page 230)
- "Configuring VRRP notification control" (page 231)
- "Configuring VRRP on a port" (page 232)
- "Configuring VRRP on a VLAN" (page 234)

- "Viewing VRRP statistics" (page 236)
- "Viewing VRRP interface statistics" (page 238)

Configuring a VRRP interface

Use this procedure to create a VRRP interface.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **VRRP**.
3	Click the **Interface** tab.
4	Click **Insert**.
5	Complete the fields as required.
6	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure a VRRP interface.

Variable	Value
IfIndex	The index value that uniquely identifies the interface to which this entry is applicable.
InetAddrType	The address type for the VRRP interface. In this case, IPv6.
VrId	A number that uniquely identifies a virtual router on a VRRP router. The virtual router acts as the default router for one or more assigned addresses (1 to 255).
LinkLocal	The assigned IPv6 addresses that a virtual router is responsible for backing up.
VirtualMacAddr	The MAC address of the virtual router interface.

Variable	Value
State	The state of the virtual router interface: • initialize—waiting for a startup event • backup—monitoring availability and state of the master router • master—functioning as the forwarding router for the virtual router IP addresses.
Control	Displays whether VRRP is enabled or disabled for the port (or VLAN).
Priority	The priority value used by this VRRP router. Set a value from 1 to 255, where 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default is 100.
AdvInterval	The time interval (in seconds) between sending advertisement messages. The range is 1 to 255 seconds with a default of 1 second. Only the master router sends advertisements.
MasterIpAddr	The IP address of the physical interface of the master virtual router that forwards packets sent to the virtual IP addresses associated with the virtual router.
UpTime	The time interval (in hundredths of a second) since the virtual router was initialized.
CriticalIpAddr	An IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding.
CriticalIpAddrEnabled	Sets the IP interface on the local router to enable or disable the backup.
BackUpMaster	Lets you use the backup VRRP switch traffic forwarding. This reduces the traffic on the IST link. The default is disabled.
BackUpMasterState	Indicates whether the backup VRRP switch traffic forwarding is enabled or disabled.
FasterAdvIntervalEnable	Enables or disables the Fast Advertisement Interval. When disabled, the regular advertisement interval is used. The default is disable.
FasterAdvInterval	Sets the Fast Advertisement Interval between sending VRRP advertisement messages. The interval is between 200 and 1000 milliseconds, and you must enter the same value on all participating routers. The default is 200. You must enter the values in multiples of 200 milliseconds.

Variable	Value
AcceptMode	Controls whether a master router accepts packets addressed to the address owner's IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.
Action	Lists options to override the holddown timer manually and force preemption: • **none** does not override the timer • **preemptHoldDownTimer** preempts the timer
HoldDownTimer	Configures the amount of time (in seconds) to wait before preempting the current VRRP master.
HoldDownTimeRemaining	Indicates the amount of time (in seconds) left before the HoldDownTimer expires.
GlobalIPAddr	The global IPv6 address assigned to the virtual router interface.

Configuring additional addresses on the VRRP interface

Use this procedure to specify additional addresses for the VRRP interface to back up.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **VRRP**.
3	Click the **Interface** tab.
4	Select an existing VRRP interface.
5	Click **AssociatedIPAddr**. Note that you can also access the **AssociatedIPAddr** button from the Port VRRP tab (**Configuration > Edit > Port > IPv6 > VRRP**) or from the VLAN VRRP tab (**Configuration > VLANs > IPv6 > VRRP**)
6	Click **Insert**.
7	Complete the fields for the associated address.
8	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure additional VRRP addresses.

Variable	Value
IfIndex	The index value that uniquely identifies the interface to which this entry is applicable.
InetAddrType	The address type for the VRRP interface. In this case, IPv6.
VrId	A number that uniquely identifies a virtual router on a VRRP router. The virtual router acts as the default router for one or more assigned addresses (1 to 255).
IpAddr	The additional IPv6 address that the virtual router is responsible for backing up.
IpAddrPrefixLength	The IPv6 prefix length.

Configuring VRRP notification control

Use this procedure to configure VRRP notification control.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **VRRP**.
3	In the **NotificationCtrl** box, click to enable or disable notification control.
4	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure VRRP notification control.

Variable	Value
NotificationCntl	Indicates whether the VRRP-enabled router generates SNMP traps for events. • enabled—SNMP traps are generated • disabled—no SNMP traps are sent

Configuring VRRP on a port

Use this procedure to configure VRRP on a port. You can configure VRRP on a port only if the port is assigned an IP address.

Procedure steps

Step	Action
1	From the Device Physical View, select a port.
2	In the navigation tree, open the following folders: **Configuration, Edit, Port**.
3	Double-click **IPv6**.
4	Click the **VRRP** tab.
5	Click **Insert**.
6	In the **VrId** box, enter a virtual router ID.
7	Select the **AcceptMode** box if you want the master router to accept packets for which it is not the IPv6 address owner as its own.
8	In the **LinkLocal** box, enter an IPv6 address.
9	Enter an advertisement interval.
10	Specify the priority.
11	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure VRRP on a port.

Variable	Value
IfIndex	The index value that uniquely identifies the interface to which this entry is applicable.
InetAddrType	The address type for the VRRP interface. In this case, IPv6.
VrId	A number that uniquely identifies a virtual router on a VRRP router. The virtual router acts as the default router for one or more assigned addresses (1 to 255).
LinkLocal	The assigned IPv6 addresses that a virtual router is responsible for backing up.
VirtualMacAddr	The MAC address of the virtual router interface.

Variable	Value
State	The state of the virtual router interface: • initialize—waiting for a startup event • backup—monitoring availability and state of the master router • master—functioning as the forwarding router for the virtual router IP addresses.
Control	Displays whether VRRP is enabled or disabled for the port (or VLAN).
Priority	The priority value used by this VRRP router. Set a value from 1 to 255, where 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default is 100.
AdvInterval	The time interval (in seconds) between sending advertisement messages. The range is 1 to 255 seconds with a default of 1 second. Only the master router sends advertisements.
MasterIpAddr	The IP address of the physical interface of the master virtual router that forwards packets sent to the virtual IP addresses associated with the virtual router.
UpTime	The time interval (in hundredths of a second) since the virtual router was initialized.
CriticalIpAddr	An IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding.
CriticalIpAddrEnabled	Sets the IP interface on the local router to enable or disable the backup.
BackUpMaster	Lets you use the backup VRRP switch traffic forwarding. This reduces the traffic on the IST link. The default is disabled.
BackUpMasterState	Indicates whether the backup VRRP switch traffic forwarding is enabled or disabled.
FasterAdvIntervalEna ble	Enables or disables the Fast Advertisement Interval. When disabled, the regular advertisement interval is used. The default is disable.
FasterAdvInterval	Sets the Fast Advertisement Interval between sending VRRP advertisement messages. The interval is between 200 and 1000 milliseconds, and you must enter the same value on all participating routers. The default is 200. You must enter the values in multiples of 200 milliseconds.

Variable	Value
AcceptMode	Controls whether a master router accepts packets addressed to the address owner's IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.
Action	Lists options to override the holddown timer manually and force preemption: • **none** does not override the timer • **preemptHoldDownTimer** preempts the timer
HoldDownTimer	Configures the amount of time (in seconds) to wait before preempting the current VRRP master.
HoldDownTimeRemaining	Indicates the amount of time (in seconds) left before the HoldDownTimer expires.
GlobalIPAddr	The global IPv6 address assigned to the virtual router interface.

Configuring VRRP on a VLAN

Use this procedure to configure VRRP on a VLAN. You can configure VRRP on a VLAN only if the VLAN is assigned an IP address.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, VLAN**.
2	Double-click **VLANs**.
3	In the Basic tab, select a VLAN.
4	Click **IPv6**.
5	Select the **VRRP** tab.
6	Click **Insert**.
7	Edit the fields as required.
8	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to use configure VRRP on a VLAN.

Variable	Value
IfIndex	The index value that uniquely identifies the interface to which this entry is applicable.
InetAddrType	The address type for the VRRP interface. In this case, IPv6.
VrId	A number that uniquely identifies a virtual router on a VRRP router. The virtual router acts as the default router for one or more assigned addresses (1 to 255).
LinkLocal	The IP address of the virtual router interface.
VirtualMacAddr	The MAC address of the virtual router interface.
State	The state of the virtual router interface: • initialize—waiting for a startup event • backup—monitoring availability and state of the master router • master—functioning as the forwarding router for the virtual router IP addresses.
Control	Displays whether VRRP is enabled or disabled for the port or VLAN.
Priority	Priority value used by this VRRP router. The range is from 1 to 255, where 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default is 100.
AdvertisementInterval	The time interval (in seconds) between sending advertisement messages. The range is from 1 to 255 seconds with a default of 1 second. Only the master router sends advertisements.
MasterIPAddr	The IP address of the master router.
UpTime	The time interval (in hundredths of a second) since the virtual router was initialized.
CriticalIpAddr	Indicates if a user-defined critical IP address must be enabled. There is no effect if a user-defined IP address does not exist.
CriticalIpAddrEnable	Sets the IP interface on the local router to enable or disable the backup.
BackUpMaster	Lets you use the VRRP backup master switch.
BackUpMasterState	Indicates whether the backup VRRP switch traffic forwarding is enabled or disabled.
FasterAdvIntervalEnabled	Lets you use the Fast Advertisement Interval. When disabled, the regular advertisement interval is used. The default is disabled.

Variable	Value
FasterAdvInterval	Sets the Fast Advertisement Interval between sending VRRP advertisement messages. The interval can be between 200 and 1000 milliseconds, and it must be the same on all participating routers. The default is 200. Enter the values in multiples of 200 milliseconds.
Action	Use the action list to manually override the delay timer and force preemption: • preemptHoldDownTimer—preempt the timer • none—allow the timer to keep working
HoldDownTimer	The time interval (in seconds) a router is delayed for the following conditions: • The VRRP hold-down timer runs when the switch transitions from initialization to backup to master. This occurs only on a switch bootup. • The VRRP hold-down timer does not run under the following condition: In a nonbootup condition, the backup switch becomes master after the Master Downtime Interval (3 * hello interval), if the master virtual router goes down. • The VRRP hold-down timer also applies to the VRRP BackupMaster feature.
HoldDownTimeRemaining	The seconds remaining before preemption.
GlobalIPAddr	Specifies the global IPv6 address associated with the link-local VRRP IPv6 address that the virtual router backs up.

Viewing VRRP statistics

View VRRP statistics to monitor network performance.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **VRRP**.
3	Click the **Stats** tab.
	Note that you can also access a VRRP **Statistics** button from the Port VRRP tab (**Configuration > Edit > Port > IPv6 >**

VRRP) or from the VLAN VRRP tab (**Configuration > VLANs > IPv6 > VRRP**)

--End--

Variable definitions

Use the data in the following table to use the VRRP Stats tab.

Variable	Value
MasterTransitions	Specifies the total number of times that this virtual router's state has transitioned to MASTER. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime.
RcvdAdvertisements	Specifies the total number of VRRP advertisements received by this virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime.
AdvIntervalErrors	Specifies the total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
IpTtlErrors	Specifies the total number of VRRP packets received by the Virtual router with IPv4 TTL (for VRRP over IPv4) or IPv6 Hop Limit (for VRRP over IPv6) not equal to 255. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime
RcvdPriZeroPackets	Specifies the total number of VRRP packets received by the virtual router with a priority of '0'. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime.
SentPriZeroPackets	Specifies the total number of VRRP packets sent by the virtual router with a priority of '0'. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime.

Variable	Value
RcvdInvalidTypePkts	Specifies the number of VRRP packets received by the virtual router with an invalid value in the 'type' field. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime.
AddressListErrors	Specifies the total number of packets received for which the address list does not match the locally configured list for the virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime.
PacketLengthErrors	Specifies the total number of packets received with a packet length less than the length of the VRRP header. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of the DiscontinuityTime.
RcvdInvalidAuthentica tions	Specifies the total number of packets received with an unknown authentication type.

Viewing VRRP interface statistics

View VRRP interface statistics to monitor network performance.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **VRRP**.
3	Click the **Interface** tab.
4	Select an interface.
5	Click the **Statistics** button.

--End--

Variable definitions

Use the data in the following table to use the VRRP Stats tab.

Variable	Value
MasterTransitions	The total number of times that this virtual router’s state has transitioned to MASTER. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
RcdAdvertisements	The total number of VRRP advertisements received by this virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
AdvIntervalErrors	The total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
IpTtlErrors	The total number of VRRP packets received by the Virtual router with IPv4 TTL (for VRRP over IPv4) or IPv6 Hop Limit (for VRRP over IPv6) not equal to 255. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
RcvdPriZeroPackets	The total number of VRRP packets received by the virtual router with a priority of ’0’. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
SentPriZeroPackets	The total number of VRRP packets sent by the virtual router with a priority of ’0’. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
RcvdInvalidTypePkts	The number of VRRP packets received by the virtual router with an invalid value in the ’type’ field. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
AddressListErrors	The total number of packets received for which the address list does not match the locally configured list for the virtual router. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.

Variable	Value
PacketLengthErrors	The total number of packets received with a packet length less than the length of the VRRP header. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
RcvdInvalidAuthentications	The total number of packets received with an unknown authentication type.
DiscontinuityTime	The value of sysUpTime on the most recent occasion at which any one or more of this entry's counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value.
RefreshRate	The minimum reasonable polling interval for this entry. This object provides an indication of the minimum amount of time required to update the counters in this entry.

IPv6 VRRP configuration using the CLI

To provide fast failover of a default router for IPv6 LAN hosts, the Ethernet Routing Switch 8600 supports the Virtual Router Redundancy Protocol (VRRP v3) for IPv6. VRRP supports a virtual IPv6 address shared between two or more routers connecting the common subnet to the enterprise network. VRRPv3 for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

ATTENTION
An Ethernet Routing Switch 8600 acting as a VRRP Master does not reply to SNMP Get requests to the VRRP virtual interface address. It will, however, respond to SNMP Get requests to its physical IP address.

When you use the Fast Advertisement Interval option to configure a master and backup switch, you must enable the Fast Advertisement Interval option on both switches for VRRP to work correctly. If you configure one switch with the regular advertisement interval, and the other switch with the Fast Advertisement Interval, it causes an unstable state and drops advertisements.

Prerequisites to VRRP configuration

- Ensure that RSMLT is not configured on the VLAN.

Navigation

Job aid: Roadmap of IPv6 VRRP CLI commands

The following table lists the IPv6 VRRP commands and parameters that you use to perform the procedures in this section.

Table 18
Roadmap of IPv6 VRRP commands

Command	Parameter
config ethernet <ports> ipv6 vrrp <vrid>	info
	action <action_choice>
	accept-mode {enable|disable}
	address [link-local <link-local-addr>] [addr <global-addr>]
	adver-int <seconds>
	backup-master <enable|disable>
	critical-ipv6 <ipaddr>
	critical-ipv6-enable <enable|disable>
	delete [addr <addr>] [all]
	disable
	enable
	fast-adv-enable <enable|disable>
	fast-adv-int <milliseconds>
	holddown-timer <seconds>
	priority <prio>
config ipv6 vrrp	info
	send-trap <enable|disable>
config vlan <vid> ipv6 vrrp <vrid>	info
	action <action_choice>
	accept-mode {enable|disable}
	address [link-local <link-local-addr>] [addr <global-addr>]
	adver-int <seconds>
	backup-master <enable|disable>
	critical-ipv6 <ipaddr>
	critical-ipv6-enable <enable|disable>
	delete [addr <addr>] [all]

Table 18
Roadmap of IPv6 VRRP commands (cont'd.)

Command	Parameter
	`disable`
	`enable`
	`fast-adv-enable <enable|disable>`
	`fast-adv-int <milliseconds>`
	`holddown-timer <seconds>`
	`priority <prio>`
`show ipv6 vrrp`	`global-settings`
	`info [vrid <value>] [link-local <value>]`
	`show-all`
	`stats [vrid <value>] [link-local <value>]`
`clear ipv6`	`global-stats`
	`ports <ports> vrid <value>`
	`vlan <vid> vrid <value>`

Configuring VRRP on a port

Use the following procedure to configure VRRP on a port.

Procedures steps

Step	Action
1	To configure VRRP on a port, enter: **`config ethernet <ports> ipv6 vrrp <vrid>`**
2	To confirm your configuration, enter: **`config ethernet <ports> ipv6 vrrp <vrid> info`**

--End--

Variable definitions

Use the data in the following table to use the **`config ethernet <ports> ipv6 vrrp <vrid>`** command.

Variable	Value
<vrid>	A unique integer value that represents the virtual router ID in the range 1 to 255. The virtual router acts as the default router for one or more assigned addresses.
action <action_choice>	Indicates options to override the hold-down timer manually and force preemption. • **action_choice** can be set to **preempt** to preempt the timer or set to **none** to allow the timer to keep working.
accept-mode <enable|disable>	Controls whether a master router accepts packets addressed to the address owner's IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.
address [link-local <link-local-addr>] [addr <global-addr>]	Sets the IPv6 address to associate with the virtual router ID. • **<link-local-addr>** is the link-local IPv6 address. • **<global-addr>** is the global IPv6 address.
adver-int <seconds>	Sets the the time interval between sending VRRP advertisement messages. • **seconds** is between 1 and 255 seconds. The value must be the same on all participating routers. The default is 1.
backup-master <enable|disable>	Enables or disables the VRRP backup master. This option is supported only on triangular Split MultiLink Trunking (SMLT) ports. **ATTENTION** Do not enable Backup Master if Critical IP is enabled.

Variable	Value
`critical-ipv6 <ipv6addr>`	Sets the critical IPv6 address for VRRP. • `ipv6addr` is the IPv6 address on the local router, which is configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).
`critical-ipv6-enable <enable|disable>`	Enables or disables the critical IPv6 address option. **ATTENTION** Do not enable Critical IPv6 if Backup Master is enabled.
`delete [addr <addr>] [all]`	Deletes the specified VRRP address from the port.
`disable`	Disables VRRP on the port.
`enable`	Enables VRRP on the port.
`fast-adv-enable <enable|disable>`	Enables or disables the Fast Advertisement Interval. The default is disabled. • `enable` means use the Fast Advertisement Interval. • `disable` means use the regular advertisement interval.
`fast-adv-int <milliseconds>`	Sets the Fast Advertisement Interval, the time interval between sending VRRP advertisement messages. • `milliseconds` can be between 200 and 1000 milliseconds, and must be the same on all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds.

Variable	Value
holddown-timer <seconds>	Modifies the behavior of the VRRP failover mechanism by allowing the router enough time to detect the Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) routes. • **seconds** is the time interval (in seconds) a router is delayed when changing to master state.
info	Displays the current port VRRP configuration.
priority <prio>	Sets the port VRRP priority. • **prio** is the value (between 1 and 254) used by the VRRP router. The default is 100. Assign the value 255 to the router that owns the IP address associated with the virtual router.

Configuring VRRP on a VLAN

Use this procedure to configure VRRP on a VLAN.

Procedure steps

Step	Action
1	Configure VRRP on a VLAN by using the following command: **config vlan <vid> ipv6 vrrp <vrid>**
2	Confirm your configuration by using the following command: **config vlan <vid> ipv6 vrrp <vrid> info**

--End--

Variable definitions

Use the data in the following table to use the **config vlan <vid> ipv6 vrrp <vrid>** command.

Variable	Value
<vid>	The VLAN ID in the range of 1 to 4094.

Variable	Value
`<vrid>`	The virtual router ID in the range of 1 to 255, a number that uniquely identifies a virtual router on a VRRP router. The virtual router acts as the default router for one or more assigned addresses.
`action <action_choice>`	Indicates options to override the hold-down timer manually and force preemption. • `action_choice` can be set to `preempt` to preempt the timer or set to `none` to allow the timer to keep working.
`accept-mode <enable|disable>`	Controls whether a master router accepts packets addressed to the address owner's IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.
`address [link-local <link-local-addr>] [addr <global-addr>]`	Sets the IPv6 address to associate with the virtual router ID. • `<link-local-addr>` is the link-local IPv6 address. • `<global-addr>` is the global IPv6 address.
`adver-int <seconds>`	Sets the time interval (in seconds) between sending advertisement messages. • `seconds` is in the range of 1 to 255. The default is 1.
`backup-master <enable|disable>`	Enables or disables the VRRP backup master for a VLAN. This option is only supported on SMLT ports. **ATTENTION** Do not enable Backup Master if Critical IP is enabled.
`critical-ipv6-enable <enable|disable>`	Enables or disables the critical IPv6 address option. **ATTENTION** Do not enable Critical IP if Backup Master is enabled.

Variable	Value
critical-ip <ipv6addr>	Sets the critical IPv6 address for VRRP. • **ipv6addr** is the IPv6 address on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).
delete [addr <addr>] [all]	Deletes the specified VRRP address from the VLAN.
disable	Disables the VRRP on the VLAN.
enable	Enables VRRP on the VLAN.
fast-adv-enable <enable|disable>	Enables or disables the Fast Advertisement Interval. The default is disabled. • **enable** enables the Fast Advertisement Interval. • **disable** enables the Regular Advertisement Interval.
fast-adv-int <milliseconds>	Sets the time interval between sending Fast Advertisement messages. • **milliseconds** is the interval between 200 and 1000 milliseconds. This interval must be the same on all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds.
holddown-timer <seconds>	Sets the time interval (in seconds) that a router is delayed when changing to master state.
info	Displays the current VLAN VRRP settings.
priority <prio>	Sets the port VRRP priority value used by this VRRP router. • **prio** is between 1 and 254. The default is 100. Assign the value 255 to the router that owns the IP address associated with the virtual router.

Configuring global VRRP settings

Configure global VRRP settings to enable or disable SNMP traps.

Procedure steps

Step	Action
1	Configure global VRRP settings by using the following command: **`config ipv6 vrrp send-trap <enable|disable>`**
2	Confirm the configuration by using the following comman d: **`config ipv6 vrrp send-trap info`**

--End--

Showing VRRP interface information

If you enter a virtual router ID or an IP address when showing VRRP interface information, the information displays only for that virtual router ID or for that interface.

Procedure steps

Step	Action
1	To display VRRP information about the interface, enter: **`show ipv6 vrrp`** **`global-settings`** **`info [vrid <value>] [link-local <value>]`** **`show-all`** **`stats [vrid <value>] [link-local <value>]`**

--End--

Variable definitions

Use the data in the following table to use the **`show ipv6 vrrp info`** command.

Variable	Value
`global-settings`	Displays global VRRP settings.
`info`	Displays VRRP interface configurations.
`vrid <value>`	A unique integer value that represents the virtual router ID in the range 1 to 255. The virtual router acts as the default router for one or more assigned addresses.
`[link-local <value>]`	The link-local IPv6 VRRP address.

Variable	Value
show-all	Displays all VRRP output: global settings, configuration information, and statistics.
stats	Displays VRRP statistics.

Job aid

The following table describes parameters for the **show ipv6 vrrp info** command.

Parameter	Description
VRID	Indicates the virtual router ID on a VRRP router.
P/V	Indicates whether this device responds to pings directed to a virtual router IP address.
IP	Indicates the assigned IP addresses that a virtual router backs up.
MAC	Indicates the virtual MAC address of the virtual router in the format 00-00-5E-00-02-<VRID>, where the first three octets consist of the IANA OUI; the next two octets indicate the address block of the VRRP protocol; and the remaining octets consist of the VRID.
STATE	Indicates the current state of the virtual router. • initialize—waiting for a startup event • backup—monitoring the state and availability of the master router • master—forwarding IP addresses associated with this virtual router.
CONTROL	Indicates the virtual router function. Set the value to enabled to transition the state of the router from initialize to backup. Set the value to disabled to transition the router from master or backup to initialize.

Parameter	Description
PRIO	Indicates the priority for the virtual router (for example, master election) with respect to other virtual routers that are backing up one or more associated IP addresses. Higher values indicate higher priority. A priority of 0, which you cannot set, indicates that this router stopped participating in VRRP and a backup virtual router transitions to become the new master. A priority of 255 is used for the router that owns the associated IP addresses.
ADV	Indicates the advertisement interval, in milliseconds, between sending advertisement messages.
MASTER	Indicates the master router real (primary) IP address. This is the IP address listed as the source in the VRRP advertisement last received by this virtual router.
UP TIME	Indicates the time interval (in hundredths of a second) since this virtual router was initialized.
CRITICAL IP	Indicates the IP address of the interface that causes a shutdown event.
CRITICAL IP (ENABLED)	Indicates if the critical IP address is enabled.
BACKUP MASTER	Indicates the backup master IP address.
BACKUP MASTER STATE	Indicates the backup master state.
FAST ADV	Indicates the Fast Advertisement Interval, in milliseconds, between sending advertisement messages. When the Fast Advertisement Interval is enabled, the Fast Advertisement Interval is used instead of the regular advertisement interval.
FAST ADV (ENABLED)	Indicates the state of fast advertisement.
ACCEPT MODE	Controls whether a master router accepts packets addressed to the address owner’s IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.

Parameter	Description
ACTION	Specifies whether to override the holddown timer manually and force preemption. Options are none (does not override the timer) and preempt (preempts the timer).
HLD DWN	Indicates the amount of time (in seconds) to wait before preempting the current VRRP master.
REM	Remaining hold-down timer value.
GLOBAL ADDRESS	Specifies the global IPv6 address associated with the link-local VRRP IPv6 address that the virtual router backs up.

Showing VRRP information for a VLAN

Show VLAN information to display the extended VRRP configuration for all VLANs or a specified VLAN on the switch.

Procedure steps

Step	Action
1	Show the extended VRRP configuration for all VLANs on the switch or for a specified VLAN by using the following command: **show vlan info vrrp ipv6 <extended|main> [<vid>]**

--End--

Variable definitions

Use the data in the following table to use the **show vlan info vrrp ipv6** command.

Variable	Value
<main|extended>	Indicates values for extended or main VRRP configurations.
<vid>	Indicates the VLAN ID in the range of 1 to 4094.

Job aid

The following table shows the field descriptions for the **show vlan info vrrp ipv6 main**command.

Parameter	Description
VLAN ID	Indicates the VLAN ID.
VRRP ID	Indicates the virtual router ID

Parameter	Description
IPv6 ADDRESS	The IPv6 address associated with the virtual router.
VIRTUAL MAC ADDRESS	The MAC address associated with the virtual router.

The following table shows the field descriptions for the **`show vlan info vrrp ipv6 extended`**command.

Parameter	Description
VLAN ID	Indicates the VLAN ID.
VRRP ID	Indicates the virtual router ID
STATE	Indicates the current state of the virtual router. • initialize—waiting for a startup event • backup—monitoring the state or availability of the master router • master—forwarding IP addresses associated with this virtual router
CONTROL	Indicates the virtual router function. Set the value to enabled to transition the state of the router from initialize to backup. Set the value to disabled to transition the router from master or backup to initialize.
PRIORITY	Indicates the priority for the virtual router (for example, master election) with respect to other virtual routers that are backing up one or more associated IP addresses. Higher values indicates higher priority. A priority of 0, which you cannot set, indicates that this router ceased to participate in VRRP and a backup virtual router transitions to become a new master. Use a priority of 255 for the router that owns the associated IP addresses.
MASTER IPADDR	Indicates the master router real (primary) IP address. This is the IP address listed as the source in the VRRP advertisement last received by this virtual router.
ADVERTISE INTERVAL	Indicates the time interval, in seconds, between sending advertisement messages. Only the master router sends VRRP advertisements.
CRITICAL IPADDR	Indicates the IP address of the interface that causes a shutdown event.
HOLDDWN	Indicates the amount of time (in seconds) to wait before preempting the current VRRP master.

Parameter	Description
ACTION TIME	Specifies whether to override the holddown timer manually and force preemption. Options are none (does not override the timer) and preempt (preempts the timer).
CRITICAL IP ENABLE	Indicates that a user-defined critical IP address is enabled. No indicates the use of the default IP address (*::* or *0:0:0:0:0:0:0:0*).
BACKUP MASTER	Indicates the state of designating a backup master router.
BACKUP MASTER STATE	Indicates the state of the backup master router.
FAST ADV INTERVAL	Indicates the time interval, in milliseconds, between sending Fast Advertisement messages. When the Fast Advertisement Interval is enabled, the Fast Advertisement Interval is used instead of the regular advertisement interval.
FAST ADV ENABLE	Indicates the Fast Advertisement Interval status.

Clearing IPv6 VRRP statistics

Use the following procedure to clear IPv6 VRRP statistics.

Procedure steps

Step	Action
1	To clear global IPv6 VRRP statistics, enter: **`clear ipv6 vrrp`**
2	To clear IPv6 VRRP statistics on a particular port, enter: **`clear ipv6 vrrp ports <ports> vrid <value>`**
3	To clear IPv6 VRRP statistics on a particular VLAN, enter: **`clear ipv6 vrrp VLAN <vid> vrid <value>`**

--End--

Variable definitions

Use the data in the following table to use the **`clear ipv6 vrrp`** command.

Variable	Value
<ports>	Specifies the port value.
`<vid>`	Indicates the VLAN ID in the range of 1 to 4094.
`vrid <value>`	A unique integer value that represents the virtual router ID in the range 1 to 255. The virtual router acts as the default router for one or more assigned addresses.

IPv6 VRRP configuration using the NNCLI

To provide fast failover of a default router for IPv6 LAN hosts, the Ethernet Routing Switch 8600 supports the Virtual Router Redundancy Protocol (VRRP v3) for IPv6. VRRP supports a virtual IPv6 address shared between two or more routers connecting the common subnet to the enterprise network. VRRPv3 for IPv6 provides a faster switchover to an alternate default router than is possible using the ND protocol.

ATTENTION
An Ethernet Routing Switch 8600 acting as a VRRP Master does not reply to SNMP Get requests to the VRRP virtual interface address. It will, however, respond to SNMP Get requests to its physical IP address.

When you use the Fast Advertisement Interval option to configure a master and backup switch, you must enable the Fast Advertisement Interval option on both switches for VRRP to work correctly. If you configure one switch with the regular advertisement interval, and the other switch with the Fast Advertisement Interval, it causes an unstable state and drops advertisements.

VRRP configuration prerequisites

- Ensure that RSMLT is not configured on the VLAN.

Navigation

- “Job aid: Roadmap of IPv6 VRRP NNCLI commands” (page 258)
- “Configuring VRRP on a port or a VLAN” (page 259)
- “Showing VRRP interface information” (page 264)
- “Showing VRRP interface information” (page 264)
- “Clearing IPv6 VRRP statistics” (page 254)

Job aid: Roadmap of IPv6 VRRP NNCLI commands

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 19
Roadmap of IPv6 VRRP commands

Command	Parameter
FastEthernet/Gigabit Ethernet/VLAN Interface Configuration Mode	
ipv6 vrrp <1-255>	accept-mode enable
	action {none|preempt }
	adver-int <1-255>
	backup-master enable
	critical-ipv6-addr <X:X:X:X:X:X:X:X>
	critical-ipv6 enable
	enable
	fast-adv enable
	fast-adv-int <200-1000>
	holddown-timer <0-21600>
	priority <1-255>
ipv6 vrrp address <1-255>	global <X:X::X:X>/len
	link-local <fe80::X:X:X:X>
PrivExec Mode	
show ipv6 vrrp	
show ipv6 vrrp address	link-local <fe80::X:X:X:X>
	vrid <1-255>
show ipv6 vrrp interface	<port-type> [<portList>] [<1-4094>] [statistics]
	vlan [<1-4094>] [<portList>]
	verbose
	vrid <1-255>
show ipv6 vrrp statistics	link-local <fe80::X:X:X:X>
	vrid <1-255>
clear ipv6 vrrp {fastethernet <slot|port>| gigabitethernet <slot|port>| vlan <vid>} vrid <value>	

Configuring VRRP on a port or a VLAN

Use the following procedure to configure VRRP on a port or a VLAN.

Prerequisites

- Access Interface configuration mode.
- Enable IPv6 forwarding globally.
- Configure IPv6 on the interface.

Procedure steps

Step	Action
1	Configure the VRRP address on a port by using the following command: **ipv6 vrrp address <1-255> {[global <X:X:X:X:X:X:X:X>/len] [link-local <fe80::X:X:X:X>}**
2	Configure VRRP properties on a port by using the following command: **ipv6 vrrp <1-255>**
3	Enable the VRRP instance by using the following command: **ipv6 vrrp <1-255> enable**
4	Delete VRRP from the port by using the following command: **no ipv6 vrrp <1-255>**
5	Show the global VRRP settings by using the following command: **show ipv6 vrrp**

--End--

Variable definitions

Use the data in the following table to configure VRRP.

Variable	Value
{[global <X:X:X:X:X:X:X:X>/len] [link-local <fe80::X:X:X:X>}	Specifies a global or link-local (or both) IPv6 VRRP address.
accept-mode enable	Controls whether a master router accepts packets addressed to the address owner's IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.

Variable	Value
action {none|preempt}	Use the action choice option to manually override the hold-down timer and force preemption. • **none|preempt** can be set to preempt the timer or set to none to allow the timer to keep working. To set this option to the default value, use the **default** operator with this command.
adver-int <1-255>	Sets the the time interval between sending VRRP advertisement messages. The range is between 1 and 255 seconds. This value must be the same on all participating routers. The default is 1. To set this option to the default value, use the **default** operator with this command.
backup-master enable	Enables the VRRP backup master. This option is supported only on triangular Split MultiLink Trunking (SMLT) ports. Use the **no** operator to disable the VRRP backup master: **no ipv6 vrrp <1-255> backup-master enable** To set this option to the default value, use the **default** operator with this command. **ATTENTION** Do not enable Backup Master if Critical IPv6 is enabled.
critical-ipv6-addr <X:X:X:X:X:X:X:X>	Sets the critical IPv6 address for VRRP. • **X:X:X:X:X:X:X:X** is the IPv6 address on the local router, which is configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup in case the interface goes down).
critical-ipv6 enable	Enables the critical IPv6 address option. Use the **no** operator to disable the critical IPv6 address option: **no ipv6 vrrp <1-255> critical-ipv6 enable** To set this option to the default value, use the **default** operator with this command. **ATTENTION** Do not enable Critical IPv6 if Backup Master is enabled.

Variable	Value
enable	Enables VRRP on the port. Use the **no** operator to disable VRRP on the port: **no ipv6 vrrp <1-255> enable** To set this option to the default value, use the **default** operator with this command.
fast-adv enable	Enables the Fast Advertisement Interval. The default is disabled. Use the **no** operator to disable VRRP on the port: **no ipv6 vrrp <1-255> fast-adv enable** To set this option to the default value, use the **default** operator with this command.
fast-adv-int <200-1000>	Sets the Fast Advertisement Interval, the time interval between sending VRRP advertisement messages. • `200-1000` is the range in milliseconds, and must be the same on all participating routers. The default is 200. You must enter values in multiples of 200 milliseconds. To set this option to the default value, use the **default** operator with this command.
holddown-timer <0-21600>	Modifies the behavior of the VRRP failover mechanism by allowing the router enough time to detect the Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) routes. • `0-21600` is the time interval (in seconds) a router is delayed when changing to master state. To set this option to the default value, use the **default** operator with this command.
priority <1-255>	Sets the port VRRP priority. • `1-255` is the value used by the VRRP router. The default is 100. Assign the value 255 to the router that owns the IPv6 address associated with the virtual router. To set this option to the default value, use the **default** operator with this command.

Showing VRRP port or VLAN information

Display VRRP port or VLAN information to verify your configuration.

Prerequisites

- Access privExec Configuration Mode.

Procedure steps

Step	Action
1	Show the extended VRRP configuration for all VLANs on the switch or for the specified VLAN by using the following command: **show ipv6 vrrp interface** **<port-type> [<1-4094>] [<portList>]** **vlan [<1-4094>] [<portList>]** **vrid <1-255>** **[statistics]** **[verbose]**

--End--

Variable definitions

Use the data in the following table to use the **show ipv6 vrrp interface** command.

Variable	Value
<port-type> [<1-4094>] [<portList>]	Displays information by port type, and optionally by specified VLAN ID and ports.
vlan [<1-4094>] [<portList>]	Displays information by VLAN, and optionally by specified VLAN ID and ports.
vrid <1-255>	Displays information by virtual router ID.
statistics	Displays VRRP statistics for the interface.
verbose	Displays extended information.

Job aid

The following table shows the field descriptions for the **show ipv6 vrrp interface** command.

Parameter	Description
VLAN ID	Indicates the VLAN ID.
PORT NUM	Indicates the port number.
VRRP ID	Indicates the virtual router ID on a VRRP router.

Parameter	Description
IPv6 ADDRESS	Indicates the assigned IPv6 addresses that a virtual router backs up.
VIRTUAL MAC ADDRESS	Indicates the virtual MAC address of the virtual router in the format 00-00-5E-00-02-<VRID>, where the first three octets consist of the IANA OUI; the next two octets indicate the address block of the VRRP protocol; and the remaining octets consist of the VRID.

The following table shows the field descriptions for the **`show ipv6 vrrp interface verbose`**command.

Parameter	Description
VLAN ID	Indicates the VLAN ID.
PORT NUM	Indicates the port number.
VRRP ID	Indicates the virtual router ID
STATE	Indicates the current state of the virtual router. • initialize—waiting for a startup event • backup—monitoring the state or availability of the master router • master—forwarding IP addresses associated with this virtual router
CONTROL	Indicates the virtual router function. Set the value to enabled to transition the state of the router from initialize to backup. Set the value to disabled to transition the router from master or backup to initialize.
PRIORITY	Indicates the priority for the virtual router (for example, master election) with respect to other virtual routers that are backing up one or more associated IP addresses. Higher values indicates higher priority. A priority of 0, which you cannot set, indicates that this router ceased to participate in VRRP and a backup virtual router transitions to become a new master. Use a priority of 255 for the router that owns the associated IP addresses.
MASTER IPADDR	Indicates the master router real (primary) IP address. This is the IP address listed as the source in the VRRP advertisement last received by this virtual router.
ADVERTISE INTERVAL	Indicates the time interval, in seconds, between sending advertisement messages. Only the master router sends VRRP advertisements.

Parameter	Description
CRITICAL IPADDR	Indicates the IP address of the interface that causes a shutdown event.
HOLDDWN	Indicates the amount of time (in seconds) to wait before preempting the current VRRP master.
ACTION TIME	Specifies whether to override the holddown timer manually and force preemption. Options are none (does not override the timer) and preempt (preempts the timer).
CRITICAL IP ENABLE	Indicates that a user-defined critical IP address is enabled. No indicates the use of the default IP address (*::* or *0:0:0:0:0:0:0:0*).
BACKUP MASTER	Indicates the state of designating a backup master router.
BACKUP MASTER STATE	Indicates the state of the backup master router.
FAST ADV INTERVAL	Indicates the time interval, in milliseconds, between sending Fast Advertisement messages. When the Fast Advertisement Interval is enabled, the Fast Advertisement Interval is used instead of the regular advertisement interval.
FAST ADV ENABLE	Indicates the Fast Advertisement Interval status.

Showing VRRP interface information

Use this procedure to show VRRP information by IPv6 address or virtual router ID.

If you enter a virtual router ID or an IPv6 address when showing VRRP information, the information displays only for that virtual router ID or for that interface.

Prerequisites

- Access privExec Configuration Mode.

Procedure steps

Step	Action
1	To display VRRP configuration information, enter the following command: **`show ipv6 vrrp address [link-local <fe80::X:X:X:X>] [vrid <1-255>]`**
2	To display VRRP statistics, enter the following command: **`show ipv6 vrrp statistics [link-local <fe80::X:X:X:X>] [vrid <1-255>]`**

--End--

Variable definitions

Use the data in the following table to use the **`show ipv6 vrrp`** command.

Variable	Value
`[link-local <fe80::X:X:X:X>]`	Displays information by link-local IPv6 address.
`[vrid <1-255>]`	Displays information by virtual router ID.

Job aid

The following table shows the field descriptions for the **`show ipv6 vrrp address`** command.

Parameter	Description
VRID	Indicates the virtual router ID on a VRRP router.
P/V	Indicates whether this device responds to pings directed to a virtual router's IPv6 address.
IP	Indicates the assigned IPv6 addresses that a virtual router backs up.
MAC	Indicates the virtual MAC address of the virtual router in the format 00-00-5E-00-02-<VRID>, where the first three octets consist of the IANA OUI; the next two octets indicate the address block of the VRRP protocol; and the remaining octets consist of the VRID.
STATE	Indicates the current state of the virtual router. • initialize—waiting for a startup event • backup—monitoring the state or availability of the master router • master—forwarding IPv6 addresses associated with this virtual router.

Parameter	Description
CONTROL	Indicates the virtual router function. Set the value to enabled to transition the state of the router from initialize to backup. Set the value to disabled to transition the router from master or backup to initialize.
PRIO	Indicates the priority for the virtual router (for example, master election) with respect to other virtual routers that are backing up one or more associated IPv6 addresses. Higher values indicate higher priority. A priority of 0, which you cannot set, indicates that this router has stopped participating in VRRP and a backup virtual router transitions to become the new master. A priority of 255 is used for the router that owns the associated IPv6 addresses.
ADV	Indicates the Advertisement Interval, in milliseconds, between sending advertisement messages.
MASTER	Indicates the master router real (primary) IPv6 address. This is the IPv6 address listed as the source in the VRRP advertisement last received by this virtual router.
UP TIME	Indicates the time interval (in hundredths of a second) since this virtual router was initialized.
CRITICAL IPv6	Indicates the IPv6 address of the interface that causes a shutdown event.
CRITICAL IPv6 (ENABLED)	Indicates if the critical IPv6 address is enabled.
BACKUP-MASTER	Indicates the backup master IPv6 address.
BACKUP-MASTER STATE	Indicates the backup master state.
FAST ADV	Indicates the Fast Advertisement Interval, in milliseconds, between sending advertisement messages. When the Fast Advertisement Interval is enabled, the Fast Advertisement Interval is used instead of the regular advertisement interval.
FAST ADV (ENABLED)	Indicates the state of fast advertisement.
ACCEPT MODE	Controls whether a master router accepts packets addressed to the address owner’s IPv6 address as its own if it is not the IPv6 address owner. The default value is disable.
ACTION	Specifies whether to override the holddown timer manually and force preemption. Options are none (does not override the timer) and preempt (preempts the timer).

Parameter	Description
HLD DWN	Indicates the amount of time (in seconds) to wait before preempting the current VRRP master.
REM	Indicates the remaining hold-down timer value.
GLOBAL ADDRESS	Specifies the global IPv6 address associated with the link-local VRRP IPv6 address that the virtual router backs up.

Clearing VRRP statistics

Use the following procedure to clear IPv6 VRRP statistics.

Procedure steps

Step	Action
1	To clear IPv6 VRRP statistics, enter: **clear ipv6 vrrp {fastethernet <slot|port>| gigabitethernet <slot|port>| vlan <vid>} vrid <value>**

--End--

Variable definitions

Use the data in the following table to use the **clear ipv6 vrrp** command.

Variable	Value
{fastethernet <slot|port>| gigabitethernet <slot|port>| vlan <vid>}	Specifies the port or VLAN for which to clear statistics.
[vrid <1-255>]	Specifies the virtual router ID.

IPv6 RSMLT configuration using Enterprise Device Manager

Routed Split MultiLink Trunking (RSMLT) forwards packets in the event of core router failures, thus minimizing dropped packets during the routing protocol convergence.

To configure IPv6 RSMLT functionality, use the same configuration path as required for IPv4 RSMLT. RSMLT configuration on a given VLAN simultaneously affects both IPv4 and IPv6. All options apply equally to IPv6 and IPv4 RSMLT.

Note that enabling RSMLT on a VLAN for IPv6 enables RSMLT even in the absence of IPv4 configuration on the VLAN.

In addition to the IPv4 RSMLT tabs, the Enterprise Device Manager provides tabs for viewing IPv6-specific RSMLT information.

Navigation

Configuring RSMLT on a VLAN

You can configure RSMLT on each IP VLAN interface.

Prerequisites

- IP routing protocol on VLAN Layer 3 interfaces is enabled.
- VLANs with Layer 3 interfaces participate in Split MultiLink Trunking (SMLT).

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, VLAN**.
2	Double-click **VLANs**.
3	In the VLANs Basic tab, select a VLAN.
4	Click **IP**.
5	Click the **RSMLT** tab.
6	Select **Enable**.
7	In the **HoldDownTimer** box, enter a hold-down timer value.
8	In the **HoldUpTimer** box, enter a hold-up timer value.
9	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure RSMLT.

Variable	Value
Enable	Enables RSMLT.
HoldDownTimer	Defines how long the recovering or rebooting switch remains in a non-Layer 3 forwarding mode for the peer router MAC address. The range of this value is from 0 to 3600 seconds.
HoldUpTimer	Defines how long the RSMLT switch maintains forwarding for its peer. The value is a range from 0 to 3600 seconds or 9999. 9999 means infinity.

Enabling RSMLT-edge

Enable RSMLT-edge to store the RSMLT peer MAC/IP address-pair in its local configuration file and restore the configuration if the peer does not restore after a simultaneous reboot of both RSMLT peer switches.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IP**.
2	Double-click **RSMLT**.
3	In the Globals tab, select the **EdgeSupportEnable** option box.
4	Click **Apply**.

--End--

Viewing and editing IPv6 RSMLT local information

Use the following procedure to view and edit RSMLT local VLAN switch information.

Any configurations you make using this tab are not specific to IPv6. The configurations applied under the IPv6 RSMLT tab also apply to IPv4 RSMLT.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **RSMLT**.
3	In the **Local** tab, edit fields as required.
4	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to view and edit IPv6 RSMLT local information.

Variable	Value
IfIndex	The IP route SMLT operation index.
Ipv6Addr	The IP address of the VLAN when RSMLT is enabled.
Ipv6PrefixLength	The IPv6 prefix length.

Variable	Value
Enable	Specifies the status of RSMLT
HoldDownTimer	Defines how long the recovering/rebooting switch remains in a non-Layer 3 forwarding mode for the peer router MAC address. The range of this value is from 0 to 3600 seconds.
HoldDownTimeRemaining	Indicates the time remaining in the HoldDownTimer.
HoldUpTimer	Defines how long the RSMLT switch maintains forwarding for its peer. The value is a range from 0 to 3600 seconds or 9999. 9999 means infinity.
HoldUpTimeRemaining	Indicates the time remaining in the HoldUpTimer.
OperStatus	Displays the RSMLT operating status as either up or down.
SmltId	The ID range for the SMLT. A valid range is 1 to 32.
SltId	The ID range for the SMLT. A valid range is 1 to 512.
VlanId	The VLAN ID of the chosen VLAN.
MacAddr	The MAC address of the selected VLAN.
VrfId	Identifies the VRF.
VrfName	Indicates the VRF name.

Viewing and editing IPv6 RSMLT peer information

Use this procedure to view and edit RSMLT peer switch information.

Any configurations you make using this tab are not specific to IPv6. The configurations applied under the IPv6 RSMLT tab also apply to IPv4 RSMLT.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **RSMLT**.
3	Click the **Peer** tab.
4	Edit fields as required.
5	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to view and edit IPv6 RSMLT peer information.

Variable	Value
IfIndex	The IP route SMLT operation index.
Ipv6Addr	The IP address of the VLAN when RSMLT is enabled.
Ipv6PrefixLength	IPv6 prefix length.
AdminStatus	Indicates whether the peer is enabled.
HoldDownTimer	Defines how long the recovering/rebooting switch remains in a non-Layer 3 forwarding mode for the peer router MAC address. The range of this value is from 0 to 3600 seconds.
HoldDownTimeRemaining	Displays the time remaining of the HoldDownTimer.
HoldUpTimer	Defines how long the RSMLT switch maintains forwarding for its peer. The value is a range from 0 to 3600 seconds or 9999. 9999 means infinity.
HoldUpTimeRemaining	Displays the time remaining of the HoldUpTimer.
OperStatus	Displays the RSMLT operating status as either up or down.
SmltId	The ID range for the Split MultiLink Trunk. A valid range is 1 to 32.
SltId	The ID range for the Split MultiLink Trunk. A valid range is 1 to 512.
VlanId	The ID of the VLAN on which RSMLT is enabled.
MacAddr	The MAC address of the selected VLAN.
VrfId	Identifies the VRF.
VrfName	Indicates the VRF name.

Viewing IPv6 RSMLT-edge information

View RSMLT-edge to verify the RSMLT peer MAC/IP address-pair in its local config file and restore the configuration if the peer does not restore after a simultaneous reboot of both RSMLT-peer switches.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders: **Configuration, IPv6**.
2	Double-click **RSMLT**.
3	Click the **Edge Peer** tab.

--End--

Variable definitions

Use the data in the following table to view IPv6 RSMLT-edge information.

Parameter	Description
PeerVlanId	The ID of the VLAN associated with this entry
PeerIpv6Address	The IPv6 address of the peer RSMLT interface.
PeerIpv6PrefixLength	Peer IPv6 address prefix.
PeerMacAddress	The peer MAC address.
PeerVrfId	Identifies the Peer VRF.
PeerVrfName	The Peer VRF name.
PeerIsRaPrefix	True if this is a Router Advertisement prefix, False if this is a global address.
PeerConfType	Type of configured address, passed opaquely to Infinity.
PeerNoAdvertise	True if advertisement of this prefix is disabled, passed opaquely to Infinity.
PeerOspf6Advertise	True if OSPFv3 advertisement of this prefix is enabled, passed opaquely to Infinity.
PeerPrefCandidate	True if address is considered for preferred selection, passed opaquely to Infinity.
PeerPfxValidLife	Valid lifetime in seconds, passed opaquely to Infinity.
PeerPfxPrefLife	Preferred lifetime in seconds, passed opaquely to Infinity.
PeerPfxOnLinkFlag	If set then this prefix can be used for onlink determination, passed opaquely to Infinity.
PeerPfxAutoFlag	If set then this prefix can be used for address autoconfig, passed opaquely to Infinity.

IPv6 RSMLT configuration using the CLI

Routed Split MultiLink Trunking (RSMLT) forwards packets in the event of core router failures, thus minimizing dropped packets during the routing protocol convergence.

To configure IPv6 RSMLT functionality, use the same set of commands as required for IPv4 RSMLT. RSMLT configuration on a given VLAN simultaneously affects both IPv4 and IPv6. For example, the following command is used for configuring IPv6 RSMLT on VLAN:

config vlan <vid> ip rsmlt

All options apply equally to IPv6 and IPv4 RSMLT.

Note that the preceding command enables IPv6 RSMLT on a VLAN even in the absence of IPv4 configuration on the VLAN.

RSMLT configuration procedures

This task flow shows you the sequence of procedures you perform to configure RSMLT.

RSMLT configuration navigation

- “Job aid: Roadmap of IPv6 RSMLT CLI commands” (page 275)
- “Configuring RSMLT on a VLAN” (page 276)
- “Showing IP RSMLT information” (page 277)
- “Configuring RSMLT-edge” (page 278)

Job aid: Roadmap of IPv6 RSMLT CLI commands

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 20
Roadmap of RSMLT commands

Command	Parameter
`config vlan <vid> ip rsmlt`	`info`
	`disable`
	`enable`
	`holddown-timer <seconds>`
	`holdup-timer <seconds>`
`config ip rsmlt`	`rsmlt-edge-support <enable|disable>`
	`clear-rsmlt-peer [<vlanId>]`
	`info`
`show ip rsmlt info [<local|peer>]`	

Configuring RSMLT on a VLAN

You can configure RSMLT on each IP VLAN interface.

Prerequisites

- The IPv6 routing protocol must be enabled on the VLAN interfaces.
- VLANs with Layer 3 interfaces must also participate in Split MultiLink Trunking (SMLT).

Procedure steps

Procedure steps

Step	Action
1	Create an RSMLT on a VLAN by using the following command: **`config vlan <vid> ip rsmlt`**
2	Confirm your configuration by using the following command: **`config vlan <vid> ip rsmlt info`**

--End--

Variable definitions

Use the data in the following table to use the **`config vlan ip rsmlt`** command.

Variable	Value
`disable`	Disables RSMLT on the VLAN.
`enable`	Enables RSMLT on the VLAN.

Variable	Value
`holddown-timer <seconds>`	Defines how long the recovering/rebooting switch remains in a non-Layer 3 forwarding mode for the peer router MAC address. • **seconds** is the timer value in seconds. The range of the value is from 0 to 3600 seconds.
`holdup-timer <seconds>`	Defines how long the RSMLT switch maintains forwarding for its peer. • **seconds** is the timer value in seconds. The value is a range from 0 to 3600 seconds or 9999. 9999 means infinity.
`info`	Displays the RSMLT local and peer information.
`vid`	The VLAN ID in the range of 1 to 4094.

Showing IP RSMLT information

Show RSMLT information to view data for all RSMLT interfaces. The output of the command includes the IPv6 formation for the local and peer nodes.

Procedure steps

Step	Action
1	Display RSMLT information about the interface by using the following command: **show ip rsmlt info [<local|peer>]**

--End--

Variable definitions

Use the data in the following table to use the **show ip rsmlt info [<local|peer>]** command.

Variable	Value
`[<local|peer>]`	Specifies the local or peer switch.

Job aid

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

Table 21
show ip rsmlt info command

Parameter	Description
VID	Indicates the VLAN ID.
IP	Indicates the IP address of the router.
MAC	Indicates the MAC address assigned.
ADMIN	Indicates the administrative status of RSMLT on the router.
OPER	Indicates the operational status of RSMLT on the router.
HDTMR	Indicates the hold-down timer value in the range of 0 to 3600 seconds.
HUTMR	Indicates the range of the hold-up timer in the range of 0 to 3600 seconds or 9999. 9999 means infinity.
HDT REMAIN	Indicates the time remaining of the hold-down timer.
HUT REMAIN	Indicates the time remaining of the hold-up timer.
SMLT ID	Indicates the Split MultiLink Trunk ID.
SLT ID	Indicates the SLT ID.

Configuring RSMLT-edge

Configure RSMLT-edge to store the RSMLT peer MAC/IP address pair in its local configuration file and restore the configuration if the peer does not restore after a simultaneous reboot of both RSMLT peer switches. If enabled, all peer MAC/IP information for all RSMLT-enabled VLANs saved during next the save configuration command.

Procedure steps

Step	Action
1	Enable or disable RSMLT-edge by using the following command: **config ip rsmlt rsmlt-edge-support <enable|disable>**
2	Clear the peer MAC/IP information for the VLAN by using the following command: **config ip rsmlt clear-rsmlt-peer <vlanId>**

3 Display RSMLT configuration and status information by using the following command:
`config ip rsmlt info`

--End--

Variable definitions

Use the data in the following table to use the **`config ip rsmlt rsmlt-edge-support`** command.

Variable	Value
`disable`	Disables RSMLT peer forwarding.
`enable`	Enables RSMLT peer forwarding.

IPv6 RSMLT configuration using the NNCLI

Routed Split MultiLink Trunking (RSMLT) forwards packets in the event of core router failures, thus minimizing dropped packets during the routing protocol convergence.

To configure IPv6 RSMLT functionality, use the same set of commands as required for IPv4 RSMLT. RSMLT configuration on a given VLAN simultaneously affects both IPv4 and IPv6. For example, the following command is used for configuring IPv6 RSMLT on a VLAN:

```
(config-if)# ip rsmlt
```

All options apply equally to IPv6 and IPv4 RSMLT.

Note that the preceding command enables IPv6 RSMLT on a VLAN even in the absence of IPv4 configuration on the VLAN.

RSMLT configuration procedures

Refer to the following procedures to configure RSMLT.

RSMLT navigation

- "Job aid: Roadmap of IPv6 RSMLT NNCLI commands" (page 281)
- "Configuring RSMLT on a VLAN" (page 282)
- "Showing IP RSMLT information" (page 283)
- "Configuring RSMLT-edge" (page 284)

Job aid: Roadmap of IPv6 RSMLT NNCLI commands

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 22
Roadmap of RSMLT commands

Command	Parameter
PrivExec Mode	
`show ip rsmlt`	`edge-support`
	`<local|peer>`
Interface Configuration Mode	
`ip rsmlt`	`holddown-timer <0-3600>`
	`holdup-timer <seconds>`
Global Configuration Mode	
`ip rsmlt`	`edge-support`
`no ip rsmlt`	`peer-address`

Configuring RSMLT on a VLAN

You can configure RSMLT on each IP VLAN interface.

Prerequisites

- Access VLAN Interface Configuration Mode.
- The IPv6 routing protocol must be enabled on the VLAN interfaces.
- VLANs with Layer 3 interfaces must also participate in Split MultiLink Trunking (SMLT).

Procedure steps

Step	Action
1	Enable RSMLT on a VLAN by using the following command: **`ip rsmlt`** Use the **`no`** operator to disable RSMLT: **`no ip rsmlt`** To set this value to the default value, use the **`default`** operator with this command.

--End--

Variable definitions

Use the data in the following table to use the **`ip rsmlt`** command.

Variable	Value
holddown-timer <0-3600>	Defines how long the RSMLT switch does not participate in Layer 3 forwarding. • `0-3600` is the timer value in seconds. To set this value to the default value, use the **default** operator with this command. Nortel recommends that you configure this value to be longer than the anticipated routing protocol convergence.
holdup-timer <seconds>	Defines how long the RSMLT switch maintains forwarding for its peer. • **seconds** is the timer value in seconds. The value is a range from 0 to 3600 seconds or 9999. 9999 means infinity. To set this value to the default value, use the **default** operator with this command.

Showing IP RSMLT information

Show IP RSMLT information to view data about all RSMLT interfaces. The output of the command includes the IPv6 formation for the local and peer nodes.

Prerequisites

- Access privExec Configuration Mode or Global Configuration Mode.

Procedure steps

Step	Action
1	Display RSMLT information about the interface by using the following command: **show ip rsmlt [<local|peer>]**

--End--

Variable definitions

Use the information in the following command to complete the **show ip rsmlt** command.

Table 23
show ip rsmlt info command

Variable	Value
`[<local|peer>]`	Specifies values for the local or peer switch.

Job aid

The following table shows the field descriptions for the`show ip rsmlt [<local|peer>]` command.

Table 24
show ip rsmlt info command

Parameter	Description
VID	Indicates the VLAN ID.
IP	Indicates the IP address of the router.
MAC	Indicates the MAC address assigned.
ADMIN	Indicates the administrative status of RSMLT on the router.
OPER	Indicates the operational status of RSMLT on the router.
HDTMR	Indicates the hold-down timer value in the range of 0 to 3600 seconds.
HUTMR	Indicates the hold-up timer value in the range of 0 to 3600 seconds or 9999. 9999 means infinity.
HDT REMAIN	Indicates the time remaining of the hold-down timer.
HUT REMAIN	Indicates the time remaining of the hold-up timer.
SMLT ID	Indicates the Split MultiLink Trunk ID.
SLT ID	Indicates the SLT ID.

Configuring RSMLT-edge

Configure RSMLT-edge to store the RSMLT peer MAC/IP address-pair in its local config file and restore the configuration if the peer does not restore after a simultaneous reboot of both RSMLT-peer switches. If enabled, all peer MAC/IP information for all RSMLT-enabled VLANs are saved during next the save config command.

Prerequisites

- Access Global configuration mode.

Procedure steps

Step	Action
1	Enable RSMLT-edge by using the following command: **`ip rsmlt edge-support`** Use the **`no`** operator to disable RSMLT-edge: **`no ip rsmlt edge-support`**
2	Clear RSMLT peer information and delete the RSMLT peer address by using the following command: **`no ip rsmlt peer-address <vlan ID>`**
3	Display RSMLT-edge status information by using the following command: **`show ip rsmlt edge-support`**

--End--

Variable definitions

Use the data in the following table to use the **`no ip rsmlt peer-address`** command.

Variable	Value
`vlan ID`	The ID of the VLAN in the range of 0 to 4094.

IPv4-to-IPv6 transition mechanism configuration using Enterprise Device Manager

This section describes how to use Enterprise Device Manager to configure transition mechanisms, or tunnels, for IPv6 traffic through IPv4 networks. For conceptual information about tunnels, see "IPv6 routing fundamentals" (page 25).

Prerequisites to IPv4-to-IPv6 transition mechanism configuration

- Both the source and destination devices must use IPv6 and IPv4 addresses.

IPv4-to-IPv6 transition mechanism configuration navigation

Configuring the local VLAN or brouter port

Configure a tunnel for IPv6 VLANs or brouter ports to communicate through an IPv4 network. Manual tunnels are point-to-point, so you configure both source and destination addresses. You must configure both IPv6 and IPv4 addresses for both source and destination devices. The IPv6 addresses must represent the same network, for example 6666::1/96 and 6666::2/96.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **Tunnel**.
3	Click **Insert**.
4	In the **LocalAddress** box, click the button and select the IPv4 address for the local VLAN or brouter port.
5	In the **RemoteAddress** box, type the IPv4 address for the destination VLAN or brouter port.
6	In the **EncapsMethod** area, select **manual**.
7	In the **ID** box, type a number to represent the tunnel.
8	In the **IPv6AddressAddr** box, type the IPv6 address assigned to the tunnel VLAN or brouter port.
9	In the **IPv6AddressPrefixLength** box, type the number of bits to advertise in the IPv6 address.
10	Click **Insert**. After you create the tunnel, the Local Address tab displays the IPv4 addresses associated with the tunnel.

--End--

Variable definitions

Use the data in the following table to use the Tunnel tab.

Variable	Value
Address Type	Displays the address type for the tunnel: IPv4 for IPv6 packets encapsulated in IPv4.
LocalAddress	Identifies the local endpoint address of the tunnel.
RemoteAddress	Identifies the remote endpoint of the tunnel.
EncapsMethod	Displays the tunnel mode: IPv6 for manually configured tunnels and sixtoFour for automatically configured tunnels. The default value is manual.
ID	Identifies the tunnel number.
IfIndex	Displays a unique value that identifies the tunnel interface internally. The value is derived from the tunnel ID.

Configuring the destination VLAN or brouter port

Use the following procedure to configure a tunnel for IPv6 VLANs or brouter ports to communicate through an IPv4 network. Manual tunnels are point-to-point, so you configure both source and destination addresses. You must configure both IPv6 and IPv4 addresses for both source and destination devices. The IPv6 addresses must represent the same network, for example 6666::1/96 and 6666::2/96.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **Tunnel**.
3	Click **Insert**.
4	In the **LocalAddress** box, click the button and select the IPv4 address for the destination VLAN or brouter port.
5	In the **RemoteAddress** box, type the IPv4 address for the local VLAN or brouter port.
6	In the **EncapsMethod** area, select **manual**.
7	In the **ID** box, type a number to represent the tunnel.
8	In the **IPv6AddressAddr** box, type the IPv6 address that you configured for the tunnel VLAN or brouter port for the destination VLAN or brouter port.
9	In the **IPv6AddressPrefixLength** box, type the number of bits to advertise in the IPv6 address.
10	Click **Insert**.
	After you create the tunnel, the Local Address tab displays the IPv4 addresses associated with the tunnel.

--End--

Variable definitions

Use the data in the following table to use the Tunnel tab.

Variable	Value
Address Type	Displays the address type for the tunnel: IPv4 for IPv6 packets encapsulated in IPv4.
LocalAddress	Identifies the local endpoint address of the tunnel.
RemoteAddress	Identifies the remote endpoint of the tunnel.

Variable	Value
EncapsMethod	Displays the tunnel mode: IPv6 for manually configured tunnels and sixtoFour for automatically configured tunnels.
ID	Identifies the tunnel number.
IfIndex	Displays a unique value that identifies the tunnel interface internally. The value is derived from the tunnel ID.

Configuring OSPF on a tunnel

Configure the Open Shortest Path First (OSPF) protocol on IPv6 tunnels to support dynamic routing on the tunnel.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **Tunnel**.
3	Select the tunnel on which to configure OSPF.
4	Click **IPv6 OSPF**.
	The OSPF Interface tab appears.
5	Click **Insert**.
6	In the **AreaId** box, click the button and select the required area ID.
7	In the **AdminStat** area, select **enabled**.
8	In the **RtrPriority** box, modify the priority value if required.
9	Modify values in the **TransitDelay**, **RetransitInterval**, **HelloInterval**, **RtrDeadInterval**, or **PollInterval** boxes, if required.
10	In the **MulticastForwarding** area, select the required option: **blocked**, **multicast**, or **unicast**.
11	Select the **Demand** check box to enable demand for an instance.
12	In the **Metric** box, type the metric value for a demand for an instance.
13	In the **InstId** box, type the instance ID.
14	Click **Insert**.

15	On the **OSPF Interface** tab, click **Apply**.

--End--

Deleting a tunnel

Delete a tunnel to remove it from the configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **Tunnel**.
3	Select the tunnel to delete.
4	Click **Delete**.

--End--

Modifying tunnel hop limits

Modify tunnel hop limits to update hop limit values on previously configured tunnels.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **Tunnel**.
3	Click the **Tunnel Interface** tab.
4	In the row for the tunnel to configure, double-click the **HopLimit** column to modify the displayed information as required.
5	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to use the Tunnel Interface tab.

Variable	Value
Index	Identifies the tunnel interface internally. The value is derived from the tunnel ID.
EncapsMethod	Displays the tunnel mode: IPv6 for manually configured tunnels and 6to4 for automatically configured tunnels.
HopLimit	Configures the maximum number of hops in the tunnel. The default value is 255.
Security	Indicates the type of security on the tunnel interface.
TOS	Displays the method used to configure the high 6 bits (the differentiated services codepoint) of the IPv4 type of service (TOS) or IPv6 traffic class in the outer IP header. A value of -1 indicates that the bits are copied from the payload header. A value of -2 indicates that a traffic conditioner is invoked and more information can be available in a traffic conditioner MIB module. A value from 0 to 63 indicates that the bit field is configured to the indicated value.
FlowLabel	Displays the method used to set the IPv6 Flow Label value. This object need not be present in rows where tunnelIfAddressType indicates the tunnel is not over IPv6. A value of -1 indicates that a traffic conditioner is invoked and more information can be available in a traffic conditioner MIB. Any other value indicates that the Flow Label field is configured to the indicated value.
AddressType	Displays Manual for a manually configured tunnel, or sixToFour for autoconfigured tunnels.
LocalInetAddress	Identifies the local endpoint address of the tunnel.
RemoteInetAddress	Identifies the remote endpoint of the tunnel.
EncapsLimit	Displays the address of the local endpoint of the tunnel (that is, the source address used in the outer IP header). If the address is unknown, the value is 0.0.0.0 for IPv4 or :: for IPv6. The tunnelIfAddressType displays the object type.

IPv4-to-IPv6 transition mechanism configuration using the CLI

This chapter describes how to use the CLI to configure IPv6 transition mechanisms, or tunnels. For conceptual information about tunnels, see "IPv6 routing fundamentals" (page 25).

Prerequisites to IPv4-to-IPv6 transition mechanism configuration

- You must configure the local and remote switches with IPv4 addresses that you can ping.
- You must configure the local and remote switches with one or more of the following protocols to route IPv4 traffic: Static, RIP, or OSPF.

IPv4-to-IPv6 transition mechanism configuration navigation

Job aid: Roadmap of tunnel configuration CLI commands

The following table lists the commands and parameters that you use to perform the procedures in this chapter.

Table 25
Job aid: Roadmap of tunnel configuration CLI commands

Command	Parameter
`config ipv6 tunnel <tunnel id> create local-addr <source ipv4 address> ipv6addr <source ipv6address/prefix-lenth> remot-address <dst ipv4address>`	`info`
	`delete`
	`hop-limit <value>`

Table 25
Job aid: Roadmap of tunnel configuration CLI commands (cont'd.)

Command	Parameter
`config ipv6 tunnel <tunnel-id> ospf`	`info`
	`admin-status <enable|disable>`
	`create <area> [priority <value>] [metric <value>] [retransmit-interval <value>] [transit-delay <value>] [hello-interval <value>] [dead-interval <value>]`
	`delete`
	`hello-interval <seconds>`
	`dead-interval <seconds>`
	`poll-interval <seconds>`
	`metric <metric>`
	`priority <priority>`
	`retransmit-interval <seconds>`
	`transit-delay <seconds>`

Configuring manual tunnels

Create a tunnel to transfer traffic between IPv6 devices in an IPv4 network. Configure manual tunnels when you want to define both the local and destination addresses.

Use this procedure to configure the tunnel at both the source and destination addresses.

Procedure steps

Step	Action
1	Configure the tunnel at the source by using the following command: **`config ipv6 tunnel <tunnel id> create local-addr <source ipv4 address> ipv6addr <source ipv6 address/prefix length> remote-address <remote ipv4 address>`**
2	Configure the tunnel at the destination by using the following command: **`config ipv6 tunnel <tunnel id> create local-addr <remote ipv4 address> ipv6 addr <remote ipv6`**

address/prefix length> remote-address <source ipv4 address>

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 tunnel** command.

Variable	Value
create [local addr <value>] [ipv6addr <value>] [remote-address <value>]	Creates the tunnel for a VLAN or brouter port. • **local addr <value>** configures the address for the local device. • **ipv6addr <value>** configures the local address for the tunneled device in IPv6/prefix-length format. • **remote-address <value>** configures the address for the device that is tunneled to in IPv4 or IPv6/prefix-length format.
delete	Deletes the tunnel.
hop-limit <value>	Configures the maximum number of hops that a packet can make before it is dropped. • **value** is in the range 0–255.
info	Displays the current settings for the command.
tunnel id	Specifies the ID number of the tunnel in the range of 1-5000.

Example of configuring manual tunnels

Procedure steps

Step	Action
1	Configure the tunnel at the source. **ERS-8610:5#config ipv6 tunnel 1044 create local addr 20.10.10.107 ipv6addr 0100:0200:0300:0004:0005:0006:0000:aa01/80 remote-address 10.20.20.105**
2	Configure the tunnel at the destination.

```
ERS-8610:5#config ipv6 tunnel 1045 create local
addr 10.20.20.105 ipv6addr 0100:0200:0300:0004:00
05:0006:0000:aa02/80 remote-address 20.10.10.107
```

--End--

Configuring OSPF on a tunnel

Configure OSPF on a VLAN or brouter tunnel to create a dynamic IPv6 tunnel on the OSPF interface.

Procedure steps

Step	Action
1	Configure OSPF on a tunnel by using the following command: `config ipv6 tunnel <tunnel-id> ospf`

--End--

Variable definitions

Use the data in the following table to use the `config ipv6 tunnel ospf` command.

Variable	Value
`admin-status <enable|disable>`	Configures the state (enabled or disabled) of the OSPF interface.
`create <area> [priority <value> ] [metric <value> ] [retransmit-interval <value> ] [transit-delay <value> ] [hello-interval <value> ] [dead-interval <value> ] [type <value> ]`	Creates an OSPF interface. • `<area>` is the area IP address (0.0.0.0 to 255.255.255.255) {a.b.c.d}. • `priority <value>` is the priority in the range 0–255. • `metric <value>` is the metric in the range 0–65535. • `retransmit-interval <value>` is the retransmit interval in the range 1–1800 seconds. • `transit-delay <value>` is the transit delay in the range 1–1800 seconds.

<table>
<tr><th>Variable</th><th>Value</th></tr>
<tr><td></td><td><code>hello-interval <value></code> is the hello interval in the range 1–65535 seconds.
<code>dead-interval <value></code> is the dead interval in the range 1–4095 seconds.</td></tr>
<tr><td><code>dead-interval <seconds></code></td><td>Configures the OSPF dead interval for the interface.

<code>seconds</code> is the number of seconds the switch OSPF neighbors wait before determining that this OSPF router is down. The range is from 1–4095. This value must be at least four times the Hello interval value. The default is 40.</td></tr>
<tr><td><code>delete</code></td><td>Deletes an OSPF interface.</td></tr>
<tr><td><code>hello-interval <seconds></code></td><td>Configures the OSPF hello interval for the interface.

<code>seconds</code> is the number of seconds between hello packets sent on this interface. The range is 1–65535. The default is 10.

ATTENTION
When you change the hello interval values, you must save the configuration file and reboot the switch for the values to be restored and checked for consistency.</td></tr>
<tr><td><code>info</code></td><td>Displays OSPF characteristics for the interface.</td></tr>
<tr><td><code>metric <metric></code></td><td>Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements.
<code>metric</code> is the range 0–65535.</td></tr>
<tr><td><code>poll-interval <seconds></code></td><td>Configures the polling interval for the OSPF interface in seconds.
<code>seconds</code> is 0–2147483647.</td></tr>
</table>

Variable	Value
priority <priority>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. **priority** is in the range 0–255. The default is 1.
retransmit-interval <seconds>	Configures the retransmit interval for the OSPF interface; the number of seconds between link-state advertisement retransmissions. **seconds** is an integer 1–1800.
transit-delay <seconds>	Configures the transit delay time for the OSPF interface, the estimated time in seconds required to transmit a link-state update packet over the interface. **seconds** is an integer 1–1,800.
tunnel-id	Specifies the ID number of the tunnel in the range of 1–2147477248.

Deleting a tunnel

Delete a configured tunnel to remove it from the configuration.

Procedure steps

Step	Action
1	Delete a tunnel by using the following command: **config ipv6 tunnel <tunnel ID> delete**

--End--

Variable definitions

Use the data in the following table to use the **config ipv6 tunnel delete** command.

Variable	Value
`tunnel-id`	Specifies the ID number of the tunnel in the range of 1–2147477248.

IPv4-to-IPv6 transition mechanism configuration using the NNCLI

This section describes how to use the NNCLI to configure IPv6 transition mechanisms, or tunnels. For conceptual information about tunnels, see "IPv6 routing fundamentals" (page 25).

Prerequisites to IPv4-to-IPv6 transition mechanism configuration

- You must configure the local and remote switches with IPv4 addresses that you can ping.
- You must configure the local and remote switches with one or more of the following protocols to route IPv4 traffic: Static, RIP, or OSPF.

IPv4-to-IPv6 transition mechanism configuration navigation

Job aid: Roadmap of tunnel configuration NNCLI commands

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 26
Job aid: Roadmap of tunnel configuration NNCLI commands

Command	Parameter
Global Configuration mode	

Table 26
Job aid: Roadmap of tunnel configuration NNCLI commands (cont'd.)

Command	Parameter
`ipv6 tunnel <tunnel id>`	`source <A.B.C.D> address <ipv6 address/prefix-len> destination <A.B.C.D>`
	`hop-limit <value>`
OSPF Router Configuration mode	
`ipv6 tunnel <tunnel id>`	`dead-interval <seconds>`
	`enable`
	`hello-interval <seconds>`
	`metric <value>`
	`poll-interval <seconds>`
	`priority <value>`
	`retransmit-interval <seconds>`
	`transmit-delay <seconds>`
	`area <A.B.C.D> [dead-interval <seconds>] [hello-interval <seconds>] [metric <value>] [priority <value>] [retransmit-interval <seconds>] [transmit-delay <seconds>]`

Configuring manual tunnels

Create a tunnel to transfer traffic between IPv6 devices in an IPv4 network. Configure manual tunnels when you want to define both the local and destination addresses.

Use this procedure to configure the tunnel at both the source and destination addresses.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the tunnel at the source and destination by using the following command:

```
ipv6 tunnel <tunnel id> source <A.B.C.D> address <ipv6
address/prefix-len> destination <A.B.C.D>
```

2 Configure the hop limit by using the following command:

```
ipv6 tunnel <tunnel id> hop-limit <value>
```

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 tunnel`** command.

Variable	Value
`address <ipv6 address/prefix-len>`	Configures the local address for the tunneled device in IPv6/prefix-length format.
`destination <A.B.C.D>`	Configures the address for the device that is tunneled to in IPv4 or IPv6/prefix-length format.
`hop-limit <value>`	Configures the maximum number of hops that a packet can make before it is dropped. • **`value`** is in the range 0–255. To set this option to the default value, use the **`default`** operator with the command. The default value is 255.
`source <A.B.C.D>`	Configures the address for the local device.
`tunnel id`	Specifies the ID number of the tunnel in the range of 1-5000.

Example of configuring manual tunnels

Procedure steps

Step	Action

1 Configure the tunnel at the source.

```
ERS-8606:5(config)#ipv6 tunnel 1044 source
20.10.10.107 address 0100:0200:0300:0004:0005:000
6:0000:aa01/80 destination 10.20.20.105
```

2 Configure the tunnel at the destination.

```
ERS-8606:5(config)#ipv6 tunnel 1045 source
10.20.20.105 address 0100:0200:0300:0004:0005:000
6:0000:aa02/80 destination 20.10.10.107
```

--End--

Configuring OSPF on a tunnel

Configure OSPF on a VLAN or brouter tunnel to create a dynamic IPv6 tunnel on the OSPF interface.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure OSPF on a tunnel by using the following command:

```
ipv6 tunnel <tunnel id> [dead-interval <seconds>]
enable [hello-interval <seconds>] [metric <value>]
[poll-interval <seconds>] [priority <value>]
[retransmit-interval <seconds>] [transmit-delay
<seconds>]
```

Step	Action
2	Configure the OSPF area for the tunnel by using the following command:

```
ipv6 tunnel <tunnel id> area <A.B.C.D> [dead-interval
<seconds>] [hello-interval <seconds>] [metric <value>]
[priority <value>] [retransmit-interval <seconds>]
[transmit-delay <seconds>]
```

--End--

Variable definitions

Use the data in the following table to use the **ipv6 tunnel** command.

Variable	Value
area <A.B.C.D>	Configures the area IP address (0.0.0.0 to 255.255.255.255) {a.b.c.d}.

<table>
<tr><th>Variable</th><th>Value</th></tr>
<tr><td>dead-interval <seconds></td><td>Configures the OSPF dead interval for the interface.

• seconds is the number of seconds the switch OSPF neighbors wait before determining that this OSPF router is down. The range is from 1-4095. This value must be at least four times the hello interval value. The default is 40.

To set this option to the default value, use the default operator with the command.</td></tr>
<tr><td>enable</td><td>Configures the state (enabled or disabled) of the OSPF interface. To set this option to the default value, use the default operator with the command.</td></tr>
<tr><td>hello-interval <seconds></td><td>Configures the OSPF Hello interval for the interface.

• seconds is the number of seconds between hello packets sent on this interface. The range is 1–65535. The default is 10.

ATTENTION
When you change the hello interval values, you must save the configuration file and reboot the switch for the values to be restored and checked for consistency.

To set this option to the default value, use the default operator with the command.</td></tr>
<tr><td>metric <value></td><td>Configures the OSPF metric for the interface. The switch advertises the metric in router link advertisements.

• value is the range 0–65535.

To set this option to the default value, use the default operator with the command.
The default value is 1.</td></tr>
</table>

Variable	Value
poll-interval <seconds>	Configures the polling interval for the OSPF interface in seconds. • **seconds** is between 1–2 147 483 647. To set this option to the default value, use the **default** operator with the command. The default value is 120.
priority <value>	Configures the OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become either the designated router or a backup. The priority is used only during election of the designated router and backup designated router. • **value** is in the range 0–255. The default is 1. To set this option to the default value, use the **default** operator with the command.
retransmit-interval <seconds>	Configures the retransmit interval for the OSPF interface; the number of seconds between link-state advertisement retransmissions. • **seconds** is an integer between 1–1800. To set this option to the default value, use the **default** operator with the command. The default value is 5.
transit-delay <seconds>	Configures the transit delay time for the OSPF interface, the estimated time in seconds required to transmit a link-state update packet over the interface. • **seconds** is an integer between 1–1800. To set this option to the default value, use the **default** operator with the command. The default value is 1.
tunnel-id	Specifies the ID number of the tunnel in the range of 1-5000.

Multicast protocol configuration using Enterprise Device Manager

This chapter contains procedures to configure Multicast Listener Discovery (MLD).

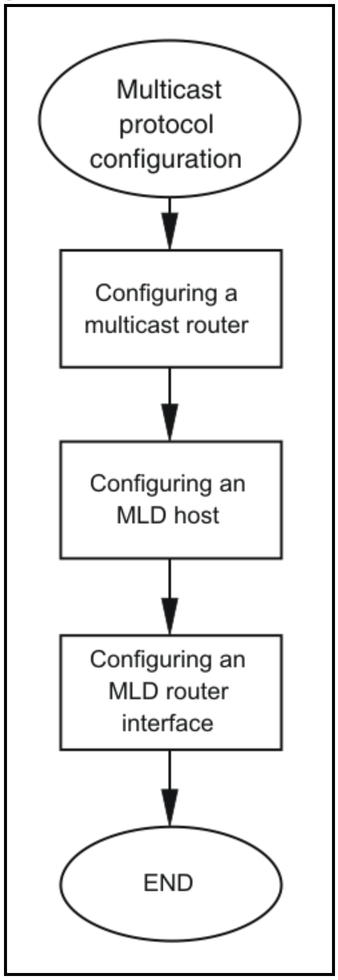
MLD discovers devices soliciting multicast traffic to update multicast tables. This improves efficiency and saves bandwidth; only devices that require multicast traffic receive it rather than every device on the network.

For more information about MLD concepts, see "IPv6 routing fundamentals" (page 25).

Multicast protocol configuration procedures

This task flow shows you the sequence of procedures you perform to configure multicast routing protocols for IPv6. To link to any procedure, click the procedure in "Multicast protocol configuration navigation" (page 308).

Figure 15
Multicast protocol configuration procedures



Multicast protocol configuration navigation

- "Configuring a multicast router" (page 308)
- "Configuring an MLD host" (page 309)
- "Configuring an MLD router interface" (page 310)
- "Viewing the MLD cache" (page 311)

Configuring a multicast router

Configure a multicast router to enable Multicast Listening Discovery (MLD) on the router at a chassis level.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Edit**.
2	Double-click **Chassis**.
3	Click the **Mcast Mlt Distribution** tab.
4	Select the **Enable** check box to enable multicast multilink trunk (MLT) routing.
5	In the **GrpMask** box, type the group mask address in IPv4 format. The default is 255.255.255.255.
6	In the **SrcMask** box, type the source mask address in IPv4 format. The default is 255.255.255.255.
7	Select the **RedistributeEnable** check box to enable redistribution.
8	Click **Apply**.

--End--

Configuring an MLD host

Configure the switch as an MLD host to listen to multicast packets.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **MLD**.
3	Select the **MulticastAdminStatus** check box.
4	Click **Apply**.

--End--

Variable definitions

Use the data in the following table to configure the MLD Globals tab.

Variable	Value
MulticastAdminStatus	Select to configure the switch as an MLD host.

Configuring an MLD router interface

Configure MLD on a router interface to customize the MLD configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **MLD**.
3	Click the **Interfaces** tab.
4	Click **Insert**.
5	In the **IfIndex** box, click **Port** or **VLAN** and select a port number or VLAN.
6	Edit the remaining values as required.
7	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to use the MLD Interfaces tab.

Variable	Value
IfIndex	Configures a unique value identifying a physical interface or a logical interface (VLAN).
Query Interval	Configures the query interval in seconds. The range is 0–65535. The default is 125.
Version	Configures the version of MLD. The versions are 1 or 2. The default is 1.
Querier	Indicates the IPv6 address to query.
QueryMaxResponseDelay	Configures the query maximum response time in 1/10 of a second. The range is 0–65535. The default is 10.
Joins	Indicates the number of joins.
Groups	Indicates the groups being listened to.
Robustness	Configures the robustness value. The range is 0–65535. The default is 2.
LastListenQueryIntvl	Configures the last member query interval in 1/10 of a second. The range is 0–65535. The default is 1.

Variable	Value
QuerierUpTime	Indicates the amount of time that the querier is enabled.
QuerierExpiryTime	Inidcates the expiry time for the querier.

Viewing the MLD cache

View the MLD cache to see IPv6 multicast groups for which members exist on an interface.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **MLD**.
3	Click the **Cached** tab.

--End--

Variable definitions

Use the data in the following table to use the MLD Cached tab.

Variable	Value
Address	Displays the IPv6 address for the interface.
IfIndex	Displays a unique value to identify a physical interface or a logical interface (VLAN).
Self	Indicates if the local system is a member of the group address on the current interface.
LastReporter	Displays the source IPv6 address for the last received membership report for the IPv6 multicast group address on the current interface. If no membership report is received, the object value is 0::0.
UpTime	Indicates the duration of time that MLD is enabled.
ExpiryTime	Indicates the expiry time.

Multicast protocol configuration using the CLI

This chapter describes the procedures to configure Multicast Listener Discovery (MLD) on your Nortel Ethernet Routing Switch 8600.

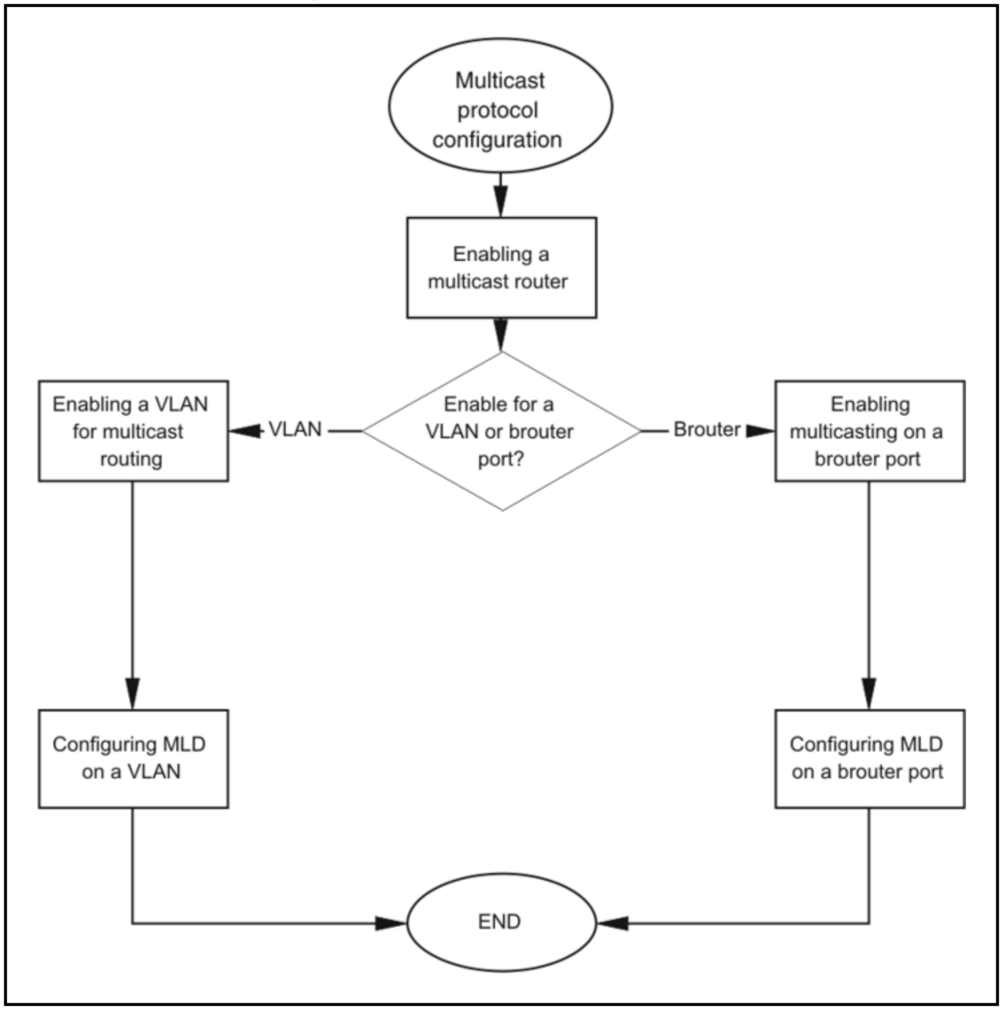
MLD provides group management capabilities by allowing hosts to inform routers of membership status within groups. MLD discovers the presence of multicast listeners on directly attached links. MLD provides the necessary information to route multicast packets to routers requiring multicast traffic.

For more information about MLD concepts, see "IPv6 routing fundamentals" (page 25).

Multicast protocol configuration procedures

This task flow shows you the sequence of procedures you perform to configure multicast routing protocols for IPv6. To link to any procedure, click the procedure in "Multicast protocol configuration navigation" (page 314).

Figure 16
Multicast protocol configuration procedures



Multicast protocol configuration navigation

- “Job aid: Roadmap of IPv6 multicast CLI commands” (page 314)
- “Enabling a multicast router” (page 315)
- “Enabling a VLAN for multicast routing” (page 315)
- “Configuring MLD on a VLAN” (page 316)
- “Enabling multicasting on a brouter port” (page 317)
- “Configuring MLD on a brouter port” (page 317)

Job aid: Roadmap of IPv6 multicast CLI commands

The following table lists the commands and parameters that you use to perform the procedures in this chapter.

Table 27
Job aid: Roadmap of IPv6 multicast CLI commands

Command	Parameter
`config ethernet <ports> ipv6 mcast <enable|disable>`	
`config ethernet <ports> ipv6 mld`	`info`
	`last-memb-query-int <seconds>`
	`query-interval <seconds>`
	`query-maxresp <1seconds>`
	`robustval <integer>`
	`version <1|2>`
`config ipv6 mcast <enable|disable>`	—
`config vlan <vid> ipv6 mcast <enable|disable>`	—
`config vlan <vid> ipv6 mld`	`info`
	`last-memb-query-int <seconds>`
	`query-interval <seconds>`
	`query-maxresp <1seconds>`
	`robustval <integer>`
	`version <1|2>`

Enabling a multicast router

Enable the router for multicast traffic to globally enable the MLD protocol.

Procedure steps

Step	Action
1	Enable the multicast router by using the following command: `config ipv6 mcast <enable|disable>`

--End--

Enabling a VLAN for multicast routing

Configure a VLAN for multicast traffic to enable MLD on the VLAN.

Procedure steps

Step	Action
1	Enable a VLAN for multicast routing by using the following command: **`config vlan <vid> ipv6 mcast <enable|disable>`**

--End--

Variable definitions

Use the data in the following table to use the **`config vlan ipv6 mcast <enable|disable>`** command.

Variable	Value
`vid`	Specifies a VLAN ID in the range of 1–4094.

Configuring MLD on a VLAN

Configure MLD on a VLAN to customize the configuration.

Procedure steps

Step	Action
1	Configure MLD by using the following command: **`config vlan <vid> ipv6 mld`**

--End--

Variable definitions

Use the data in the following table to use the **`config vlan ipv6 mld`** command.

Variable	Value
`info`	Displays the current VLAN MLD configuration setting.
`last-memb-query-int <seconds>`	Configures the query interval time in 1/10 of a second for the last member. **`seconds`** is in the range 0–65535.

Variable	Value
`query-interval <seconds>`	Configures the query interval time in 1/10 of a second. `seconds` is in the range 0–65535.
`query-maxresp <1seconds>`	The maximum query response time advertised in MLD queries on this interface. `seconds` is in the range 0–65535.
`robustval <integer>`	Configures the robustness value. `integer` is in the range 0–65535.
`version <1|2>`	Configures the version of MLD to version 1 or version 2.
`vid`	Specifies a VLAN ID in the range of 1–4094.

Enabling multicasting on a brouter port

Configure multicasting on a brouter port to enable MLD on the port.

Procedure steps

Step	Action
1	Enable multicasting by using the following command: `config ethernet <ports> ipv6 mcast <enable|disable>`

--End--

Variable definitions

Use the data in the following table to use the **`config ethernet ipv6 mcast`** command.

Variable	Value
`ports`	Specifies a port/slot or a port list.

Configuring MLD on a brouter port

Configure MLD on a brouter port to customize the configuration.

Procedure steps

Step	Action
1	Configure MLD by using the following command:

config ethernet <ports> ipv6 mld

--End--

Variable definitions

Use the data in the following table to use the **config ethernet ipv6 mld** command.

Variable	Value
info	Displays the current brouter port MLD configuration setting.
last-memb-query-int <seconds>	Configures the query interval time in 1/10 of a second for the last member. **seconds** is in the range 0–65535.
ports	Specifies a port/slot or a port list.
query-interval <seconds>	Configures the query interval time in 1/10 of a second. **seconds** is in the range 0–65535.
query-maxresp <1seconds>	The maximum query response time advertised in MLD queries on this interface. **seconds** is in the range 0–65535.
robustval <integer>	Configures the robustness value. **integer** is in the range 0–65535.
version <1|2>	Configures the version of MLD to version 1 or version 2.

Multicast protocol configuration using the NNCLI

This chapter describes the procedures used to configure Multicast Listener Discovery (MLD) on your Nortel Ethernet Routing Switch 8600.

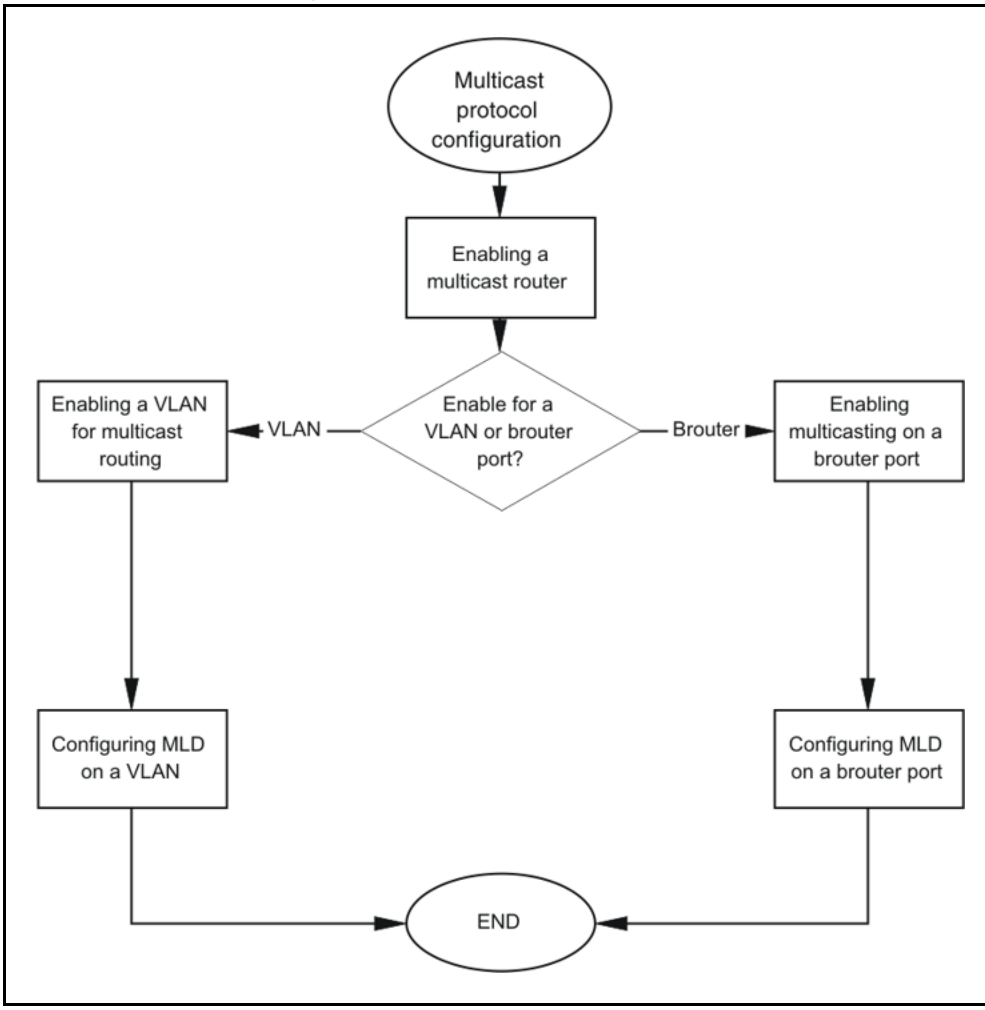
MLD provides group management capabilities by allowing hosts to inform routers of membership status within groups. MLD discovers the presence of multicast listeners on directly attached links. MLD provides the necessary information to route multicast packets to routers requiring multicast traffic.

For more information about MLD concepts, see "IPv6 routing fundamentals" (page 25).

Multicast protocol configuration procedures

This task flow shows you the sequence of procedures you perform to configure multicast routing protocols for IPv6. To link to any procedure, click the procedure in "Multicast protocol configuration navigation" (page 320).

Figure 17
Multicast protocol configuration procedures



Multicast protocol configuration navigation

- "Job aid: Roadmap of IPv6 multicast NNCLI commands" (page 320)
- "Enabling a multicast router" (page 321)
- "Enabling a VLAN for multicast routing" (page 321)
- "Configuring MLD on a VLAN" (page 322)
- "Enabling multicasting on a brouter port" (page 323)
- "Configuring MLD on a brouter port" (page 324)

Job aid: Roadmap of IPv6 multicast NNCLI commands

The following table lists the commands and parameters that you use to perform the procedures in this chapter.

Table 28
Job aid: Roadmap of IPv6 multicast NNCLI commands

Command	Parameter
Global Configuration mode	
`ipv6 multicast-routing`	–
Interface Configuration mode	
`ipv6 interface multicast-routing`	`mtu <bytes>`
	`reachable-time <value>`
	`retransmit-timer <value>`
`ipv6 mld`	`last-memb-query-int <value>`
	`query-interval <value>`
	`query-max-response-time <value>`
	`robustval <value>`
	`version <1|2>`

Enabling a multicast router

Enable the router for multicast traffic to globally enable MLD.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Enable the multicast router by using the following command: `ipv6 multicast-routing`

--End--

Enabling a VLAN for multicast routing

Configure a VLAN for multicast traffic to enable MLD on the VLAN.

Prerequisites

- You must log on to the VLAN Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Enable a VLAN for multicast routing by using the following command: **`ipv6 interface multicast-routing [reachable-time <value>] [retransmit-timer <value>]`**

--End--

Variable definitions

Use the data in the following table to use the **`ipv6 interface multicast-routing`** command.

Variable	Value
`reachable-time <value>`	Configures the reachable time, in milliseconds, for the interface. The range is 0–3600000.
`retransmit-timer <value>`	Configures the time between attempts to transmit multicast packets, in milliseconds, for the interface. The range is 0–3600000.

Configuring MLD on a VLAN

Configure MLD on a VLAN to customize the configuration.

Prerequisites

- You must log on to the VLAN Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure MLD by using the following command: **`ipv6 mld [last-memb-query-int <value>] [query-interval <value>] [query-max-response-time <value>] [robustval <value>] [version <1|2>]`**

--End--

Variable definitions

Use the data in the following table to use the **ipv6 mld** command.

Variable	Value
last-memb-query-int <value>	Configures the query interval time in 1/10 of a second for the last member. **value** is in the range 0–65535. The default value is 1.
query-interval <value>	Configures the maximum query response time advertised in MLD queries on this interface. **value** is in the range 0–65535. The default value is 125.
query-max-response-time <value>	Configures the query interval time in 1/10 of a second for the last member. **value** is in the range 0–65535. The default value is 10.
robustval <value>	Configures the robustness value. **value** is in the range 0–65535. The default value is 2.
version <1|2>	Configures the version of MLD to version 1 or version 2. The default value is 1.

Enabling multicasting on a brouter port

Configure multicasting on a brouter port to enable MLD on the port.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Enable multicasting by using the following command:

```
ipv6 interface multicast-routing [reachable-time
<value>] [retransmit-timer <value>]
```

--End--

Variable definitions

Use the data in the following table to use the **ipv6 interface multicast-routing** command.

Variable	Value
reachable-time <value>	Configures the reachable time, in milliseconds, for the interface. The range is –03600000.
retransmit-timer <value>	Configures the time between attempts to transmit multicast packets, in milliseconds, for the interface. The range is 0–3600000.

Configuring MLD on a brouter port

Configure MLD on a brouter port to customize the configuration.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure MLD by using the following command: `ipv6 mld [last-memb-query-int <value>] [query-interval <value>] [query-max-response-time <value>] [robustval <value>] [version <1|2>]`

--End--

Variable definitions

Use the data in the following table to use the **ipv6 mld** command.

Variable	Value
last-memb-query-int <value>	Configures the query interval time in 1/10 of a second for the last member. **value** is in the range 0–65535. The default value is 1.
query-interval <value>	Configures the query interval time in 1/10 of a second. **value** is in the range 0–65535. The default value is 125.
query-max-response-time <value>	Configures the maximum query response time advertised in MLD queries on this interface. **value** is in the range 0–65535. The default value is 10.
robustval <value>	Configures the robustness value. **value** is in the range 0–65535. The default value is 2.
version <1|2>	Configures the version of MLD to version 1 or version 2. The default value is 1.

IPv6 traffic filter configuration using Enterprise Device Manager

This chapter describes how to configure and manage traffic filters for R and RS modules on the Ethernet Routing Switch 8600 with Enterprise Device Manager. Specifically, it provides configuration instructions for advanced filtering features using the appropriate options under Security, Data Path, Advanced Filters (ACE/ACLs) on the main Enterprise Device Manager menu. For conceptual information about IP filters, see "IPv6 routing fundamentals" (page 25).

For additional information about IPv4 filters, see *Nortel Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for R and RS Modules* (NN46205-507).

IPv6 traffic filter configuration navigation

Configuring an ACT

Configure an access control template (ACT) to create, delete, apply, or specify attributes. After you apply the ACT you cannot change the attributes. ACT IDs 4001 to 4096 are reserved for system-defined ACTs.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click **Insert** to add a new ACT.
4	Select the required IPv6 attributes.
5	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure an ACT.

Variable	Value
ActId	Specifies a unique identifier for the ACT. The range is 1–4096.
Name	Specifies a descriptive user-defined name for the ACT entry.
ArpAttrs	Specifies one of the following ARP attributes: • none • operation (This is the only valid option for ARP attributes.) **ATTENTION** ArpAttrs is not a supported for IPv6 filters.

Variable	Value
EthernetAttrs	Specifies one or more of the following Ethernet attributes: • none • srcMac • dstMac • etherType • port • vlan • vlanTagPrio
IpAttrs	Specifies one or more of the following IP attributes: • none • scrip • dstip • ipFragFlag • ipOptions • ipProtoType • dscp
ProtocolAttrs	Specifies one or more of the following protocol attributes: • none • tcpSrcPort • udpSrcPort • tcpDstPort • udpDstport • tcpFlags • icmpMsgFlags
IPv6Attrs	Specifies one or more of the following IPv6 attributes: • none • srcIpv6 • dstIpv6 • NextHdr

Modifying ACT attributes

Modify ACT attributes to change the configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Double-click the required attribute field on the ACT tab.
4	Select the required options.
5	Click **OK** to apply the required attributes.
6	In the Apply column for the modified entry, ensure that **True** is selected.
7	Click **Apply**. The specified attributes field on the ACT tab updates.

--End--

> **ATTENTION**
> You can only modify an ACT once. If you require further modifications, delete the entry and create a new ACT with the required attributes.

Inserting a pattern in an ACT

Insert a pattern in an ACT to apply the template.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Select the ACT in which to insert a pattern.
4	Click the **Pattern** button.
5	Click **Insert**. **ATTENTION** An ACT uses IPv4 or IPv6 attributes, but not both. You cannot combine IPv4 and IPv6 attributes in the same ACL.
6	Select the required options in the dialog box.

7 Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the Pattern tab.

Variable	Value
ActId	Specifies a unique identifier for the ACT. The range is 1–4096.
Index	Index identifier.
Name	Specifies a descriptive, user-defined name for the ACL pattern entry.
Base	Specifies one of the following as the user-defined header for the access control entries (ACE) of the ACL.
	• none • macSrcBegin • ipHdrBegin • ipTosBegin • ipDstBegin • tcpDstportBegin • udpSrcportBegin • ipHdrEnd • updEnd • etherBegin • ethTypeLenBegin • ipOptionsBegin • ipProtoBegin • tcpBegin • tcpFlagsEnd • udpDstportBegin • icmpMsgBegin • ipv6HdrBegin • macDstBegin • arpBegin • ipPayloadBegin • ipSrcBegin • tcpSrcportBegin • udpBegin • etherEnd • tcpEnd
Offset	Set the offset in bits to the beginning offset of the user-defined field with the selected header option as a base. Valid values range from 0–76800.
Length	Configures the number of bits to extract from the beginning of the offset. Valid values range from 1–56.

Inserting an ACL

An ACL comprises an ordered list of filter rules or ACEs. The ACEs provide specific actions that you configure. After you configure an ACE, when a packet meets the match criteria specified in one or more ACEs within an ACL, the corresponding action runs.

ATTENTION
If you configured any IPv6 attributes on the ACT, you must select IPv6 in the PktType field when you insert the ACL. If an ACT uses only Ethernet attributes, you can configure a single IPv4 ACL and a single IPv6 ACL.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Click **Insert**.
5	Type an ACL ID from 1 through 4096.
6	Select the act ID by clicking the ellipsis button (**...**).
7	Click **OK**.
8	Specify the ACL type.
9	Type a name for the ACL entry.
10	In the **VlanList** box, click the button and select the required entry.
11	In the **PortList** box, click the button and select the required entry.
12	Specify the **DefaultAction** and the **GlobalAction**.
13	Enable or disable the state.
14	In the **PktType** box, select the IPv6 option.
15	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the ACL.

Variable	Value
AclId	Specifies a unique identifier for the ACL entry in the range 1–4096.
ActId	Specifies a unique identifier for the ACT entry in the range 1–4096.

Variable	Value
Type	Specifies whether the ACL is VLAN or port-based. Valid options: • inVlan • outVlan • inPort • outPort **ATTENTION** The inVlan and outVlan ACL types drop packets if the VLAN is added after ACE creation. For VLAN-based filters, ensure that the ACE configuration is set to all R or RS module slots, regardless of the VLAN port membership on a slot.
Name	Specifies a descriptive user-defined name for the ACL entry.
VlanList	Identifies an array indicating all the VLANs associated with the ACL entry. The value is used only with inVlan and outVlan ACL types.
PortList	Specifies the ports added to the ACL entry. The value is used only with inPort and outPort ACL types.
DefaultAction	Specifies the action taken when no ACEs in the ACL match. Valid options are deny and permit, with permit as the default.
GlobalAction	Indicates the action applied to all ACEs that match in an ACL: • none • mirror • count • mirror-count **ATTENTION** Mirroring is not supported for egress filters in the Nortel Ethernet Routing Switch 8600 Release 4.1 software.

Variable	Value
State	Enables or disables all of the ACEs in the ACL. The default value is enable.
PktType	Specifies if the packet type is IPv4 or IPv6.

Modifying an ACL

Modify an ACL to change the configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Double-click the field you want to change. For example, if you double-click the GlobalAction field, you can select from several options in the activated list.
5	Select the required option.
6	Click **Apply**to commit the required action.

--End--

Inserting ACE common entries

Insert access control entries (ACE) to add an ACE to an ACL.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Select the ACL to which to add an ACE.
5	Click the **ACE** button.
6	Click **Insert**.
7	Type data in the required fields.

8 Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the ACE.

Variable	Value
AceId	Specifies a unique identifier and priority for the ACE.
Name	Specifies a descriptive, user-defined name for the ACE entry. The system automatically assigns a name if you do not choose one.
Mode	Indicates the operating mode associated with the ACE. Valid options are deny and permit, with none as the default.
MltIndex	Specifies whether to override the MLT index picked by the MLT algorithm when a packet is sent on MLT ports. Valid values range 0–8, with 0 as the default.
RemarkDscp	Specifies whether the Differentiated Services Code Point (DSCP) field value marks non standard traffic classes and local use Per Hop Behavior (PHB). The default is disable.
RemarkDot1Priority	Specifies whether Dot1 Priority as described by Layer 2 standards, 802.1Q, and 802.1P is enabled. The default is disable.
Police	Configures the desired policing profile identifier. Valid values range from 0–16383, with zero (0) as the default. When policing is not desired, you must configure the value to zero.
RedirectNextHop	Redirects matching IP traffic to the next hop.
RedirectUnreach	Configures the desired behavior for redirected traffic in case the specified next hop is not reachable. The default value is deny.

Variable	Value
EgressQueue	Specifies the egress queue for 10/100 GbE module. • If you specify only 1 value, then this value is applied to the 1 Gb and 10 Gb queues as well. • If you specify 2 values, then the first value is applied to the 10/100 module and the second value is applied to 1 Gb and 10 Gb modules. • If you specify all three values, then all three values apply respectively to the appropriate egress queue. • If you specify a value greater than 8, it is not applied to the 10/100 GbE module because it uses only 8 queues. However, the value is applied only to the 1 Gb and 10 Gb module types. The default value is 64.
EgressQueue1g	Specifies the egress queue for the 1 Gb module. The default value is 64.
EgressQueue10g	Specifies the egress queue for the 10 Gb module. The default value is 64.
EgressQueueNNSC	Identifies the configured ACE Nortel Networks Service Class (NNSC). The default is disable.
StopOnMatch	Indicates whether to stop or continue if an ACE matching the packet is found. When a match occurs, the switch does not attempt a match on the other ACEs with a lower priority.
Flags	Specifies one of the following flag values: • none: Default value for the flags. • count: Enables or disables counting if a packet matching the ACE is found. • copyToPrimaryCp: Enables or disables the copying of matching packets to the primary CP. • copyToSecondaryCp: Enables or disables the copying of matching packets to the secondary CP. • mirror: Enables or disables mirroring the matching packets to an interface. The Nortel Ethernet Routing Switch 8600 mirrors one port or mirrors to one port.

Variable	Value
IPfixState	Enables or disables IP flow information export (IPfix).
RedirectNextHopIpv6	The IPv6 address to redirect the next hop.

Modifying ACE common entries

Modify ACE common entries to change the current configuration.

ATTENTION
Except the debug actions, disable the AdminState of the ACE before you perform any modifications.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Select the ACL.
5	Click the **ACE** button.
6	Double-click a field you want to change. For example, if you double-click on the Mode field, you can select from several options in the activated list.
7	Select the required option.
8	Click **Apply**to commit the action.

--End--

Configuring a list of IPv6 source IP addresses for an ACE

Configure an ACE IPv6 source address so that the filter looks for a specific IPv6 source address.

Prerequisites

- The associated ACL packet type must be IPv6.
- The associated ACT IPv6 attributes must be srcIpv6

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Select an IPv6 ACL.
5	Click **ACE**.
6	From the ACE Common tab, select an ACE.
7	Click**IPv6**.
8	Click **Insert**.
9	Specify the operation (the only option is eq [equals]) and the IPv6 addresses.
10	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the Source Address tab.

Variable	Value
AclId	Specifies the ACL ID.
AceId	Specifies the ACE ID.
Oper	Specifies the ACE operation. The only option is eq (equals).
List	Specifies the IPv6 addresses—a binary string of 16 octets in network byte-order. Enter a single IPv6 address, range of IPv6 addresses, or multiple IPv6 addresses.

Configuring a list of IPv6 destination IP addresses for an ACE

Configure an ACE IPv6 destination address to have the filter look for a specific IPv6 destination address.

Prerequisites

- The associated ACL packet type must be IPv6.
- The associated ACT IPv6 attributes must be dstIpv6.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Select an IPv6 ACL.
5	Click **ACE**.
6	From the ACE Common tab, select an ACE.
7	Click**IPv6**.
8	Click the **Destination Address** tab.
9	Click **Insert**.
10	Specify the operation (the only option is eq [equals]) and the IPv6 addresses.
11	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the Destination Address tab.

Variable	Value
AclId	Specifies the ACL ID.
AceId	Specifies the ACE ID.
Oper	Select eq to specify IPv6 addresses equal to the addresses included in the List field.
List	Type a single IPv6 address, range of IPv6 addresses, or multiple IPv6 addresses.

Configuring an IPv6 next header rule for an ACE

Configure an ACE IPv6 next header so that the filter looks for a packets with the next header parameter set.

Prerequisites

- The associated ACL packet type must be IPv6.
- The associated ACT IPv6 attributes must be nxtHdr.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
	The ACL box appears with the ACL tab displayed.
4	Select an IPv6 ACL.
5	Click **ACE**.
6	Select an ACE.
7	Click**IPv6**.
8	Click the **Next Hdr** tab.
9	Click **Insert**.
10	Specify the operation and the Next header parameters.
11	Click **Insert**.

--End--

Variable definitions

Use the data in the following table to configure the next header rule.

Variable	Value
AclId	Specifies the ACL ID.
AceId	Specifies the ACE ID.
Oper	Specifies the ACE operation. The options are eq (equal) or ne (not equal).
NxtHdr	Specifies the next header. .

Deleting an ACT

Delete an ACT to remove it from the configuration.

> **ATTENTION**
> You cannot delete or modify an ACT associated with ACLS.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Select the **ActId** or name of the ACT to delete.
4	Click **Delete**.

--End--

Deleting an ACL

Delete an ACL to remove it from the configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Select the ACL to delete.
5	Click **Delete** to remove the selected ACL.
	A dialog box prompts you to confirm the deletion.
6	Click **Yes** to delete the ACL.

--End--

Deleting ACE common entries

Delete ACE common entries to remove them from the configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Select the ACL.

5. Click the **ACE** button.
6. Select the name of the ACE common entry to delete.
7. Click **Delete** to remove the selected entry.

--End--

IPv6 traffic filter configuration using the CLI

This chapter describes how to block unwanted traffic from entering a switch or to prioritize desired traffic. Traffic filters instruct an interface to selectively handle specified traffic. The switch determines which packets receive special handling based on information in the packet headers.

Using traffic filters, you can reduce network congestion and control access to network resources by blocking, forwarding, or prioritizing specified traffic on an interface. You can apply multiple traffic filters to a single interface.

For conceptual information about traffic filtering, see "IPv6 routing fundamentals" (page 25).

For additional information about filters, see *Nortel Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for R and RS Modules* (NN46205-507) .

IPv6 traffic filter configuration navigation

Job aid: Roadmap of traffic filter CLI commands

The following table lists the commands and parameters that you use to perform the procedures in this chapter.

Table 29
Job aid: Roadmap of traffic filter CLI commands

Command	Parameter
config filter acl <acl-id>	create <type> act <value> [pktType] <value> [name <value>]
	delete
	enable
	disable
	name <value>
	info
config filter acl <acl-id> ace <ace-id>	create [name <value>]
	delete
	enable
	disable
	name <value>
	info
config filter acl <acl-id> ace <ace-id> advanced	custom-filter1<pattern1-name><ace-op><value>
	custom-filter2<pattern2-name><ace-op><value>
	custom-filter3<pattern3-name><ace-op><value>
	delete
config filter acl <acl-id> ace <ace-id> ipv6	delete <ipv6-attributes>
	dst-ipv6 <ace-op> <dst-ipv6-list>
	info
	src-ipv6 <ace-op> <src-ipv6-list>
	nxt-hdr <ace-op> <nxt-hdr>
config filter acl <acl-id> port	add <ports>
	remove <ports>
	info
config filter acl <acl-id> set	default-action <value>
	global-action <value>
	info

Table 29
Job aid: Roadmap of traffic filter CLI commands (cont'd.)

Command	Parameter
`config filter acl <acl-id> vlan`	`add <vid> [<vid2-vid3>]`
	`remove <vid> [<vid2-vid3>]`
	`info`
`config filter act <act-id>`	`create [name <value>]`
	`delete`
	`apply`
	`name <value>`
	`info`
	`arp <arp-attributes>`
	`ip <ip-attributes>`
	`ipv6 <ipv6-attributes>`
	`ethernet <ethernet-attributes>`
	`protocol <protocol-attributes>`
`config filter act <act-id> pattern <pattern-name>`	`add <base> <offset> <length>`
	`name <pattern-name>`
	`info`

Configuring ACTs

Configure an access control template (ACT) to create, delete, apply, and specify attributes. After you apply the ACT you cannot change the attributes. ACT IDs 4001 to 4096 are reserved for system-defined ACTs.

System-defined ACTs are available for filters as required.

ATTENTION
An ACT can use IPv4 or IPv6 attributes, but not both. You cannot combine IPv4 and IPv6 attributes in the same ACL.

Procedure steps

Step	Action
1	Configure an ACT by using the following command: `config filter act <act-id>`

--End--

Variable definitions

Use the data in the following table to use the **config filter act** command.

Variable	Value
act-id	Specifies an ACT ID in the range 1–4096.
apply	Applies or commits the ACT. After the switch issues the command, you can make changes to the ACT only by first deleting it if no ACLs are associated with the ACT.
arp <arp-attributes>	Specifies the permitted ARP attributes for the ACT template. The list of allowed attributes must be separated by commas and includes, [none | operation]
create [name <value>]	Creates an ACT. **Name <value>** is an optional parameter that specifies a descriptive name for the ACT using 0–32 characters. If you do not enter a name, a default name is generated, for example, ACT-1 for act-id = 1. **ATTENTION** In the Nortel Ethernet Routing Switch 8600, act-id acts as an index to the ACT table. Thus, you can change the name at any time, even after you apply it.
delete	Deletes an ACT only when no ACLs are associated with the ACT.
ethernet <ethernet-attributes>	Specifies the permitted Ethernet attributes for the ACT template. The list of allowed attributes must be separated by commas and includes, [none | srcMac, dstMac, etherType, [portvlan], vlanTagPrio]. **ATTENTION** 1. You can select port or vlan-id, but not both. 2. If you select none, • The entry deletes the Ethernet node. • The entry prevents you from selecting any other attribute choices.

Variable	Value
info	Information about the ACTs that you created.
ip <ip-attributes>	Specifies the permitted IP attributes for the ACT template. The list of allowed attributes must be separated by commas and includes, [none | srcIp, dstIp, ipFragFlag, ipOptions, ipProtoType, dscp].
ipv6 <ipv6-attributes>	Specifies the permitted IPv6 for the ACT template. The list of allowed attributes must be separated by commas and includes, [none | srcIpv6, dstIpv6, nextHdr]
name <value>	Specifies a name for the ACT. **<value>** is an optional parameter that specifies a name for the ACT using 0–32 characters.
protocol <protocol-attributes>	Specifies the permitted protocol attributes for the ACT template. The list of allowed attributes must be separated by commas and includes, [none | tcpSrcPort, udpSrcPort, tcpDstPort, udpDstPort, tcpFlags, icmpMsgFlags]

Creating a template for user-created patterns

Create a template for patterns within an ACT. You can associate a maximum of three patterns with an ACT.

Procedure steps

Step	Action
1	Create a template by using the following command: **config filter act <act-id> pattern <pattern-name>**

--End--

Variable definitions

Use the data in the following table to use the **config filter act pattern** command.

Variable	Value
act-id	Specifies an ACT ID in the range of 1–4096.
add <base> <offset> <length>	Adds a template for patterns you create. Options include: • base: the base and the offset together determine the beginning of the pattern. Permitted values for the base include the following: — ether-begin — mac-dst-begin — mac-src-begin — ethTypeLen-begin — arp-begin — ip-hdr-begin — ip-options-begin — ip-payload-begin — ip-tos-begin — ip-proto-begin — ip-src-begin — ip-dst-begin — ipv6-hdr-begin — tcp-begin — tcp-srcport-begin — tcp-dstport-begin — tcp-flags-end — udp-begin — udp-srcport-begin — udp-dstport-begin — ether-end — ip-hdr-end — icmp-msg-begin — tcp-end — udp-end • offset: the number of bits from the base where the pattern starts. • length: the length in bits of the user-defined field from 1–56.

Variable	Value
`info`	Displays information about the template patterns you created under an ACT.
`name <pattern-name>`	Renames the pattern with a new name that you define. Each of the three patterns must use a unique name.
`patternname`	Specifies a pattern name with a range 0–32 characters.

Applying the ACT

After you create and configure the ACT, apply it to implement the configuration.

Procedure steps

Step	Action
1	Apply the ACT by using the following command: **`configure filter act <act id> apply`**

--End--

Configuring ACLs

Configure access control lists (ACL) to create lists of rules for the ACT.

> **ATTENTION**
> If the ACT contains IPv6 attributes, you must configure an ACL of pktType IPv6. If the ACT uses only Ethernet attributes, you can configure one ACL of pktType IPv4 and an ACL of pktType IPv6.

Procedure steps

Step	Action
1	Configure an ACL by using the following command: **`config filter acl <acl-id>`**

--End--

Variable definitions

Use the data in the following table to use the **`config filter acl`** command.

Variable	Value
`acl-id`	Specifies an ACL ID in the range 1–4096.

Variable	Value
`create <type> act <value> [pktType] <value> [name <value> ]`	Creates an access control list (ACL) only when an ACT is associated with that ACL: • `<type>`: type of ACL, including [InVlan | outVlan | InPort | outPort]. • `act <value>`: an ACT template ID in the range from 1–4096. • `pktType <value>`: ipv4 or ipv6 • `name <value>`: an optional parameter that specifies a descriptive name for the ACL using 0–31 characters. If you do not enter a name when you create the ACL, a default name is generated, for example, ACL-2 for acl-id = 2 **ATTENTION** The pktType field is optional for IPv4 traffic filters. It is required if you apply the ACL to IPv6 packets.
`delete`	Deletes an ACL. **ATTENTION** This command removes all VLANs or brouter ports under this ACL and deletes all ACEs. The command does not delete the ACTs.
`disable`	Disables the ACL state along with all of the ACEs below it. The default value is disable.
`enable`	Enables the ACL state along with all of the ACEs below it. Enable is the default state for the ACL.
`info`	Displays information about the ACL.
`name <value>`	Renames an ACL.

Configuring global and default actions for an ACL

Configure global and default actions for an ACL to apply the configuration globally.

Procedure steps

Step	Action
1	Configure global and default actions by using the following command: **`config filter acl <acl-id> set`**

--End--

Variable definitions

Use the data in the following table to use the **`config filter acl set`** command.

Variable	Value
`acl-id`	Specifies an ACL ID in the range of 1–4096.
`default-action <value>`	Specifies the default action when no ACEs match. Permitted options include [deny | permit], with a default of permit.
`global-action <value>`	Specifies the global action for the matching ACEs. Permitted options include [none | mirror | count | mirror-count|ipfix|mirror-ipfix|count-ipfix|mirror-count-ipfix]. The default is none.
`info`	Displays the status of the global and default actions.

Associating VLANs for an ACL

Associate or remove VLANs for a particular ACL.

Procedure steps

Step	Action
1	Associate or remove VLANs by using the following command: **`config filter acl <acl-id> vlan`**

--End--

Variable definitions

Use the data in the following table to use the **`config filter acl vlan`** command.

Variable	Value
`acl-id`	Specifies an ACL ID in the range of 1–4096.

Variable	Value
`add <vid> [ <vid2-vid3>]`	Associates a VLAN or a VLAN list with a particular ACL. `<vid>` is a list of VLANs separated by a comma or a range of VLANs specified as low-high [vlan-id -vlan-id].
`info`	Displays the ACL VLAN status.
`remove <vid> [ <vid2-vid3> ]`	Removes a VLAN or VLAN list from a particular ACL. `<vid>` is a list of VLANs separated by a comma or a range of VLANs specified as low-high [vlan-id -vlan-id].

Associating ports for an ACL

Associate or remove ports for a particular ACL.

Procedure steps

Step	Action
1	Associate or remove ports by using the following command: **`config filter acl <acl-id> port`**

--End--

Variable definitions

Use the data in the following table to use the **`config filter acl port`** command.

Variable	Value
`acl-id`	Specifies an ACL ID in the range 1–4096.
`add <ports> ]`	Associates a port or a port list with a particular ACL. `<ports>` is a list of ports separated by a comma or a range of ports specified as low-high [slot/port-slot/port].
`info`	Displays the ACL port status.
`remove <ports>`	Removes a port or a port list from a particular ACL. `<ports>` is a list of ports separated by a comma or a range of ports specified as low-high [slot/port-slot/port].

Adding an ACE with IPv6 header attributes

Add an ACE with IP header attributes as match criteria.

ATTENTION

Be aware of the following:

- You cannot select (*) after <ace-op>.
- If you select no entry, You delete the Ethernet, ARP, or IPv6 protocol node.

Procedure steps

Step	Action
1	Add an ACE with IPv6 header attributes by using the following command: **`config filter acl <acl-id> ace <ace-id> ipv6`**

--End--

Variable definitions

Use the data in the following table to use the **`config filter acl ace ipv6`** command.

Variable	Value
`ace-id`	Specifies an ACE ID in the range 1–1000.
`acl-id`	Specifies an ACL ID in the range 1–4096.
`delete <ipv6-attributes>`	Deletes the specified IPv6 ACE attributes.
`dst-ipv6 <ace-op> <dst-ipv6-list>`	Specifies the following: • an operator for a field match condition (eq) • the list of destination IPv6 addresses separated by commas
`info`	Displays the current level parameter setting and the next level directories.
`nxt-hdr <ace-op> <nxt-hdr>`	Specifies the following: • an operator for a field match condition (eq | ne) • the next header value
`src-ipv6 <ace-op> <src-ipv6-list>`	Specifies the following: • an operator for a field match condition (eq) • the list of source IPv6 addresses separated by commas

IPv6 traffic filter configuration using the NNCLI

This chapter describes how to block unwanted traffic from entering a switch or to prioritize desired traffic. Traffic filters instruct an interface to selectively handle specified traffic. The switch determines which packets receive special handling based on information in the packet headers.

Using traffic filters, you can reduce network congestion and control access to network resources by blocking, forwarding, or prioritizing specified traffic on an interface. You can apply multiple traffic filters to a single interface.

For conceptual information about traffic filtering, see "IPv6 routing fundamentals" (page 25).

For additional information about filters, see *Nortel Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for R and RS Modules* (NN46205-507).

IPv6 traffic filter configuration navigation

Job aid: Roadmap of traffic filter NNCLI commands

The following table lists the commands and parameters that you use to perform the procedures in this chapter.

Table 30
Job aid: Roadmap of traffic filter NNCLI commands

Command	Parameter
Privileged EXEC mode	
`filter apply act <act-id>`	—
Global Configuration mode	
`filter acl <acl-id>`	`enable`
	`name <word>`
	`type <inVlan|outVlan|inPort|outPort>`
	`act <act-id>`
	`pktType <ipv4|ipv6>`
`filter acl ace ipv6 <acl-id> <ace-id>`	`dst-ipv6 eq <word>`
	`nxt-hdr <eq|ne> <next-header>`
	`src-ipv6 eq <word>`
`filter acl port <acl-id> <port>`	—
`filter acl set <acl-id>`	`default-action <value>`
	`global-action <value>`
`filter acl vlan <acl-id> <vlan-id>`	—
`filter act <act-id>`	`arp <operation>`
	`ethernet <word>`
	`ip <word>`
	`ipv6 <word>`
	`name <word>`
	`protocol <word>`
`filter act pattern <act-id>`	`<word>`
	`<base> <offset> <length>`
	`name <pattern-name>`

Configuring ACTs

Configure an access control template (ACT) to create, delete, apply, and specify attributes. After you apply the ACT you cannot change the attributes. ACT IDs 4001 to 4096 are reserved for system-defined ACTs.

System-defined ACTs are available for filters as required.

> **ATTENTION**
> An ACT can use IPv4 or IPv6 attributes, but not both. You cannot combine IPv4 and IPv6 attributes in the same ACL.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create an ACT by assigning it an ID by using the following command: **`filter act <act-id>`**
2	Configure parameters for the ACT by using the following command: **`filter act <act-id> [arp <operation>] [ethernet <word>] [ip <word>] [ipv6 <word>] [name <word>] [protocol <word>]`**

--End--

Variable definitions

Use the data in the following table to use the **`filter act`** command.

Variable	Value
`act-id`	Specifies an ACT ID in the range 1–4096. **ATTENTION** In the Nortel Ethernet Routing Switch 8600, act-id is an index to the ACT table. Thus, you can change the name at any time, even after you apply it. To configure this option to the default value, use the **`default`** operator with the command.
`arp <operation>`	Specifies the permitted ARP attributes for the ACT template. The list of allowed attributes must be separated by commas and includes: [operation]

<table>
<tr><th>Variable</th><th>Value</th></tr>
<tr><td>ethernet <word></td><td>Specifies the permitted Ethernet attributes for the ACT template. The list of allowed attributes must be separated by commas and includes:

[none | srcMac, dstMac, etherType, [portvlan], vlanTagPrio].

ATTENTION
1. You can select port or vlan-id, but not both.
2. If you select none:
• The entry deletes the Ethernet node.
• The entry prevents you from selecting any other attribute choices.</td></tr>
<tr><td>ip <word></td><td>Specifies the permitted IP attributes for the ACT template. The list of allowed attributes must be separated by commas and includes:

[none | srcIp, dstIp, ipFragFlag, ipOptions, ipProtoType, dscp].</td></tr>
<tr><td>ipv6 <word></td><td>Specifies the permitted IPv6 for the ACT template. The list of allowed attributes must be separated by commas and includes:

[none | srcIpv6, dstIpv6, nextHdr]</td></tr>
<tr><td>name <word></td><td>Specifies a name for the ACT. <word> is an optional parameter that specifies a name for the ACT using 0–32 characters. If you do not enter a name, a default name is generated, for example, ACT-1 for act-id = 1.</td></tr>
<tr><td>protocol <word></td><td>Specifies the permitted protocol attributes for the ACT template. The list of allowed attributes must be separated by commas and includes:

[none | tcpSrcPort, udpSrcPort, tcpDstPort, udpDstPort, tcpFlags, icmpMsgFlags]</td></tr>
</table>

Creating a template for user-created patterns

Ceate a template for patterns within an ACT. You can associate a maximum of three patterns with an ACT.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create a template by using the following command: `filter act pattern <act-id> <word> <base> <offset> <length>`

--End--

Variable definitions

Use the data in the following table to use the **`filter act pattern`** command.

Variable	Value
`act-id`	Specifies an ACT ID in the range of 1–4096.
`<base> <offset> <length>`	Adds a template for patterns you create: • base: the base and the offset together determine the beginning of the pattern. Permitted values for the base include the following: — ether-begin — mac-dst-begin — mac-src-begin — ethTypeLen-begin — arp-begin — ip-hdr-begin — ip-options-begin — ip-payload-begin — ip-tos-begin — ip-proto-begin — ip-src-begin — ip-dst-begin — ipv6-hdr-begin — tcp-begin — tcp-srcport-begin

Variable	Value
	— tcp-dstport-begin — tcp-flags-end — udp-begin — udp-srcport-begin — udp-dstport-begin — ether-end — ip-hdr-end — icmp-msg-begin — tcp-end — udp-end • offset: the number of bits from the base where the pattern starts. This is a range from 0–76800. • length: the length in bits of the user-defined field from 1–56.
name <pattern-name>	Renames the pattern with a new name that you define. Each of the three patterns must have a unique name.
word	Specifies a name for the pattern in the range of 1–32 characters. To set this option to the default value, use the **default** operator with the command.

Applying the ACT

After you create and configure the ACT, apply it to implement the configuration.

Prerequisites

- You must log on to the Privileged EXEC mode in the NNCLI.

Procedure steps

Step	Action
1	Apply the ACT by using the following command: **filter apply act <act-id>**

--End--

Configuring ACLs

Configure access control lists (ACL) to create rules for the ACT.

> **ATTENTION**
> If an ACT contains IPv6 attributes, you must configure an ACL of pktType IPv6. If the ACT uses only Ethernet attributes, you can configure one ACL of pktType IPv4 and an ACL of pktType IPv6.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure an ACL by using the following command: **`filter acl <acl-id> type <inVlan|outVlan|inPort|outPort> act <act-id> pktType <ipv4|ipv6> name <word>`**
2	Enable an ACL by using the following command: **`filter acl <acl-id> enable`**

--End--

Variable definitions

Use the data in the following table to use the **`filter acl`** command.

Variable	Value
`acl-id`	Specifies an ACL ID in the range 1–4096.
`act <act-id>`	Specifies the ACT ID to associate with the ACL.
`enable`	Enables the ACL state along with all ACEs below it. Enable is the default state for the ACL.
`name <word>`	Renames an ACL. To configure this option to the default value, use the **`default`** operator with the command.
`pktType <ipv4|ipv6>`	Configures the packet type for the ACL. **ATTENTION** The pktType field is optional for IPv4 traffic filters. It is required if you apply the ACL to IPv6 packets.
`type <inVlan|outVlan|inPort|outPort>`	Configures the type of ACL.

Configuring global and default actions for an ACL

Configure global and default actions for an ACL to globally apply the configuration.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure default actions by using the following command: **`filter acl set <acl-id> default-action <value>`**
2	Configure global actions by using the following command: **`filter acl set <acl-id> global-action <value>`**

--End--

Variable definitions

Use the data in the following table to use the **`filter acl set`** command.

Variable	Value
`acl-id`	Specifies an ACL ID in the range of 1–4096.
`default-action <value>`	Specifies the default action when no ACEs match. Permitted options include [deny|permit], with a default of permit. To configure this option to the default value, use the **`default`** operator with the command.
`global-action <value>`	Specifies the global action for the matching ACEs. Permitted options include [none|count|count-ipfix|ipfix|mirror|mirror-count|mirror-count-ipfix|mirror-ipfix]. The default is none. To configure this option to the default value, use the **`default`** operator with the command.

Associating VLANs for an ACL

Associate or remove VLANs for a an ACL.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Associate or remove VLANs by using the following command: `filter acl vlan <acl-id> <vlan-id>`

--End--

Variable definitions

Use the data in the following table to use the **filter acl vlan** command.

Variable	Value
acl-id	Specifies an ACL ID in the range of 1–4096. To configure this option to the default value, use the **default** operator with the command.
vlan-id	Associates a VLAN or a VLAN list with a particular ACL. Format a list of VLANs separated by a comma or a range of VLANs specified as low-high [vlan-id -vlan-id]. To configure this option to the default value, use the **default** operator with the command.

Associating ports for an ACL

Associate or remove ports for an ACL.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Associate or remove ports by using the following command: `filter acl port <acl-id> <port>`

--End--

Variable definitions

Use the data in the following table to use the **filter acl port** command.

Variable	Value
acl-id	Specifies an ACL ID in the range 1–4096.
port	Associates a port or a port list with a particular ACL. Format a list of ports separated by a comma or a range of ports specified as low-high [slot/port -slot/port].

Adding an ACE with IPv6 header attributes

Add an ACE with IP header attributes as match criteria.

> **ATTENTION**
> Be aware of the following:
>
> - You cannot select (*) after <ace-op>.
> - If you select no entry, it indicates that you want to delete the respective Ethernet, ARP, or IPv6 protocol node.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Add an ACE with IPv6 header attributes by using the following command: **filter acl ace ipv6 <acl-id> <ace-id> [dst-ipv6 eq <word>] [nxt-hdr <eq|ne> <next-header>] [src-ipv6 eq <word>]**

--End--

Variable definitions

Use the data in the following table to use the **filter acl ace ipv6** command.

Variable	Value
ace-id	Specifies an ACE ID in the range 1–1000. To configure this option to the default value, use the **default** operator with the command.
acl-id	Specifies an ACL ID in the range 1–4096. To configure this option to the default value, use the **default** operator with the command.

Variable	Value
dst-ipv6 eq <word>	Specifies the following: • an operator for a field match condition—eq • the list of destination IPv6 addresses separated by commas
nxt-hdr <eq|ne> <nxt-hdr>	Specifies the following: • an operator for a field match condition (eq | ne) • the next header value from one of the following: fragment|hop-by-hop|icmpv6|ipsecah|ipsecesp|noHdr|routing|tcp|udp|undefined
src-ipv6 eq <word>	Specifies the following: • an operator for a field match condition—eq • the list of source IPv6 addresses separated by commas

Interoperability

The Nortel Ethernet Routing Switch 8600 provides interoperability with servers running Linux and Windows XP. This chapter provides basic configuration and verification procedures for the various systems.

Interoperability navigation

Enabling IPv6 in Windows XP

Enable IPv6 to add IPv6 functionality on the Windows XP system.

Procedure steps

Step	Action
1	Open the command prompt.
2	At the prompt, enter **`ipv6 install`**.

--End--

Pinging the switch from a Windows XP system

Ping the switch to test connectivity.

Procedure steps

Step	Action

1	At the command prompt on a Windows XP system, ping the switch by using the following command:
	`ping <IPv6 address>%interface ID`
	For example:
	`C:\Documents and Settings\userid>ping fe80::240:5ff:fe31:ce1d%5`

--End--

Job aid: sample ping output

Figure 18 "Job aid: Ping from a Windows XP system" (page 368) shows sample output for pinging the Nortel Ethernet Routing Switch 8600 from a Windows XP system.

Figure 18
Job aid: Ping from a Windows XP system

```
Pinging fe80::240:5ff:fe31:ce1d%5 with 32 bytes of data:
Reply from fe80::240:5ff:fe31:ce1d%5: time<1ms
Reply from fe80::240:5ff:fe31:ce1d%5: time<1ms
Reply from fe80::240:5ff:fe31:ce1d%5: time<1ms
Reply from fe80::240:5ff:fe31:ce1d%5: time<1ms
Ping statistics for fe80::240:5ff:fe31:ce1d%5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Enabling IPv6 in Linux

Enable IPv6 to allow IPv6 functionality on the Linux system. (This procedure is specific to Redhat Linux systems. For other Linux systems, see the appropriate system instructions.)

Procedure steps

Step	Action

1	Type the following command on the Linux system in /etc/sysconfig/network:
	`NETWORKING_IPV6=yes`
	`IPV6INIT=yes`

2 Reboot the Linux system.

--End--

Pinging the Linux system from the switch

Ping the Linux system from the switch by using Enterprise Device Manager to test connectivity.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Device**, **Open**. **OR** From the Device Manager toolbar, click **Open Device**.
2	In the **Device Name** box, identify the device: `<ipv6 address>%interface num=number of ping messages` For example: `f8a:0:0:0:0:0:203:1%eth0 num=1`

--End--

Pinging the Nortel Ethernet Routing Switch 8600 from the Linux system

Ping the switch from the Linux system to test connectivity.

Procedure steps

Step	Action
1	Enter the following command on the Linux system to test communication with the Nortel Ethernet Routing Switch 8600: `# ping6 interface number <8600 IPv6 address>%<interface number>`

--End--

Example of pinging the switch from a Linux system

Procedure steps

Step	Action
1	Ping the switch:

```
# ping6 -I eth0 58a:0:0:0:0:0:204:1
```

--End--

Job aid: Sample ping output

Figure 19 "Job aid: Ping from a LINUX system" (page 370) shows sample output for pinging the switch from a LINUX system.

Figure 19
Job aid: Ping from a LINUX system

```
sspc-127# ping6 fe80::2a0:ccff:fe41:9ce9%dc0
PING6(56=40+8+8 bytes) fe80::2a0:ccff:fe41:9ce9%dc0 -->
fe80::2a0:ccff:fe41:9ce9%dc0 16 bytes from
fe80::2a0:ccff:fe41:9ce9%dc0, icmp_seq=0 hlim=64 time=0.704 ms
16 bytes from fe80::2a0:ccff:fe41:9ce9%dc0, icmp_seq=1 hlim=64
time=0.219 ms 16 bytes from fe80::2a0:ccff:fe41:9ce9%dc0,
icmp_seq=2 hlim=64 time=0.217 ms 16 bytes from
fe80::2a0:ccff:fe41:9ce9%dc0, icmp_seq=3 hlim=64 time=0.216 ms
^C
--- fe80::2a0:ccff:fe41:9ce9%dc0 ping6 statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.216/0.339/0.704/0.211 ms
```

Assigning IPv6 addresses to the Linux system

Assign IPv6 addresses to interfaces on the Linux system.

Procedure steps

Step	Action
1	Navigate to /etc/sysconfig/network-scripts/ifcfg-<interface number>.
2	Enter the following command: **IPV6ADDR=<ipv6 address>**
3	Add IPv6 addresses, if required, by using the following command: **#ifconfig <interface number> inet6 add <IPv6 address>**

--End--

Viewing IPv6 neighbors from the Linux system

View IPv6 neighbors from the Linux system.

Procedure steps

Step	Action
1	View IPv6 neighbors by using the following command: **# /sbin/ip -6 neigh show**

--End--

Common procedures using Enterprise Device Manager

This chapter provides common procedures that you use to configure IPv6 routing on the Nortel Ethernet Routing Switch 8600.

Common procedures navigation

Viewing advertisements in the link-state database

View the advertisements of areas throughout the link-state database (LSDB).

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **OSPF**.

3 Click the **Area-scope LSDB** tab.

--End--

Variable definitions

Use the data in the following table to use the Area-scope LSDB tab.

Variable	Value
AreaId	A read-only field indicating the 32-bit integer that uniquely identifies an area. Area ID 0.0.0.0 is used for the OSPF backbone.
Type	A read-only field indicating the OSPF interface type. By default, switches can determine this value from the corresponding value of ifType. Broadcast LANs, such as Ethernet and IEEE 802.5, use the value broadcast; X.25 and similar technologies use the value nbma; and point-to-point links use the value pointToPoint.
RouterId	A read-only field indicating the 32-bit integer that uniquely identifies the router in the autonomous system.
Lsid	A read-only field indicating that the link-state ID is an LS type-specific field containing either a router ID or an IPv6 address. It identifies the piece of the routing domain described by the advertisement.
Sequence	A read-only field indicating that the sequence number is a signed 32-bit integer that identifies old and duplicate link-state advertisements.
Age	A read-only field indicating the age in seconds of the link-state advertisement.
Checksum	A read-only field indicating the checksum of the complete contents of the advertisement, except the age field. The age field is not included so that the advertisement age increments without updating the checksum. The checksum used is the same for Industry Standards Organization (ISO) connectionless datagrams, the Fletcher checksum.
TypeKnown	A read-only field indicating the LSA type recognized by this router.

Viewing characteristics in the AS-scope link-state database

View the characteristics of the autonomous system (AS)-scope link-state database.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **AS-scope LSDB** tab.

--End--

Variable definitions

Use the data in the following table to use the AS-scope LSDB tab.

Variable	Value
Type	A read-only field indicating the OSPF interface type. By default, switches can determine this value from the corresponding value of ifType. Broadcast LANs, such as Ethernet and IEEE 802.5, use the value broadcast; X.25 and similar technologies use the value nbma; and point-to-point links use the value pointToPoint.
RouterId	A read-only field indicating the 32-bit integer that uniquely identifies the router in the autonomous system.
Lsid	A read-only field indicating that the link-state ID is an LS type-specific field containing either a router ID or an IPv6 address. It identifies the piece of the routing domain described by the advertisement.
Sequence	A read-only field indicating that the sequence number is a signed 32-bit integer that identifies old and duplicate link-state advertisements.
Age	A read-only field indicating the age in seconds of the link-state advertisement.
Checksum	A read-only field indicating the checksum of the complete contents of the advertisement, except the age field. The age field is not affected so that the advertisement age value increments without updating the checksum. The checksum used is the same for ISO connectionless datagrams, the Fletcher checksum.
TypeKnown	A read-only field indicating the LSA type recognized by this router.

Viewing characteristics in the Link-scope link-state database

View the characteristics of the Link-scope link-state database.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Link-scope LSDB** tab.

--End--

Variable definitions

Use the data in the following table to use the Link-scope LSDB tab.

Variable	Value
LocalIfIndex	A read-only field indicating the identifier of the link from which the LSA was received.
Type	A read-only field indicating the OSPF interface type. By default, switches can determine this value from the corresponding value of ifType. Broadcast LANs, such as Ethernet and IEEE 802.5, use the value broadcast; X.25 and similar technologies use the value nbma; and point-to-point links use the value pointToPoint.
RouterId	A read-only field indicating the 32-bit integer that uniquely identifies the router in the autonomous system.
Lsid	A read-only field indicating that the link-state ID is an LS type-specific field containing either a router ID or an IPv6 address. It identifies the piece of the routing domain described by the advertisement.
Sequence	A read-only field indicating that the sequence number is a signed 32-bit integer that identifies old and duplicate link-state advertisements.
Age	A read-only field indicating the age in seconds of the link-state advertisement.
Checksum	A read-only field indicating the checksum of the complete contents of the advertisement, except the age field. The age field is not affected so that the advertisement age value increments without updating the checksum. The checksum used is the same for ISO connectionless datagrams, the Fletcher checksum.
TypeKnown	A read-only field indicating the LSA type recognized by this router.

Viewing virtual links on neighboring devices

You can view area and virtual link configuration for the neighboring device on the Virtual Neighbor tab.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Virtual Neighbors** tab.

--End--

Variable definitions

Use the data in the following table to use the Virtual Neighbors tab.

Variable	Value
Area	A read-only field that indicates the subnetwork in which the virtual neighbor resides.
RtrId	A read-only field that indicates the 32-bit integer (represented as a type IpAddress) uniquely identifying the neighboring router in the autonomous system.
LocalIfIndex	A read-only field that indicates the interface index number of the virtual neighboring router.
AddressType	A read-only field that indicates the address type of OSPFv3 addresses including, • unknown • ipv4 • ipv6 • ipv4z • ipv6z • dns
Address	A read-only field that indicates the virtual neighboring router IPv6 address.
Options	A read-only field that indicates the bit mask corresponding to the neighbor options field.

Variable	Value
State	A read-only field that indicates the OSPF interface state, • down • attempt • init • twoWay • exchangeStart • exchange • loading • full
Events	A read-only field that indicates the number of state changes or error events that occurred between the OSPF router and the neighbor router.
LsRetransQLen	A read-only field that indicates the number of elapsed seconds between advertising retransmissions of the same packet to a neighbor.
HelloSuppressed	A read-only field that indicates whether Hello packets are suppressed on the neighbor.
NbrIfId	A read-only field that indicates the interface ID that the neighbor advertises in Hello packets on this link; the local interface index for the neighbor.
RestartHelperStatus	A read-only field that indicates whether the router is a hitless restart helper for the neighbor, • notHelping • helping
RestartHelperAge	A read-only field that indicates the remaining time in the current OSPF hitless restart interval. The range is 1 through 1800.
RestartHelperExitReason	A read-only field that indicates the outcome of the last attempt to act as a hitless restart helper for the neighbor, • none indicates no restart was attempted (default) • inProgress indicates a restart attempt is currently underway • completed indicates a completed restart

Variable	Value
	• timedout indicates a timed-out restart • topologyChanged indicates a cancelled restart due to a topology change

Viewing OSPF neighbor information

Two routers with interfaces to a common network are neighbors and appear on the Neighbors tab for each neighboring router. The OSPF Hello protocol maintains and dynamically discovers neighbor relationships. The exception is an NBMA network; you manually configure permanent neighbors on each router eligible to become the DR.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **OSPF**.
3	Click the **Neighbors** tab.

--End--

Variable definitions

Use the data in the following table to configure the Neighbors tab.

Variable	Value
IfIndex	A read-only field indicating the local link ID of the link over which the neighbor is reached.
RtrId	A read-only field indicating the router ID of the neighboring router, which in OSPF uses the same format as an IPv6 address but identifies the router independent of IPv6 address.
Address	A read-only field indicating the IPv6 address for the neighbor associated with the local link.
Options	A read-only field indicating the bit mask corresponding to the options field on the neighbor.
Priority	A read-only field indicating the preferential treatment assignment, which places the transmitted packets into queues. The priority field also indicates the possible selection of the priority field in the data link header when the switch forwards the packet.

Variable	Value
State	A read-only field indicating the OSPF interface state: • down • attempt • init • twoWay • exchangeStart • exchange • loading • full
Events	A read-only field indicating the number of state changes or error events occurring between the OSPF router and the neighbor router.
LSRetransQLen	A read-only field indicating the number of elapsed seconds between advertising retransmissions of the same packet to a neighbor.
HelloSuppressed	A read-only field indicating whether hellos are suppressed at a neighbor.
NbrIfid	A read-only field indicating the interface ID that the neighbor advertises in hello packets on this link; that is, the neighbor local interface index.
RestartHelperStatus	A read-only field indicating that the router is a hitless restart helper for the neighbor, • notHelping • helping
RestartHelperAge	A read-only field indicating the time remaining in current OSPF hitless restart interval, if the router acts as a restart helper for the neighbor. The range is 1 through 1800 seconds.
RestartHelperExitReason	A read-only field indicating the outcome of the last attempt to act as a hitless restart helper for the neighbor, • none indicates no restart was attempted (default) • inProgress indicates a restart attempt is currently underway • completed indicates a completed restart

Variable	Value
	• timedout indicates a timed-out restart • topologyChanged indicates a cancelled restart due to the topology change

Viewing TCP and UDP information

View TCP and UDP information to view the current configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **TCP/UDP**.
3	Select the required tab: • TCP Globals • TCP Connections • TCP Listeners • UDP Endpoints

--End--

Variable definitions

Use the data in the following table to use the TCP/UDP tabs.

Variable	Value
TCP Globals tab	
RtoAlgorithm	Determines the timeout value used for retransmitting unacknowledged octets.
RtoMin	Displays the minimum time (in milliseconds) permitted by a TCP implementation for the retransmission timeout.
RtoMax	Displays the maximum time (in milliseconds) permitted by a TCP implementation for the retransmission timeout.
MaxConn	Displays the maximum connections for the device.

Variable	Value
TCP Connections tab	
LocalAddressType	Displays the type (IPv6 or IPv4) for the address in the LocalAddress field.
LocalAddress	Displays the IPv6 address for the TCP connection.
LocalPort	Displays the local port number for the TCP connection.
RemAddressType	Displays the type (IPv6, IPv4) for the remote address for the TCP connection.
RemAddress	Displays the IPv6 address for the remote TCP connection.
RemPort	Displays the remote port number for the TCP connection.
State	Displays an integer that represents the state for the connection: • 1: closed • 2: listen • 3: synSent • 4: synReceived • 5: established • 6: finWait1 • 7: finWait2 • 8: closeWait • 9: lastAck(9) • 10: closing • 11: timeWait • 12: deleteTCB
Process	Displays the process ID for the system process associated with the TCP connection.
TCP Listeners tab	
LocalAddressType	Displays the type for the address (IPv6 or IPv4).
LocalAddress	Displays the local IPv6 address.
LocalPort	Displays the local port number.

Variable	Value
Process	Displays the ID for the TCP process.
UDP Endpoints tab	
LocalAddressType	Displays the local address type (IPv6 or IPv4).
LocalAddress	Displays the local IPv6 address.
LocalPort	Displays the local port number.
RemoteAddressType	Displays the remote address type (IPv6 or IPv4).
RemoteAddress	Displays the remote IPv6 address.
RemotePort	Displays the remote port number.
Instance	Distinguishes between multiple processes connected to the UDP endpoint.
Process	Displays the ID for the UDP process.

Viewing routes information

View routes information to view the current configuration.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, IPv6**.
2	Double-click **IPv6**.
3	Click the **Routes** tab.

--End--

Variable definitions

Use the data in the following table to use the Routes tab.

Variable	Value
Dest	Displays the IPv6 destination network address. The prefix value must match the PrefixLength.
PfxLength	Displays the number bits you want to advertise from the prefix. The prefix value must match the value in the Dest field. The range is 0 to 128.
IfIndex	Displays the ID for the VLAN or port.
NextHop	Displays the IPv6 address of the next hop of this route.

Variable	Value
Protocol	Displays the routing protocol (OSPF).
Metric	Displays the metric assigned to this interface. The default value of the metric is the reference bandwidth or ifSpeed. The value of the reference bandwidth is configured by the rcOspfv3ReferenceBandwidth object.

Viewing IPv6 attributes for an ACL

View IPv6 attributes for an ACL to view ACE Advanced entries associated with an ACL.

Procedure steps

Step	Action
1	In the navigation tree, open the following folders:**Configuration, Security, Data Path**.
2	Double-click **Advanced Filters (ACE/ACLs)**.
3	Click the **ACL** tab.
4	Select any of the parameters of an IPv6 ACL.
5	Click **IPv6**.

--End--

Variable definitions

Use the data in the following table to use the ACE IPv6, ACL (x) dialog box.

Variable	Value
ACL ID	Specifies the unique identifier for the ACL.
ACEID	Specifies the unique identifier for the ACE.
SrcAddrList	Lists the source IPv6 addresses.
SrcAddrOper	Specifies equal (eq) or not equal (ne) or any in relation to the listed source addresses.
DstAddrList	Lists the IPv6 destination addresses.
DstAddrOper	Specifies equal (eq) or not equal (ne) or any in relation to the listed destination addresses.
NxtHdrNxtHdr	Displays the next header value.
NxtHdrOper	Specifies equal (eq) or not equal (ne) or any in relation to the listed next header.

Common procedures using the CLI

This chapter describes common procedures that you use while configuring IPv6 routing on the Nortel Ethernet Routing Switch 8600.

Common procedures navigation

Pinging a device

When you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. When the switch receives the reply, a message indicates that the specified IP address is responding. If no reply is received, a message indicates that the address is not responding.

Procedure steps

Step	Action
1	Ping a device by using the following command: **`ping <HostName/ipv4address/ipv6address> [scopeid <value>] [datasize <value> ] [count <value> ] [-s] [-I <value> ] [-t <value> ] [-d]`**

--End--

Variable definitions

Use the data in the following table to use the **`ping`** command.

Variable	Value
count <value>	Configures the number of times to ping. For IPv4 or IPv6, the range is 1–9999. **ATTENTION** To specify a count for the ping operation, you must also specify a size. For example: **ping 8888:0:0:0:0:0:0:1 count 10**
-d	Configures ping debugging (for IPv4/IPv6).
datasize <value>	Configures the size of ping data sent in bytes, for IPv4: 16–4076, for IPv6: 16-65487.
HostName/ipv6address	Specifies the host name or IPv6 (x:x:x:x:x:x:x:x) address {string length 1–256}.
-I <value>	Configures the interval between transmissions in seconds (1–60).
-s	Configures the continuous ping at the interval rate defined by the **[-I]** parameter (for IPv4/IPv6)
scopeid <value>	Configures the circuit ID (for IPv6) (1–9999).
-t <value>	Configures the no answer timeout value (IPv4 or IPv6) {1–120}.

Common procedures using the NNCLI

This chapter describes common procedures that you use while configuring IPv6 routing on the Nortel Ethernet Routing Switch 8600.

Common procedures navigation

Pinging a device

When you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. When the switch receives the reply, a message indicates that the specified IP address is responding. If no reply is received, a message indicates that the address is not responding.

Procedure steps

Step	Action
1	Ping a device by using the following command: **ping <HostName/ipv4address/ipv6address> [scopeid <value>] [datasize <value>] [count <value>] [-s] [-I <value>] [-t <value>] [-d]**

--End--

Variable definitions

Use the data in the following table to use the **ping** command.

Variable	Value
count <value>	Configures the number of times to ping (for IPv4 or IPv6). The range is 1–9999. **ATTENTION** To specify a count for the ping operation, you must also specify a size. For example: **ping 8888:0:0:0:0:0:0:1**
-d <value>	Configures ping debugging (for IPv4 or IPv6).
datasize <value>	Configures the size of ping data sent in bytes, for IPv4:16–4076, for IPv6: 16-65487.
HostName/ipv6address	Specifies the host name or IPv6 (x:x:x:x:x:x:x:x) address {string length 1–256}.
-I <value>	Configures the interval between transmissions in seconds (1–60).
-s	Configures the continuous ping at the interval rate defined by the **[-I]** parameter (for IPv4 or IPv6).
scopeid <value>	Configures the circuit ID (for IPv6) (1–9999).
-t <value>	Configures the no answer timeout value (for IPv4 or IPv6) {1–120}.

IPv6 CLI configuration

This chapter contains enhanced configuration examples of IPv6 routing with the Nortel Ethernet Routing Switch 8600.

IPv6 CLI configuration navigation

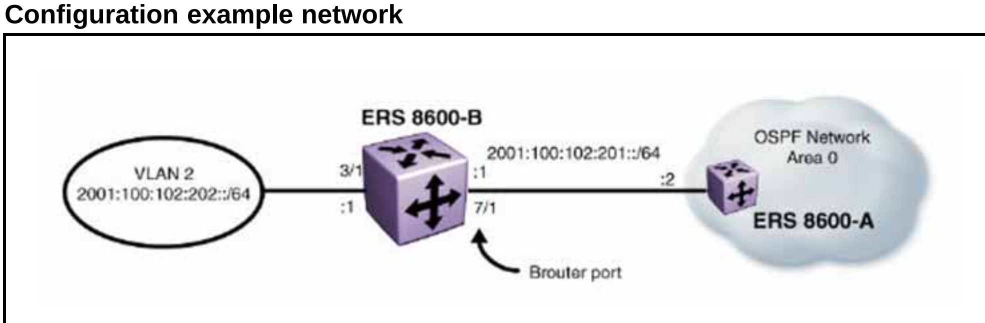
OSPF configuration

You can configure OSPFv3 on an interface (brouter port) or VLAN. This configuration example configures the following in reference to Ethernet Routing Switch 8600-B:

- Configure an IPv6 VLAN, VLAN 2, with port member 3/1.
- Configure a core IPv6 brouter port, port 7/1.
- Use IPv6 address 2001:100:102::/64.

Figure 20 "Configuration example network" (page 389) represents the network for the configuration example.

Figure 20
Configuration example network



Configuring OSPFv3

Procedure steps

Step	Action
1	Configure VLAN 2 and add port members. For IPv6, configure port-based or protocol-based VLANs. For this example, create port-based VLAN 2: `ERS8600-B:5#` **`config vlan 2 create byport 1`** `ERS8600-B:5#` **`config vlan 2 ports add 3/1`**
2	Configure and enable the IPv6 address on VLAN 2: `ERS8600-B:5#` **`config vlan 2 ipv6 create addr 2001:100:102:202::1/64`** `ERS8600-B:5#` **`config vlan 2 ipv6 admin enable`**
3	Enable OSPFv3 on VLAN 2: `ERS8600-B:5#` **`config vlan 2 ipv6 ospf create 0.0.0.0`** `ERS8600-B:5#` **`config vlan 2 ipv6 ospf admin-status enable`**
4	Configure brouter port 7/1 with IPv6: `ERS8600-B:5#` **`config ethernet 7/1 ipv6 create addr 2001:100:102:201::1/64 vlan 3999`** `ERS8600-B:5#` **`config ethernet 7/1 ipv6 admin enable`**
5	Enable OSPFv3 on brouter port 7/1: `ERS8600-B:5#` **`config Ethernet 7/1 ipv6 ospf create 0.0.0.0`** `ERS8600-B:5#` **`config ethernet 7/1 ipv6 ospf admin-status enable`**

--End--

By default, IPv6 router discovery is enabled. Any IPv6 device connected to VLAN 2 discovers the 2001:100:102:202::1 address belonging to ERS8600-B. Verify the discovery by using the following command:

```
ERS8600-B:5# config vlan 2 ipv6 nd info
```

Verifying operations from ERS 8600-A

The following commands verify that ERS 8600-A is learning routes from ERS 8600-B.

Procedure steps

Step	Action
1	Enter the following command to verify that ERS 8600-A learned routes to VLAN 2 from ERS 8600-B: `ERS8600-A:6# show ipv6 route info`

2	Verify connectivity to both IPv6 interfaces with the ping command:
	`ERS8600-A:6# ping 2001:100:102:201::1`
	`2001:0100:0102:0201:0000:0000:0000:0001 is Alive`
	`ERS8600-A:6# ping 2001:100:102:202::1`
	`2001:0100:0102:0202:0000:0000:0000:0001 is Alive`

3	Verify the OSPFv3 neighbor by using the following command: `ERS8600-A:6# show ipv6 ospf neighbor`
4	From ERS 8600-A, verify the OSPF router ID and link state information through ERS 8600-B by using the following command: `ERS8600-A:6# show ipv6 ospf lsdb detail`
5	Verify the IPv6 neighbor cache by using the following command: `ERS8600-A:6# show ipv6 neighbor info`

--End--

Verifying operations from ERS 8600-B

Verify the OSPFv3 configuration and operations from ERS 8600-B.

Procedure steps

Step	Action
1	Verify OSPF by using the following command: `ERS8600-B:5# show ipv6 ospf info`
2	Verify IPv6 addresses: `ERS8600-B:5# show ipv6 addr info`
3	Verify neighbor discovery by using the following command. In a successful configuration, the IPv6 VLAN 2 and brouter port 7/1 prefixes appear in the output.

```
ERS8600-B:5# show ipv6 nd_prefix info
```

--End--

Verifying OSPFv3 operations from a PC

In the following example, a Windows XP desktop PC connects to VLAN 2 on ERS 8600-B.

Procedure steps

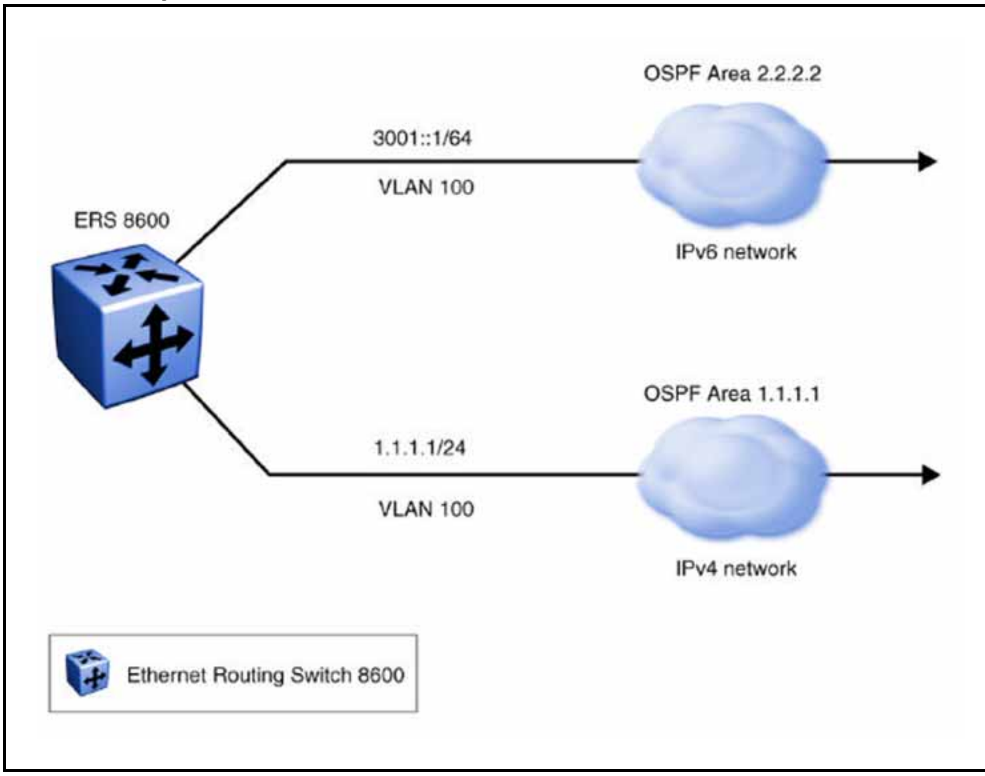
Step	Action
1	At the command prompt (select **Start, Run**, enter **cmd**, and click **OK**), enter the following commands to verify that the IPv6 addresses from ERS 8600-B appears in the output: `C:\>` **`netsh`** **`netsh>interface`** **`netsh interface>ipv6`** **`netsh interface ipv6>show neighbors`**
2	Verify that you can ping the IPv6 network address for ERS 8600-B: `C:\>` **`ping 2001:100:102:202::1`**
3	Verify that you can ping the IPv6 network address for ERS 8600-A: `C:\>` **`ping 2001:100:102:201::2`**

--End--

Routing both IPv4 and IPv6 traffic

The following figure shows the configuration of a dual-stack system or a switch that routes both IPv4 and IPv6 traffic. The following example contains steps to configure both brouter ports and VLANs.

Figure 21
Dual stack system



Use the following example to configure OSPF.

Procedure steps

Step	Action

1	Create an IPv4 interface.
	Enter the following command for a VLAN:
	`config vlan 100 ip create 1.1.1.1/24 100`
	Enter the following command for a brouter port:
	`config ethernet 2/1 ip create 1.1.1.1/24 100`

2	Configure an OSPF area for the interface.
	Enter the following command for a VLAN:
	`config vlan 100 ip ospf area 1.1.1.1`
	Enter the following command for a brouter port:
	`config ethernet 2/1 ip ospf area 1.1.1.1`

3	Enable OSPF on the interface. Enter the following command for a VLAN:

config vlan 100 ip ospf enable

Enter the following command for a brouter port:

config ethernet 2/1 ip ospf enable

4 Create an IPv6 interface on the same VLAN or brouter port where you configured IPv4.

Enter the following command for a VLAN:

config vlan 100 ipv6 create addr 3001::1/64

Enter the following command for a brouter port:

config ethernet 2/1 ipv6 create addr 3001::1/64 vlan 100

5 Enable the IPv6 interface.

Enter the following command for a VLAN:

config vlan 100 ipv6 admin-status en

Enter the following command for a brouter port:

config ethernet 2/1 ipv6 admin-status en

6 Create an OSPFv3 area by using the following command:

config ipv6 ospf area 2.2.2.2 create

7 Create an OSPFv3 interface.

Enter the following command for a VLAN:

config vlan 100 ipv6 ospf create 2.2.2.2 metric 2

Enter the following command for a brouter port:

config ethernet 2/1 ipv6 ospf create 2.2.2.2 metric 2

8 Enable OSPF on the IPv6 interface.

Enter the following command for a VLAN:

config vlan 100 ipv6 ospf admin enable

Enter the following command for a brouter port:

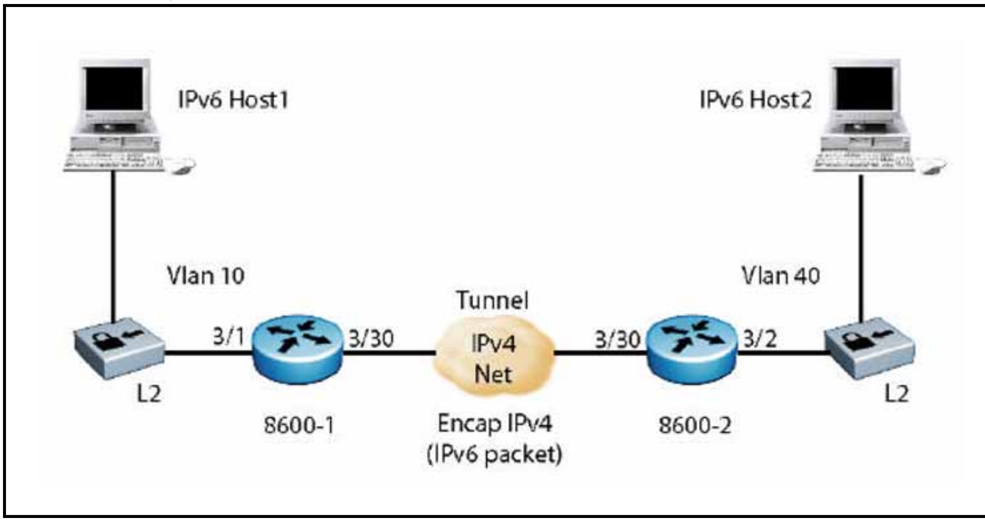
config ethernet 2/1 ipv6 ospf admin enable

--End--

Tunnel configuration between brouter ports

The following figure shows the tunnel configuration between brouter ports.

Figure 22
Tunnel configuration between brouter ports



Prerequisites

- You must configure static routes, RIP, or OSPF on both the source (8600 1) and remote (8600 2) IPv4 interfaces to communicate on an IPv4 network.
- The brouter ports on the source and destination devices use IPv4 addresses available through the IPv4 network.

This example section requires you to perform the following procedures:

1. "Creating an IPv6 VLAN with ports on the source device" (page 395)
2. "Creating an IPv4 brouter port on the source device" (page 396)
3. "Creating an IPv6 VLAN with ports on the remote device" (page 396)
4. "Creating an IPv4 brouter port on the destination device" (page 397)
5. "Configuring a tunnel on the source device" (page 397)
6. "Configuring a tunnel on the destination device" (page 397)

Creating an IPv6 VLAN with ports on the source device

Configure the IPv6 VLAN with ports (VLAN 10 in the figure) on the source device, or 8600.

Procedure steps

Step	Action
1	Create a VLAN by using the following command:

```
config vlan 10 create byport 1
```

2 Add ports to the VLAN by using the following command:

```
config vlan 10 ports add 3/1
```

3 Assign an IPv6 address to the to the VLAN by using the following command:

```
config vlan 10 ipv6 create addr 4000::1/120
```

4 Enable the new VLAN by using the following command:

```
config vlan 10 ipv6 admin enable
```

--End--

Creating an IPv4 brouter port on the source device

Procedure steps

Step	Action
1	Create a brouter port with an IPv4 address by using the following command: `config ethernet 3/30 ip create 172.21.80.1/24 1000`
2	Enable OSPF on the port by using the following command: `config ethernet 3/30 ip ospf enable`
3	Enable OSPF on the device by using the following command: `config ip ospf enable`

--End--

Creating an IPv6 VLAN with ports on the remote device

Configure the IPv6 VLAN with ports (VLAN 40 in the figure) on the destination device, or 8600.

Procedure steps

Step	Action
1	Create a VLAN by using the following command: `config vlan 40 create byport 1`
2	Add ports to the VLAN by using the following command: `config vlan 40 ports add 3/2`
3	Assign an IPv6 address to the to the VLAN by using the following command:

```
config vlan 40 ipv6 create addr 4000::2/120
```

4 Enable the new VLAN by using the following command:

```
config vlan 40 ipv6 admin enable
```

--End--

Creating an IPv4 brouter port on the destination device

Create an IPv4 brouter port on the destination device.

Procedure steps

Step	Action
1	Create a brouter port with an IPv4 address by using the following command: `config ethernet 3/30 ip create 192.168.20.1/24 2000`
2	Enable OSPF on the port by using the following command: `config ethernet 3/30 ip ospf enable`
3	Enable OSPF on the device by using the following command: `config ip ospf enable`

--End--

Configuring a tunnel on the source device

Configure a tunnel on the source device.

Procedure steps

Step	Action
1	Enter the following command to configure a tunnel on the source device. Enter the IPv4 address for the destination port for the remote-address value. `config ipv6 tunnel 1 create local-addr 172.21.80.1 ipv6addr 2500::1/120 remote-address 192.168.20.1`

--End--

Configuring a tunnel on the destination device

Configure a tunnel on the destination device.

Procedure steps

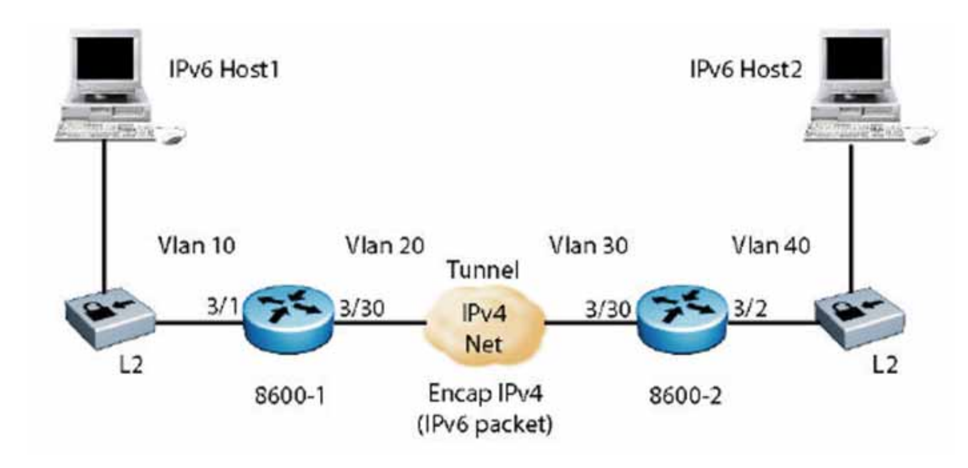
Step	Action
1	Enter the following command to configure a tunnel on the destination device. Enter the IPv4 address for the source port for the remote-address value. `config ipv6 tunnel 1 create local-addr 192.168.20.1 ipv6addr 2500::2/120 remote-address 172.21.80.1`

--End--

Tunnel configuration between VLANs

The following figure shows the configuration of a tunnel between VLANs.

Figure 23
Tunnel configuration between VLANs



Prerequisites

- You must configure static routes, RIP, or OSPF on both the source (8600 1) and remote (8600 2) IPv4 interfaces to communicate on an IPv4 network.
- Configure IPv4 address on the VLANs. Test the source and destination addresses by using the ping command.

This example requires you to perform the following procedures:

1. "Configuring an IPv6 VLAN on the source device" (page 399)
2. "Configuring an IPv4 VLAN on the source device" (page 399)
3. "Configuring an IPv6 VLAN on the destination device" (page 400)

4. “Configuring an IPv4 VLAN on the destination device” (page 400)
5. “Configuring the tunnel on the source device” (page 401)
6. “Configuring the tunnel on the destination device” (page 401)

Configuring an IPv6 VLAN on the source device

Configure the IPv6 VLAN (VLAN 10 in the figure) on the source device, or 8600 1 in the figure.

Procedure steps

Step	Action
1	Create a VLAN by using the following command: **`config vlan 10 create byport 1`**
2	Add ports to the VLAN by using the following command: **`config vlan 10 ports add 3/1`**
3	Assign an IPv6 address to the to the VLAN by using the following command: **`config vlan 10 ipv6 create addr 4000::1/120`**
4	Enable the new VLAN by using the following command: **`config vlan 10 ipv6 admin enable`**

--End--

Configuring an IPv4 VLAN on the source device

Configure an IPv4 VLAN (VLAN 20 in the figure) on the source device (8600 1 in the figure). The IPv4 VLAN encapsulates the IPv6 VLAN across the IPv4 network.

Procedure steps

Step	Action
1	Create the VLAN by using the following command: **`config vlan 20 create byport 1`**
2	Add ports to the VLAN by using the following command: **`config vlan 20 ports add 3/30`**
3	Assign an IPv4 address to the VLAN by using the following command: **`config vlan 20 ip create 172.21.80.1/24`**

4 Enable OSPF on the VLAN by using the following command:

```
config vlan 20 ip ospf enable
```

5 Enable OSPF on the device by using the following command:

```
config ip ospf enable
```

--End--

Configuring an IPv6 VLAN on the destination device

Configure the IPv6 VLAN (VLAN 40 in the figure) on the destination device, or 8600 2 in the figure.

Procedure steps

Step	Action
1	Create a VLAN by using the following command: `config vlan 40 create byport 1`
2	Add ports to the VLAN by using the following command: `config vlan 40 ports add 3/2`
3	Assign an IPv6 address to the to the VLAN by using the following command: `config vlan 40 ipv6 create addr 4000::2/120`
4	Enable the new VLAN by using the following command: `config vlan 40 ipv6 admin enable`

--End--

Configuring an IPv4 VLAN on the destination device

Configure an IPv4 VLAN (VLAN 30 in the figure) on the destination device (8600 2 in the figure). The IPv4 VLAN encapsulates the IPv6 VLAN across the IPv4 network.

Procedure steps

Step	Action
1	Create the VLAN by using the following command: `config vlan 30 create byport 1`
2	Add ports to the VLAN by using the following command: `config vlan 30 ports add 3/30`

3 Assign an IPv4 address to the VLAN by using the following command:

config vlan 30 ip create 192.168.20.1/24

4 Enable OSPF on the VLAN by using the following command:

config vlan 30 ip ospf enable

5 Enable OSPF on the device by using the following command:

config ip ospf enable

--End--

Configuring the tunnel on the source device

Procedure steps

Step	Action
1	Enter the following command to configure the tunnel on the source device. Enter the IPv4 address for the destination device (8600 2) for the remote-address value. **config ipv6 tunnel 1 create local-addr 172.21.80.1 ipv6addr 2500::1/120 remote-address 192.168.20.1**

--End--

Configuring the tunnel on the destination device

Procedure steps

Step	Action
1	Enter the following command to configure the tunnel on the destination device. Enter the IPv4 address for the source device (8600 1) for the remote-address value. **config ipv6 tunnel 1 create local-addr 192.168.20.1 ipv6addr 2500::2/120 remote-address 172.21.80.1**

--End--

CLI show commands

This chapter describes show commands to view the operational status of IPv6 routing on the Nortel Ethernet Routing Switch 8600.

CLI show command navigation

- "OSPFv3 information for VLANs" (page 419)
- "Tunnel information" (page 420)
- "Tunnel interface information" (page 421)

ACL or ACE information

Use the **`show filter acl ace`** command to display information about ACLs or ACEs. The syntax for this command is as follows.

`show filter acl ace [ <acl-id> ] [ <ace-id> ]`

The following table explains parameters for this command.

Table 31
Command parameters

Parameter	Description
`ace-id`	Specifies a unique identifier (in the range 1–1000) for this ACE entry.
`acl-id`	Specifies a unique identifier (in the range 1–4096) for this ACL entry.

If you enter the **`<acl-id>`**, ACE information appears for all ACEs associated with the ACL. If you enter the **`<ace-id>`**, ACE information for the requested ACE appears. If you provide no **`<acl-id>`**, the command shows switch-wide ACL configuration data as viewed in the following figure.

Figure 24
show filter acl ace partial command output

```
================================================================================
                          Ace Action Table (Part I)
================================================================================
Acl  Ace  AceName                  Admin   Oper    Mode    Mlt Remark  Remark
Id   Id                            State   State            Id DSCP    Dot1p
--------------------------------------------------------------------------------
10   1    DHCP                     Enable  Up      permit 0   disable disable
10   2    DNS                      Enable  Up      permit 0   disable disable
10   3    ICMP                     Enable  Up      permit 0   disable disable
10   4    VOIP                     Enable  Up      permit 0   disable disable
10   5    SNAS HTTP/HTTPS          Enable  Up      permit 0   disable disable
10   6    ARP                      Enable  Up      permit 0   disable disable
4082 1    CSE 1000 - UDP SRC       Enable  Up      permit 0   disable disable
4082 2    BCM - UDP SRC            Enable  Up      permit 0   disable disable
4082 3    BCM - UDP DST            Enable  Up      permit 0   disable disable
4082 4    BCM - TCP SRC            Enable  Up      permit 0   disable disable
4082 5    BCM - TCP DST            Enable  Up      permit 0   disable disable
4082 6    Meridian-Trunk 2.0 UDP SRCEnable  Up      permit 0   disable disable
4082 7    Meridian-Trunk 2.0 UDP DSTEnable  Up      permit 0   disable disable
4082 8    Meridian-Trunk 2.0 TCP DSTEnable  Up      permit 0   disable disable
4082 9    MSL 100IP - UDP SRC      Enable  Up      permit 0   disable disable
4082 10   MSL 100IP - UDP DST      Enable  Up      permit 0   disable disable

4082 11   MSL 100IP - TCP SRC      Enable  Up      permit 0   disable disable
4082 12   MSL 100IP - TCP DST      Enable  Up      permit 0   disable disable
4082 13   VCON - UDP SRC           Enable  Up      permit 0   disable disable
4082 14   VCON - UDP DST           Enable  Up      permit 0   disable disable
4082 15   MINERVA - UDP SRC        Enable  Up      permit 0   disable disable
4082 16   MINERVA - UDP DST        Enable  Up      permit 0   disable disable

================================================================================
                          Ace Action Table (Part II)
================================================================================
Acl  Ace  Redirect Next-Hop                        Unreach Police Egress  Egress
Id   Id                                            -able           Q      Q-1g
--------------------------------------------------------------------------------
10   1    0.0.0.0                                  deny    0       64     64
10   2    0.0.0.0                                  deny    0       64     64
10   3    0.0.0.0                                  deny    0       64     64
10   4    0.0.0.0                                  deny    0       64     64
10   5    0.0.0.0                                  deny    0       64     64
10   6    0.0.0.0                                  deny    0       64     64
4082 1    0.0.0.0                                  deny    0       64     64
4082 2    0.0.0.0                                  deny    0       64     64
4082 3    0.0.0.0                                  deny    0       64     64
4082 4    0.0.0.0                                  deny    0       64     64

--More-- (q = quit)
```

ACT data

Use the **`show filter act`** command to display ACT data. The syntax for this command is as follows.

`show filter act [ <act-id> ]`

The following table explains parameters for this command.

Table 32
Command parameters

Parameter	Description
`act-id`	Specifies a unique identifier (in the range 1–4096) for this ACT entry.

If you provide no **`<act-id>`**, the command shows switch-wide ACT configuration data.

> **ATTENTION**
> Any show command that displays information that cannot fit on oe screen appears as two tables: Part 1 and Part 2.

ACT pattern data

Use the **`show filter act-pattern`** command to display ACT pattern data. The syntax for this command is as follows.

`show filter act-pattern [ <act-id> ]`

The following table explains parameters for this command.

Table 33
Command parameters

Parameter	Description
`act-id`	Specifies a unique identifier (in the range 1–4096) for this ACT entry.

The following figure shows sample output for this command.

Figure 25
show filter act-pattern command output

```
================================================================================
                               ACT Pattern Table
================================================================================
Id   Pattern Pattern                         Pattern            Pattern Pattern
     Number  Name                            Base               Offset  Length
--------------------------------------------------------------------------------
1    1       samplepattern                   ip-options-begin   76000   56
```

Basic OSPF information about a port

Use the **`show ports stats ospf main port`** command to display basic OSPF information about the specified port or for all ports. The syntax for this command is as follows.

`show ports stats ospf main port <value>`

The following table explains parameters for this command.

Table 34
Command parameters

Parameter	Description
`port <value>`	Specifies the port or range of ports configured in the format slot/port.

Figure 26 "show ports stats ospf main command output" (page 407) shows sample output for this command.

Figure 26
show ports stats ospf main command output

```
================================================================================
                                Port Stats Ospf
================================================================================
PORT_NUM RX_HELLO   TX_HELLO   RXDB_DESCR TXDB_DESCR RXLS_UPDATE   TXLS_UPDATE
--------------------------------------------------------------------------------
4/2      0          0          0          0          0             0
4/3      0          0          0          0          0             0
```

Extended OSPF information

Use the **`show ports stats interface extended`** command to display extended OSPF information about the specified port or for all ports. The syntax for this command is as follows.

`show ports stats interface extended [port <value> ]`

The following table explains the parameters for this command.

Table 35
Command parameters

Parameter	Description
`port <value>`	Specifies the port or range of ports to configure in the format slot/port.

Figure 27 "show ports stats interface extended command output" (page 408) shows sample output for this command.

Figure 27
show ports stats interface extended command output

```
================================================================================
                        Port Stats Interface Extended
================================================================================
PORT_NUM IN_UNICST  OUT_UNICST IN_MULTICST  OUT_MULTICST IN_BRDCST  OUT_BRDCST
--------------------------------------------------------------------------------
2/1      0          0          0            0            0          0
2/2      0          0          0            0            0          0
2/3      0          0          0            0            0          0
2/4      0          0          0            0            0          0
2/5      0          0          0            0            0          0
2/6      0          0          0            0            0          0
2/7      0          0          0            0            0          0
2/8      0          0          0            0            0          0
2/9      0          0          0            0            0          0
2/10     0          0          0            0            0          0
2/11     0          0          0            0            0          0
2/12     0          0          0            0            0          0
2/13     0          0          0            0            0          0
2/14     0          0          0            0            0          0
2/15     0          0          0            0            0          0
2/16     0          0          0            0            0          0
2/17     0          0          0            0            0          0

2/18     0          0          0            0            0          0
2/19     0          0          0            0            0          0
2/20     0          0          0            0            0          0
2/21     0          0          0            0            0          0
2/22     0          0          0            0            0          0
2/23     0          0          0            0            0          0
2/24     0          0          0            0            0          0
2/25     0          0          0            0            0          0
2/26     0          0          0            0            0          0
2/27     0          0          0            0            0          0
2/28     0          0          0            0            0          0
2/29     0          0          0            0            0          0
2/30     0          0          0            0            0          0
```

Interface (VLAN or brouter port) configuration output

Use the **`show ipv6 interface info`** command to view the output of all configured interfaces. The syntax for this command is as follows.

`show ipv6 interface info`

View the output of a specific configured interface by using the following command:

`show ipv6 interface info <interface ID>`

The following figure shows sample output for this command.

Figure 28
show ipv6 interface info command output

```
================================================================================
                          Interface Information
================================================================================
IFINDX VLAN-ID/ MTU     PHYSICAL            ADMIN   OPER    RCHBLE  RETRAN  TYPE
       BROUTER          ADDRESS             STATE   STATE   TIME    TIME

--------------------------------------------------------------------------------
448    7/1      1500    0:e0:7b:bc:22:0     enable  up      0       1000    ETHER
2050   2        1500    0:e0:7b:bc:22:1     enable  up      0       1000    ETHER
--------------------------------------------------------------------------------

================================================================================
                          Address Information
================================================================================
INTF   IPV6                                       TYPE    ORIGIN    STATUS
INDEX  ADDRESS
--------------------------------------------------------------------------------
448    2001:100:102:201:0:0:0:1                   UNICAST MANUAL    PREFERRED
448    fe80:0:0:0:2e0:7bff:febc:2200              UNICAST OTHER     UNKNOWN
2050   2001:100:102:202:0:0:0:1                   UNICAST MANUAL    PREFERRED
2050   fe80:0:0:0:2e0:7bff:febc:2201              UNICAST OTHER     UNKNOWN

2 out of 2 Total Num of Interface Entries displayed.
4 out of 4 Total Num of Address Entries displayed.
```

IPv6 static route information

Use the **show ipv6 static-route info** command to display the existing IPv6 static routes for the switch or for a specific net or subnet. The syntax for this command is as follows.

show ipv6 static-route info

Figure 29 "show ipv6 static-route info command output" (page 409) shows sample output for this command.

Figure 29
show ipv6 static-route info command output

```
ERS-8606:5/show/ipv6/static-route# info

==============================================================================
                        Static Route Information
==============================================================================
DEST-IP                                   NET IFINDX(VID/BRT/TUN) ENABLE  STATUS
PREFERENCE
------------------------------------------------------------------------------
220:0:0:0:0:0:0:1                           64   128    (0      ) enable  inactive
0:0:0:0:0:0:0:0                             enable               5
------------------------------------------------------------------------------
```

MLD cache

Use the **show ipv6 mld mld-cache** command to display the MLD cache for a brouter port, VLAN, or group address. The syntax for this command is as follows.

Enter the following command to view the MLD cache for a brouter port:

show ipv6 mld mld-cache port <slot/port> detail

Enter the following command to view the MLD cache for a VLAN:

show ipv6 mld mld-cache vlan <vlan id> detail

Enter the following command to view the MLD cache for a group address:

show ipv6 mld mld-cache grp-address <address> detail

MLD configuration for a brouter port

Use the **show ports info mld** command to display configuration details for MLD on a brouter port. The syntax for this command is as follows.

show ports info mld

The following figure shows sample output for this command.

Figure 30
show ports info mld command output

```
================================================================================
                         Port Ipv6 MLD
================================================================================
BROUTER Q-INT  VR QUERIER                                Q-M-R  ROBUST L-M-Q
--------------------------------------------------------------------------------
3/1     125    1  0:0:0:0:0:0:0:0                        10     2      1
 Legend: Q-INT: query-interval VR: version
         Q-M-R: query-max-resp ROBUST: robustval
         L-M-Q: last-memb-query-int
1 out of 3 Total Num of Ipv6 MLD Entries displayed.
```

MLD configuration for a VLAN

Use the **show vlan info mld** command to display configuration details for MLD on a VLAN. The syntax for this command is as follows.

show vlan info mld

Figure 31 "Output for the show vlan info mld command" (page 411) shows sample output for this command.

Figure 31
Output for the show vlan info mld command

```
================================================================================
                         Vlan Ipv6 MLD
================================================================================
VLANID  Q-INT  VR QUERIER                             Q-M-R  ROBUST L-M-Q
--------------------------------------------------------------------------------
VID15   125    1  fe80:0:0:0:209:97ff:fef6:7a08        10     2      1
 Legend: Q-INT: query-interval VR: version
         Q-M-R: query-max-resp ROBUST: robustval
         L-M-Q: last-memb-query-int
1 out of 2 Total Num of Ipv6 MLD Entries displayed.
```

Neighbor cache

Use the **show ipv6 neighbor info** command to view entries in the neighbor cache. The syntax for this command is as follows.

show ipv6 neighbor info

Figure 32 "show ipv6 neighbors info" (page 411) shows sample output for the **show ipv6 neighbors info** command.

Figure 32
show ipv6 neighbors info

```
================================================================================
                            Neighbor Information
================================================================================
NET ADDRESS/                                     PHYS  TYPE    STATE      LAST
PHYSICAL ADDRESS                                 INTF                     UPD
--------------------------------------------------------------------------------
4040:0:0:0:0:0:0:1/                              4/18  STATIC  REACHABLE  85907
00:80:2d:c0:92:03
8888:0:0:0:0:0:0:1/                              4/29  STATIC  REACHABLE  84754
00:80:2d:c0:92:03
999:0:0:0:0:0:0:1/                               4/17  STATIC  REACHABLE  84316
00:80:2d:c0:92:03
--------------------------------------------------------------------------------
```

Neighbor discovery prefixes

Use the **show ipv6 nd-prefix info** command to view all configured neighbor discovery prefixes. The syntax for this command is as follows.

show ipv6 nd-prefix info

The following figure shows sample output for the **show ipv6 nd-prefix info** command.

Figure 33
show ipv6 nd-prefix info command output

```
================================================================================
                         Nd-Prefix Address Information
================================================================================
INTF  IPV6                                                VLAN  VALID    PREF     EUI
INDEX ADDRESS/PREFIX                                      ID    LIFE     LIFE
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Legend: EUI: eui-not-used(1), eui-used-with-ul-complement(2)
             eui-used-without-ul-complement(3)
```

OSPF areas

Use the **show ipv6 ospf area** command to display information about OSPF area parameters. The syntax for this command is as follows.

show ipv6 ospf area

Figure 34 "show ipv6 ospf area command output" (page 412) shows sample output for this command.

Figure 34
show ipv6 ospf area command output

```
================================================================================
                          OSPF Area
================================================================================
AREA_ID         STUB_AREA  NSSA  IMPORT_SUM TRANS_ROLE
--------------------------------------------------------------------------------
0.0.0.0         false      false true       always
1.1.1.1         false      false true       always
STUB_METRIC SPF_RUNS BDR_RTR_CNT ASBDR_RTR_CNT LSA_CNT LSACK_SUM
--------------------------------------------------------------------------------
10          0        0           0             0       0
10          0        0           0             0       0
```

OSPF configuration settings for a port

Use the **show ports info ospf** command to display information about the OSPF parameters of the specified port or all ports. The syntax for this command is as follows.

show ports info ospf [<ports>]

The following table explains the parameters for this command.

Table 36
Command parameters

Parameter	Description
ports	Specifies the port or range of ports to configure in the format slot/port.

Figure 35 "show ports info ospf command (partial output)" (page 413) shows sample output for this command.

Figure 35
show ports info ospf command (partial output)

```
================================================================================
                                  Port Ospf
================================================================================
PORT         HELLO   RTRDEAD OSPF
NUM    ENABLE INTVAL  INTVAL  PRIORITY METRIC AUTHTYPE AUTHKEY    AREA_ID
--------------------------------------------------------------------------------
2/1    false  10      40      1        0      none                0.0.0.0
2/2    false  10      40      1        0      none                0.0.0.0
2/3    false  10      40      1        0      none                0.0.0.0
2/4    false  10      40      1        0      none                0.0.0.0
2/5    false  10      40      1        0      none                0.0.0.0
2/6    false  10      40      1        0      none                0.0.0.0
2/7    false  10      40      1        0      none                0.0.0.0
2/8    false  10      40      1        0      none                0.0.0.0
2/9    false  10      40      1        0      none                0.0.0.0
2/10   false  10      40      1        0      none                0.0.0.0
2/11   false  10      40      1        0      none                0.0.0.0
2/12   false  10      40      1        0      none                0.0.0.0
2/13   false  10      40      1        0      none                0.0.0.0
2/14   false  10      40      1        0      none                0.0.0.0
2/15   false  10      40      1        0      none                0.0.0.0
2/16   false  10      40      1        0      none                0.0.0.0
```

OSPF information

Use the **`show ipv6 ospf info`** command to display the current OSPF settings for the switch. The syntax for this command is as follows.

`show ipv6 ospf info`

Figure 36 "show ipv6 ospf info command output" (page 414) shows sample output for this command.

Figure 36
show ipv6 ospf info command output

```
================================================================
                        OSPFv3 Global Information
================================================================
        router-id                       : 1.1.1.1
        admin-state                     : ENABLED
        version                         : 3
        area-bdr-rtr-state              : FALSE
        as-bdr-rtr-state                : FALSE
        as-scope-lsa-count              : 0
        lsa-checksum                    : 0
        originate-new-lsas              : 0
        rx-new-lsas                     : 0
        ext-lsa-count                   : 0
        ext-area-lsdb-limit             : -1
        multicast-ext                   : intraAreaMulticast
        exit-voer-flow-interval         : 4294967295
        demand-extensions               : FALSE
        traffic-engineering-support     : FALSE
        reference-bandwidth             : 1000000
        restart-support                 : none
        restart-interval                : 1800
        restart-status                  : notRestarting
        restart-age                     : 1800
        restart-exit-reason             : none
```

OSPF interface information

Use the **show ipv6 ospf interface** command to display information about the OSPF interface.

show ipv6 ospf interface

Figure 37 "show ipv6 ospf interface command output" (page 415) shows sample output for this command.

Figure 37
show ipv6 ospf interface command output

```
================================================================================
                          OSPF Interface
================================================================================
IFINDX(VID/BRT) AREAID          ADM IFSTATE  METRIC PRI DR/BDR          IFTYPE
--------------------------------------------------------------------------------
220    (3/29    ) 0.0.0.0         ena DR        1       1   2.0.0.1          BROADCAST
                                                              0.0.0.0
2050   (12      ) 3.0.0.0         ena BDR       1       1   3.0.0.1          BROADCAST
                                                              2.0.0.1
2051   (100     ) 0.0.0.0         ena BDR       1       1   1.0.0.1          BROADCAST
                                                              2.0.0.1

================================================================================
                          OSPF Virtual Interface
================================================================================
AREAID           NBRIPADDR        STATE
--------------------------------------------------------------------------------
3.0.0.0          3.0.0.1          PT-PT
```

OSPF interface timer settings

Use the **`show ipv6 ospf int-timers`** command to display OSPF interface timer settings. The syntax for this command is as follows:

`show ipv6 ospf int-timers`

Figure 38 "show ipv6 ospf int-timers command output" (page 415) shows sample output for this command.

Figure 38
show ipv6 ospf int-timers command output

```
================================================================================
                          OSPF Interface Timers
================================================================================
                                TRANSIT  RETRANS  HELLO    DEAD     POLL
IFINDX(VID/BRT) AREAID          DELAY    INTERVAL INTERVAL INTERVAL INTERVAL
--------------------------------------------------------------------------------
220    (3/29    ) 0.0.0.0       1        5        10       40       120
2050   (12      ) 3.0.0.0       1        5        10       40       120
2051   (100     ) 0.0.0.0       1        5        10       40       120

================================================================================
                          OSPF Virtual Interface Timers
================================================================================
                                TRANSIT  RETRANS  HELLO    DEAD
AREAID          NBRIPADDR       DELAY    INTERVAL INTERVAL INTERVAL
--------------------------------------------------------------------------------
3.0.0.0         3.0.0.1         1        5        10       60
```

OSPF link-state database table

Use the **`show ipv6 ospf lsdb`** command to display the OSPF link-state database (LSDB) table. The syntax for this command is as follows.

show ipv6 ospf lsdb [scope <value>] [port <value>] [vlan <value>] [tunnel <value>] [area <value>] [lsatype <value>] [lsid <value>] [adv_rtr <value>] [detail]

You can specify a scope, VLAN, tunnel, area string, link-state advertisement type (0 to 5), link state ID, or advertising router. If you add the **detail** option to the command, the output contains more information.

Figure 39 "show ipv6 ospf lsdb command output" (page 416) shows sample output with no variables for this command.

Figure 39
show ipv6 ospf lsdb command output

```
=============================================================================

Link Scope LSAs

=============================================================================
IVID/BRT/TUN TYPE       Router ID           LS ID  AGE CKSUM Sequence
-----------------------------------------------------------------------------
2           8         0.0.0.11            0.0.0.2  838  9b38  80000001
3           8         0.0.0.11            0.0.0.3  838  e5e9  80000001
=============================================================================

Area Scope LSAs

=============================================================================
AREA ID TYPE       Router ID           LS ID  AGE CKSUM Sequence
0.0.0.0 2001     0.0.0.11           0.0.0.0 793 e53e   80000004
0.0.0.0 2009     0.0.0.11           0.0.0.0 793 e416   80000004
================================================================================

AS Scope LSAs

================================================================================
TYPE       Router ID           LS ID  AGE CKSUM    Sequence

--------------------------------------------------------------------------------
```

Figure 40 "show ipv6 ospf lsdb detail command output" (page 417) shows partial output of this command with the **detail** option.

Figure 40
show ipv6 ospf lsdb detail command output

```
==============================================================================
                         Link Scope LSAs
==============================================================================
_________________________
         TYPE: link
 Interface ID: 220
         Port: 3/29
Advertised by: 2.0.0.1
Link State ID: 0.0.0.220
   Seq Number: 80000002
          AGE: 528
     Checksum: e666
   LSA Length: 60
     Priority: 0, Options: -|R|-|-|E|V6
Local Address: fe80:0000:0000:0000:020f:cdff:fe96:1200
   # Prefixes: 1
    Prefix 9000::/96    (Prefix Options -|-|-|-
==============================================================================
                         Area Scope LSAs
==============================================================================
_________________________
         TYPE: router
     Area  ID: 0.0.0.0
Advertised by: 1.0.0.1
Link State ID: 0.0.0.0
   Seq Number: 80000007
          AGE: 302
     Checksum: c835
   LSA Length: 40
         FLAGS: --|-|-|-|B Options: -|R|-|-|E|V6
         Neighbor 1.0.0.1 of type (Transit) on intf 2051
         Neighbor interface id: 2051
                        Metric: 1
```

OSPF neighbors

Use the **show ipv6 ospf neighbor** command to display OSPF neighbors configuration information. The syntax for this command is as follows.

show ipv6 ospf neighbor

Figure 41 "show isv6 ospf neighbor command output" (page 418) shows sample command output for this command.

Figure 41
show isv6 ospf neighbor command output

```
================================================================================
                                  OSPF Neighbor
================================================================================
INTERFACE NBRROUTERID      NBRIPADDR                                  PRIO_STATE
--------------------------------------------------------------------------------
2050      3.0.0.1          fe80:0:0:0:211:f9ff:fed0:202               Full
2051      1.0.0.1          fe80:0:0:0:280:2dff:fe32:5604              Full

================================================================================
                              OSPF Virtual Neighbor
================================================================================
NBRAREAID       NBRROUTERID      VIRTINTFID NBRIPV6ADDR
   STATE
--------------------------------------------------------------------------------
0.0.0.0         3.0.0.1          6050       3000:0:0:0:0:0:0:1
Full
================================================================================
                                OSPF NBMA Neighbor
================================================================================
INTERFACE NBRROUTERID      NBRIPADDR                                  STATE
--------------------------------------------------------------------------------
```

OSPF parameters configured for VLANs

Use the **show vlan info ospf** command to display OSPF parameters configured for all VLANs or a specified VLAN. The syntax for this command is as follows.

show vlan info ospf [<vid>] [port <value>]

The following table explains the parameters for this command.

Table 37
Command parameters

Parameter	Description
port <value>	Specifies the port or range of ports configured in the format slot/port.
vid	Specifies a unique integer value in the range 1–4094 that identifies the VLAN to configure.

Figure 42 "show vlan info ospf command output" (page 419) shows sample output for this command.

Figure 42
show vlan info ospf command output

```
================================================================================
                                   Vlan Ospf
================================================================================
VLAN        HELLO    RTRDEAD  DESIGRTR
ID   ENABLE INTERVAL INTERVAL PRIORITY METRIC AUTHTYPE AUTHKEY    INTF   AREAID
--------------------------------------------------------------------------------
1     false  10       40       1        10     none               b    0.0.0.0
2     true   10       40       1        10     none               n    0.0.0.0
3     true   10       40       1        10     none               b    0.0.0.0
4     false  10       40       1        10     none               b    0.0.0.0
5     false  10       40       1        0      none               b    0.0.0.0
6     false  10       40       1        0      none               b    0.0.0.0
10    true   10       40       12       10     msg_dsgt           n    0.0.0.0
12    false  10       40       1        0      none               b    0.0.0.0
50    false  10       40       1        10     none               b    0.0.0.0
120   false  10       40       1        0      none               b    0.0.0.0

TYPE Legend:
n=nbma interface, p=passive interface, b=broadcast interface
```

OSPFv3 information for brouter ports

Use the **show ports info ospfv3** command to view OSPFv3 information for brouter ports. The syntax for this command is as follows.

show ports info ospfv3

Figure 44 "Output for show vlan info ospfv3" (page 420) shows sample output for this command.

Figure 43
Output for show ports info ospfv3

```
================================================================================
                          Port Ospfv3 Interface
================================================================================
IFINDX(BTR)     AREAID          ADM IFSTATE  METRIC  PRI DR/BDR          IFTYPE
--------------------------------------------------------------------------------
192    (3/1    ) 2.2.2.2         dis DOWN     1       1   0.0.0.0         BROADCAST
                                                          0.0.0.0
1 out of 7 Total Num of Ospf Interface Entries displayed.
```

OSPFv3 information for VLANs

Use the **show vlan info ospfv3** command to view OSPFv3 information for VLANs. The syntax for this command is as follows.

show vlan info ospfv3

Figure 44 "Output for show vlan info ospfv3" (page 420) shows sample output for this command.

Figure 44
Output for show vlan info ospfv3

```
==============================================================================
                         Vlan Ospf
==============================================================================
VLAN        HELLO    RTRDEAD  DESIGRTR
ID  ENABLE INTERVAL INTERVAL PRIORITY METRIC AUTHTYPE AUTHKEY    INTF   AREAID
------------------------------------------------------------------------------
1   false   10        40        1        0       none                b    0.0.0.0

TYPE Legend:
n=nbma interface, p=passive interface, b=broadcast interface
```

Tunnel information

Use the **show ipv6 tunnel info** command to show general tunnel information. The syntax for this command is as follows.

show ipv6 tunnel info [<tunnel-id>]

The following table explains the parameters for this command.

Table 38
Command parameters

Parameter	Description
tunnel-id	Specifies the ID number of the tunnel in the range 1-2147477248.

Figure 45 "show ipv6 tunnel info output" (page 420) shows sample output for the **show ipv6 tunnel info** command.

Figure 45
show ipv6 tunnel info output

```
===============================================================
Tunnel If Information
===============================================================
TUNNEL-ID local-addrESS   REMOTE ADDRESS  TYPE  TTL

---------------------------------------------------------------
8         192.168.6.3     172.21.10.1     manual 255
```

Tunnel interface information

Use the **show ipv6 tunnel interface** command to show IPv6 tunnel interface information. The syntax for this command is as follows.

show ipv6 tunnel interface [<tunnel-id>]

The following table explains the parameters for this command.

Table 39
Command parameters

Parameter	Description
tunnel-id	Specifies the ID number of the tunnel in the range 1-2147477248 .

Figure 46 "show ipv6 tunnel interface" (page 421) shows sample output for the **show ipv6 tunnel interface** command.

Figure 46
show ipv6 tunnel interface

```
================================================================
                 Tunnel Interface Information
================================================================
IFINDX TUNNEL-ID LOCAL ADDRESS   REMOTE ADDRESS  OPER STATUS
TYPE
----------------------------------------------------------------
4359   8         192.168.6.3     172.21.10.1     active manual
----------------------------------------------------------------
================================================================
                        Address Information
================================================================
INTF   IPV6                                      TYPE    ORIGIN
STATUS
INDEX  ADDRESS
----------------------------------------------------------------
4359   4000:0:0:0:0:0:0:8                        UNICAST MANUAL
PREFERRED
4359   fe80:0:0:0:0:0:c0a8:603                   UNICAST OTHER
UNKNOWN
```

NNCLI show commands

This chapter describes privExec mode show commands to view the operational status of IPv6 routing on the Nortel Ethernet Routing Switch 8600.

NNCLI show command navigation

ACL or ACE information

Use the **show filter acl ace** command to display information about ACLs or ACEs. The syntax for this command is as follows.

show filter acl ace [<acl-id>] [<ace-id>]

The following table explains parameters for this command.

Table 40
Command parameters

Parameter	Description
ace-id	Specifies a unique identifier (in the range 1–1000) for this ACE entry.
acl-id	Specifies a unique identifier (in the range 1–4096) for this ACL entry.

If you enter the **<acl-id>**, ACE information appears for all ACEs associated with the ACL. If you enter the **<ace-id>**, ACE information for the requested ACE appears. If you provide no **<acl-id>**, the command shows switch-wide ACL configuration data as viewed in the following figure.

Figure 47
show filter acl ace partial command output

```
================================================================================
                           Ace Action Table (Part I)
================================================================================
Acl  Ace  AceName                  Admin   Oper    Mode    Mlt Remark  Remark
Id   Id                            State   State            Id DSCP    Dot1p
--------------------------------------------------------------------------------
10   1    DHCP                     Enable  Up      permit 0   disable disable
10   2    DNS                      Enable  Up      permit 0   disable disable
10   3    ICMP                     Enable  Up      permit 0   disable disable
10   4    VOIP                     Enable  Up      permit 0   disable disable
10   5    SNAS HTTP/HTTPS          Enable  Up      permit 0   disable disable
10   6    ARP                      Enable  Up      permit 0   disable disable
4082 1    CSE 1000 - UDP SRC       Enable  Up      permit 0   disable disable
4082 2    BCM - UDP SRC            Enable  Up      permit 0   disable disable
4082 3    BCM - UDP DST            Enable  Up      permit 0   disable disable
4082 4    BCM - TCP SRC            Enable  Up      permit 0   disable disable
4082 5    BCM - TCP DST            Enable  Up      permit 0   disable disable
4082 6    Meridian-Trunk 2.0 UDP SRCEnable  Up      permit 0   disable disable
4082 7    Meridian-Trunk 2.0 UDP DSTEnable  Up      permit 0   disable disable
4082 8    Meridian-Trunk 2.0 TCP DSTEnable  Up      permit 0   disable disable
4082 9    MSL 100IP - UDP SRC      Enable  Up      permit 0   disable disable
4082 10   MSL 100IP - UDP DST      Enable  Up      permit 0   disable disable

4082 11   MSL 100IP - TCP SRC      Enable  Up      permit 0   disable disable
4082 12   MSL 100IP - TCP DST      Enable  Up      permit 0   disable disable
4082 13   VCON - UDP SRC           Enable  Up      permit 0   disable disable
4082 14   VCON - UDP DST           Enable  Up      permit 0   disable disable
4082 15   MINERVA - UDP SRC        Enable  Up      permit 0   disable disable
4082 16   MINERVA - UDP DST        Enable  Up      permit 0   disable disable

================================================================================
                           Ace Action Table (Part II)
================================================================================
Acl  Ace  Redirect Next-Hop                           Unreach Police Egress Egress
Id   Id                                               -able          Q      Q-1g
--------------------------------------------------------------------------------
10   1    0.0.0.0                                     deny    0      64     64
10   2    0.0.0.0                                     deny    0      64     64
10   3    0.0.0.0                                     deny    0      64     64
10   4    0.0.0.0                                     deny    0      64     64
10   5    0.0.0.0                                     deny    0      64     64
10   6    0.0.0.0                                     deny    0      64     64
4082 1    0.0.0.0                                     deny    0      64     64
4082 2    0.0.0.0                                     deny    0      64     64
4082 3    0.0.0.0                                     deny    0      64     64
4082 4    0.0.0.0                                     deny    0      64     64

--More-- (q = quit)
```

ACT data

Use the **show filter act** command to display ACT data. The syntax for this command is as follows.

show filter act [<act-id>]

The following table explains parameters for this command.

Table 41
Command parameters

Parameter	Description
act-id	Specifies a unique identifier (in the range 1 through 4096) for this ACT entry.

If you provide no**<act-id>**, the command shows switch-wide ACT configuration data.

ATTENTION
Any show command that displays information that cannot fit on one screen appears as two tables: Part 1 and Part 2.

ACT pattern data

Use the **`show filter act-pattern`** command to display ACT pattern data. The syntax for this command is as follows.

`show filter act-pattern [ <act-id> ]`

The following table explains parameters for this command.

Table 42
Command parameters

Parameter	Description
`act-id`	Specifies a unique identifier (in the range 1–4096) for this ACT entry.

The following figure shows sample output for this command.

Figure 48
show filter act-pattern command output

```
ERS-8610:5#show filter act-pattern 1

================================================================================
                              ACT Pattern Table
================================================================================
Id   Pattern Pattern                          Pattern          Pattern Pattern
     Number  Name                             Base             Offset  Length
--------------------------------------------------------------------------------
1    1       samplepattern                    ip-options-begin 76000   56
```

Basic OSPF information about a port

Use the **`show ports statistics ospf main`** command to display basic OSPF information about the specified port or for all ports. The syntax for this command is as follows.

`show ports statistics ospf main <ports>`

The following table explains parameters for this command.

Table 43
Command parameters

Parameter	Description
`<ports>`	Specifies the port or range of ports configured in the format slot/port.

Extended OSPF information

Use the **`show routing statistics interface`** command to display extended OSPF information about the specified port or for all ports. The syntax for this command is as follows.

```
show routing statistics interface <interface> [slot/port]
```

The following table explains the parameters for this command.

Table 44
Command parameters

Parameter	Description
`interface`	Specifies the interface type for which to report statistics. The options include fastethernet and gigabitEthernet.
`slot/port`	Specifies a particular slot and port or list of ports for which to provide results. If you omit a specific port or port list, results include all ports on the interface type.

The following figure shows sample output for this command.

Figure 49
show routing statistics interface command output

```
ERS-8606:5#show routing statistics interface fastethernet

================================================================================
                              Port Stats Routing
================================================================================
PORT     IN_FRAME   IN_FRAME   IN        OUT_FRAME  OUT_FRAME
NUM      UNICAST    MULTICAST  DISCARD   UNICAST    MULTICAST
--------------------------------------------------------------------------------
4/1      36         0          0         0          98110
4/2      0          0          0         0          0
4/3      0          0          0         0          0
ERS-8606:5#
```

Interface (VLAN or brouter port) configuration output

Use the **`show ipv6 interface`** command to view the output of all configured interfaces. The syntax for this command is as follows.

```
show ipv6 interface [<interface-type>] [<interface-id>]
[<interface-index>]
```

The following table explains the parameters for this command.

Table 45
Command parameters

Parameter	Description
`interface-id`	Specifies the interface ID

Table 45
Command parameters (cont'd.)

Parameter	Description
`interface-index`	Specifies the index from 1–4096.
`interface-type`	Specifies the type of interface if you want to limit the output. The options are fastEthernet, gigabitEthernet, icmpstatistics, statistics, or vlan.

Figure 50 "show ipv6 interface" (page 428) shows sample output for this command.

Figure 50
show ipv6 interface

```
ERS-8603:3# show ipv6 interface

================================================================================
                          Interface Information
================================================================================
IFINDX VLAN-ID/ MTU     PHYSICAL           ADMIN   OPER    RCHBLE  RETRAN  TYPE
       BROUTER          ADDRESS            STATE   STATE   TIME    TIME

--------------------------------------------------------------------------------
64     1/1      1500    0:4:38:7e:86:3     disable down    0       1000    ETHER
2049   1        1500    0:4:38:7e:86:0     disable down    0       1000    ETHER
2050   2        1500    0:4:38:7e:86:1     disable down    0       1000    ETHER
2051   3        1500    0:4:38:7e:86:2     disable down    0       1000    ETHER
--------------------------------------------------------------------------------

================================================================================
                          Address Information
================================================================================
INTF   IPV6                                      TYPE    ORIGIN    STATUS
INDEX  ADDRESS
--------------------------------------------------------------------------------
64     fe80:0:0:0:204:38ff:fe7e:8603             UNICAST OTHER     UNKNOWN
2049   fe80:0:0:0:204:38ff:fe7e:8600             UNICAST OTHER     UNKNOWN
2050   fe80:0:0:0:204:38ff:fe7e:8601             UNICAST OTHER     UNKNOWN

2051   fe80:0:0:0:204:38ff:fe7e:8602             UNICAST OTHER     UNKNOWN
-------------------------------------------------------------------------------
```

IPv6 static route information

Use the **`show ipv6 route`** command to display the existing IPv6 static routes for the switch or for a specific net or subnet. The syntax for this command is as follows.

`show ipv6 route static`

Figure 51 "show ipv6 route static" (page 429) shows sample output for this command.

Figure 51
show ipv6 route static

```
ERS-8603:3# show ipv6 route static

================================================================================
                         Static Route Information
================================================================================
DEST-IP                                   NET IFINDX(VID/BRT/TUN) ENABLE  STATUS
NEXT-HOP                                  LOCAL-NEXT-HOP       PREFERENCE
--------------------------------------------------------------------------------
124:0:0:0:0:0:0:0                         10  2050  (2      ) enable  inactive
0:0:0:0:0:0:0:0                           enable            5
--------------------------------------------------------------------------------
```

MLD cache

Use the **`show ipv6 mld-cache interface`** command to display the MLD cache for a brouter port, VLAN, or group address. The syntax for this command is as follows.

`show ipv6 mld-cache interface <interface-type> <interface-id> [grp-address <0-46>] [detail]`

The following table explains the parameters for this command.

Table 46
Command parameters

Parameter	Description
`grp-address`	Specifies the group address to display.
`interface-id`	Specifies the interface ID.
`interface-type`	Specifies the type of interface if you want to limit the output. The options are fastEthernet, gigabitEthernet, or vlan.

MLD configuration

Use the **`show ipv6 mld interface`** command to display configuration details for all MLD interfaces. The syntax for this command is as follows.

`show ipv6 mld interface [<interface-type> <interface-id>] [detail]`

The following table explains the parameters for this command.

Table 47
Command parameters

Parameter	Description
`interface-id`	Specifies the interface ID.
`interface-type`	Specifies the type of interface if you want to limit the output. The options are fastEthernet, gigabitEthernet, or vlan.

Figure 52 "show ipv6 mld interface" (page 430) shows sample output for this command.

Figure 52
show ipv6 mld interface

```
ERS-8603:3# show ipv6 mld interface
================================================================================
                        MLD Interface Information
================================================================================
VID/BRT Q-INT  VR QUERIER                                  Q-M-R  ROBUST L-M-Q
--------------------------------------------------------------------------------
VID55   125    1  0:0:0:0:0:0:0:0                          10     2      1
2/1     125    1  0:0:0:0:0:0:0:0                          10     2      1
 Legend: Q-INT: query-interval VR: version
         Q-M-R: query-max-resp ROBUST: robustval
         L-M-Q: last-memb-query-int

ERS-8603:3# show ipv6 mld interface vlan 55
================================================================================
                        MLD Interface Information
================================================================================
VID/BRT Q-INT  VR QUERIER                                  Q-M-R  ROBUST L-M-Q
--------------------------------------------------------------------------------
VID55   125    1  0:0:0:0:0:0:0:0                          10     2      1
 Legend: Q-INT: query-interval VR: version
         Q-M-R: query-max-resp ROBUST: robustval
         L-M-Q: last-memb-query-int
```

Neighbor cache

Use the **`show ipv6 neighbor`** command to view entries in the neighbor cache. The syntax for this command is as follows.

`show ipv6 neighbor [<ipv6addr>] [type {other|dynamic|static|local}] [interface <interface-type> <interface-id>]`

The following table explains the parameters for this command.

Table 48
Command parameters

Parameter	Description
`interface-id`	Specifies the interface ID.

Table 48
Command parameters (cont'd.)

Parameter	Description
`interface-type`	Specifies the type of interface if you want to limit the output. The options are fastEthernet, gigabitEthernet, or vlan.
`type`	Specifies the type of mapping as one of the following: • other • dynamic • static • local

Figure 53 "show ipv6 neighbor" (page 431) shows sample output for the **show ipv6 neighbor** command.

Figure 53
show ipv6 neighbor

```
================================================================================
                              Neighbor Information
================================================================================
NET ADDRESS/                                      PHYS  TYPE     STATE      LAST
PHYSICAL ADDRESS                                  INTF                      UPD
--------------------------------------------------------------------------------
4040:0:0:0:0:0:0:1/                               4/18  STATIC   REACHABLE  85907
00:80:2d:c0:92:03
8888:0:0:0:0:0:0:1/                               4/29  STATIC   REACHABLE  84754
00:80:2d:c0:92:03
999:0:0:0:0:0:0:1/                                4/17  STATIC   REACHABLE  84316
00:80:2d:c0:92:03
--------------------------------------------------------------------------------
```

Neighbor discovery prefixes

Use the **show ipv6 nd-prefix** interface command to view all configured neighbor discovery prefixes. The syntax for this command is as follows.

show ipv6 nd-prefix interface <interface-type> <interface-id>]

The following table explains the parameters for this command.

Table 49
Command parameters

Parameter	Description
`interface-id`	Specifies the interface ID.
`interface-type`	Specifies the type of interface if you want to limit the output. The options are fastEthernet, gigabitEthernet, or vlan.

Figure 54 "show ipv6 nd-prefix interface" (page 432) shows sample output for the **show ipv6 nd-prefix interface** command.

Figure 54
show ipv6 nd-prefix interface

```
ERS-8603:3#show ipv6 nd-prefix interface vlan 2

================================================================================
                         Vlan Ipv6 Nd Prefix
================================================================================
INTF  IPV6                                              VLAN  VALID    PREF     EUI
INDEX ADDRESS/PREFIX                                    ID    LIFE     LIFE
--------------------------------------------------------------------------------
2050  8:0:0:0:0:0:0:0/24                                2     1111     999      1

1 out of 2 Total Num of Ipv6 ND prefix Entries displayed.
-------------------------------------------------------------------------------

ERS-8603:3#show ipv6 nd-prefix interface GigabitEthernet 2/1

================================================================================
                         Port Ipv6 Nd Prefix
================================================================================
INTF  IPV6                                              BTR   VALID    PREF     EUI
INDEX ADDRESS/PREFIX                                          LIFE     LIFE
--------------------------------------------------------------------------------
128   6:0:0:0:0:0:0:0/24                                2/1   1111     1555     1

1 out of 2 Total Num of Ipv6 ND prefix Entries displayed.
```

OSPF areas

Use the **show ipv6 ospf area** command to display information about OSPF area parameters. The syntax for this command is as follows.

show ipv6 ospf area

The following figure shows sample output for this command.

Figure 55
show ipv6 ospf area

```
ERS-8610:5(config)#show ipv6 ospf area

================================================================================
                                   OSPF Area
================================================================================
AREA_ID          STUB_AREA   NSSA   IMPORT_SUM  TRANS_ROLE
--------------------------------------------------------------------------------
0.0.0.0          false       false  true        always
STUB_METRIC  SPF_RUNS  BDR_RTR_CNT  ASBDR_RTR_CNT  LSA_CNT  LSACK_SUM
--------------------------------------------------------------------------------
10           0         0            0              0        0
```

OSPF configuration settings for a port

Use the **show ip ospf interface** command to display information about the OSPF parameters of the specified port or all ports. The syntax for this command is as follows.

`show ip ospf interface [<interface-type>] [<interface-id>]`

The following table explains the parameters for this command.

Table 50
Command parameters

Parameter	Description
`interface-id`	Specifies the interface ID.
`interface-type`	Specifies the type of interface if you want to limit the output. The options are fastethernet, gigabitethernet, pos, or vlan.

Figure 56 "show ip ospf interface" (page 433) shows sample output for this command.

Figure 56
show ip ospf interface

```
================================================================================
                                   Port Ospf
================================================================================
PORT         HELLO   RTRDEAD OSPF
NUM   ENABLE INTVAL  INTVAL  PRIORITY METRIC AUTHTYPE AUTHKEY    AREA_ID
--------------------------------------------------------------------------------
4/1   false  10      40      1        0      none                0.0.0.0
```

OSPF information

Use the **`show ipv6 ospf`** command to display the current OSPF settings for the switch. The syntax for this command is as follows.

`show ipv6 ospf`

The following figure shows sample output for this command.

Figure 57
show ipv6 ospf command output

```
ERS-8610:5(config)#show ipv6 ospf

================================================================================
                           OSPFv3 Global Information
================================================================================
        router-id                       : 232.158.16.0
        admin-state                     : ENABLED
        version                         : 3
        area-bdr-rtr-state              : FALSE
        as-bdr-rtr-state                : FALSE
        as-scope-lsa-count              : 0
        lsa-checksum                    : 0
        originate-new-lsas              : 0
        rx-new-lsas                     : 0
        ext-lsa-count                   : 0
        ext-area-lsdb-limit             : -1
        multicast-ext                   : intraAreaMulticast
        exit-voer-flow-interval         : 4294967295
        demand-extensions               : FALSE
        traffic-engineering-support     : FALSE
        reference-bandwidth             : 1000000
        restart-support                 : none
        restart-interval                : 1800
        restart-status                  : notRestarting

        restart-age                     : 1800
        restart-exit-reason             : none
```

OSPF interface information

Use the **show ipv6 ospf interface** command to display information about the OSPF interface.

show ipv6 ospf interface [{vlan|fastEthernet|gigabitEthernet} {vlan-id|slot/port}]

The following figure shows sample output for this command.

Figure 58
show ipv6 ospf interface

```
ERS-8603:3# show ipv6 ospf interface
================================================================================
                          OSPF Interface
================================================================================
IFINDX(VID/BRT)  AREAID          ADM IFSTATE  METRIC PRI DR/BDR          IFTYPE
--------------------------------------------------------------------------------
2050  (2      )  10.1.1.1        dis UNDEF    1      1   0.0.0.0         BROADCAST
                                                        0.0.0.0

================================================================================
                          OSPF Virtual Interface
================================================================================
AREAID           NBRIPADDR       STATE
--------------------------------------------------------------------------------
```

OSPF interface timer settings

Use the **show ipv6 ospf int-timers** command to display OSPF interface timer settings. The syntax for this command is as follows:

show ipv6 ospf int-timers

The following figure shows sample output for this command.

Figure 59
show ipv6 ospf int-timers command output

```
==========================================================================================
                              OSPF Interface Timers
==========================================================================================
                                   TRANSIT  RETRANS  HELLO    DEAD     POLL
IFINDX(VID/BRT) AREAID             DELAY    INTERVAL INTERVAL INTERVAL INTERVAL
------------------------------------------------------------------------------------------
220   (3/29    ) 0.0.0.0           1        5        10       40       120
2050  (12      ) 3.0.0.0           1        5        10       40       120
2051  (100     ) 0.0.0.0           1        5        10       40       120

==========================================================================================
                          OSPF Virtual Interface Timers
==========================================================================================
                                   TRANSIT  RETRANS  HELLO    DEAD
AREAID          NBRIPADDR          DELAY    INTERVAL INTERVAL INTERVAL
------------------------------------------------------------------------------------------
3.0.0.0         3.0.0.1            1        5        10       60
```

OSPF link-state database table

Use the **show ipv6 ospf lsdb** command to display the OSPF link-state database (LSDB) table. The syntax for this command is as follows.

show ipv6 ospf lsdb [scope <1-3>] [tunnel <1-2147483647>] [area <A.B.C.D>] [lsa-type <1-8>] [adv-rtr <A.B.C.D>] [lsid <0-4294967295>] [detail]

You can specify a scope, VLAN, tunnel, area string, link-state advertisement type (0 to 5), link state ID, or advertising router. If you add the **detail** option to the command, the output contains additional information.

Figure 60 "show ipv6 ospf lsdb" (page 436) shows sample output with no variables for this command.

Figure 60
show ipv6 ospf lsdb

```
ERS-8603:3# show ipv6 ospf lsdb
================================================================================
                         Link Scope LSAs
================================================================================
VID/BRT/TUN   TYPE            ROUTER ID       LS ID      AGE   CKSUM Sequence
--------------------------------------------------------------------------------

================================================================================
                         Area Scope LSAs
================================================================================
AREA ID         TYPE            Router ID       LS ID      AGE   CKSUM Sequence

================================================================================
                         AS Scope LSAs
================================================================================
TYPE            Router ID       LS ID      AGE   CKSUM Sequence
--------------------------------------------------------------------------------
```

OSPF neighbors

Use the **show ipv6 ospf neighbor** command to display OSPF neighbors configuration information. The syntax for this command is as follows.

show ipv6 ospf neighbor

Figure 61 "show ipv6 ospf neighbor command output" (page 436) shows sample command output for this command.

Figure 61
show ipv6 ospf neighbor command output

```
================================================================================
                                 OSPF Neighbor
================================================================================
INTERFACE NBRROUTERID     NBRIPADDR                                 PRIO_STATE
--------------------------------------------------------------------------------
2050      3.0.0.1         fe80:0:0:0:211:f9ff:fed0:202              Full
2051      1.0.0.1         fe80:0:0:0:280:2dff:fe32:5604             Full

================================================================================
                             OSPF Virtual Neighbor
================================================================================
NBRAREAID       NBRROUTERID     VIRTINTFID NBRIPV6ADDR
   STATE
--------------------------------------------------------------------------------
0.0.0.0         3.0.0.1         6050       3000:0:0:0:0:0:0:1
Full
================================================================================
                               OSPF NBMA Neighbor
================================================================================
INTERFACE NBRROUTERID     NBRIPADDR                                 STATE
--------------------------------------------------------------------------------
```

OSPFv3 information for VLANs

Use the **show ip ospf interface** command to view OSPFv3 information for VLANs. The syntax for this command is as follows.

```
show ip ospf interface vlan <vlan-id>
```

The following figure shows sample output for this command.

Figure 62
show ip ospf interface

```
ERS-8606:5#show ip ospf interface vlan 2

================================================================================
                                   Vlan Ospf
================================================================================
VLAN         HELLO     RTRDEAD  DESIGRTR
ID     ENABLE INTERVAL INTERVAL PRIORITY METRIC AUTHTYPE AUTHKEY    INTF   AREAID
--------------------------------------------------------------------------------
2      false  10       40       1        0      none                b     0.0.0.0

TYPE Legend:
n=nbma interface, p=passive interface, b=broadcast interface
```

Tunnel information

Use the **show ipv6 tunnel** command to show general tunnel information. The syntax for this command is as follows.

```
show ipv6 tunnel [<tunnel-id>] [local <A.B.C.D>] [remote
<A.B.C.D>] [detail]
```

The following table explains the parameters for this command.

Table 51
Command parameters

Parameter	Description
`detail`	Displays address information in addition to basic tunnel information.
`tunnel-id`	Specifies the ID number of the tunnel in the range 1 through 2 147 483 647.

The following figure shows sample output for the **show ipv6 tunnel** command.

Figure 63
show ipv6 tunnel

```
ERS-8606:5# show ipv6 tunnel

================================================================================
                         Tunnel If Information
================================================================================
TUNNEL-ID LOCAL ADDRESS   REMOTE ADDRESS   TYPE  TTL

--------------------------------------------------------------------------------
1         10.1.1.1        0.0.0.0          6to4  255


ERS-8606:5# show ipv6 tunnel detail

================================================================================
                         Tunnel Interface Information
================================================================================
ID         LOCAL ADDRESS   REMOTE ADDRESS   OPER STATUS TYPE
--------------------------------------------------------------------------------
1          1.1.1.1         3.3.3.3         inactive    manual

1 out of 1 Total number of entries displayed.

--------------------------------------------------------------------------------

================================================================================
                         Address Information
================================================================================
IPV6                                      TYPE    ORIGIN    STATUS
ADDRESS
--------------------------------------------------------------------------------
1:1:1:1:1:1:1:1                           UNICAST MANUAL    TENTATIVE
fe80:0:0:0:0:0:101:101                    UNICAST OTHER     UNKNOWN

2 out of 2 Total number of entries displayed.
```

ICMPv6 type and code

The Internet Control Message Protocol (ICMPv6) uses many messages identified by a type and code field (see RFC2463). Error messages use message types 0 to 127. Informational messages use message types 128 to 255.

Table 52
ICMPv6 type and code details

Type	Name	Code	Reference
1	Destination Unreachable	0—no route to destination 1—communication with destination administratively prohibited 2—(not assigned) 3—address unreachable 4—port unreachable	RFC 2463
2	Packet Too Big	N/A	RFC 2463
3	Time Exceeded	0—hop limit exceeded in transit 1—fragment reassembly time exceeded	RFC 2463
4	Parameter Problem	0—erroneous header field encountered 1—unrecognized Next Header type encountered 2—unrecognized IPv6 option encountered	RFC 2463

Table 52
ICMPv6 type and code details (cont'd.)

Type	Name	Code	Reference
128	Echo Request	N/A	RFC 2463
129	Echo Reply	N/A	RFC 2463
130	Multicast Listener Query	N/A	
131	Multicast Listener Report	N/A	
132	Multicast Listener Done	N/A	
133	Router Solicitation	N/A	RFC 2461
134	Router Advertisement	N/A	RFC 2461
135	Neighbor Solicitation	N/A	RFC 2461
136	Neighbor Advertisement	N/A	RFC 2461
137	Redirect Message	N/A	RFC 2461
138	Router Renumbering	0—router renumbering command 1—router renumbering result 255—sequence number reset	
139	ICMP Node Information Query	N/A	
140	ICMP Node Information Response	N/A	
141	Inverse neighbor discovery Solicitation Message	N/A	RFC 3122
142	Inverse neighbor discovery Advertisement Message	N/A	RFC 3122
143	Version 2 Multicast Listener Report	N/A	RFC 3810
144	Home Agent Address Discovery Request Message	N/A	RFC 3775
145	Home Agent Address Discovery Reply Message	N/A	RFC 3775
146	Mobile Prefix Solicitation	N/A	RFC 3775
147	Mobile Prefix Advertisement	N/A	RFC 3775

RFC reference for IPv6

The following is a list of RFCs used in IPv6:

- RFC
- RFC 1812, Requirements for IP Version 4 Routers
- RFC 1881, IPv6 Address Allocation Management
- RFC 1886, DNS Extensions to support IP version 6
- RFC 1887, An Architecture for IPv6 Unicast Address Allocations
- RFC 1981, Path MTU Discovery for IP version 6
- RFC 2030, Simple Network Time Protocol (SNTP) v4 for IPv4, IPv6 and OSI
- RFC 2373, IPv6 Addressing Architecture
- RFC 2375, IPv6 Multicast Address Assignments
- RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2452,IP Version 6 Management Information Base for the Transmission Control Protocol
- RFC 2454, IP Version 6 Management Information Base for the User Datagram Protocol
- RFC 2460, Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461, Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462, IPv6 Stateless Address Autoconfiguration
- RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464, Transmission of IPv6 Packets over Ethernet Networks

- RFC 2465, Management Information Base for IP Version 6: Textual Conventions and General Group
- RFC 2466, Management Information Base for IP Version 6: ICMPv6 Group
- RFC 2474, Definition of the Differential Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2526, Reserved IPv6 Subnet Anycast Addresses
- RFC 2710, Multicast Listener Discovery (MLD) for IPv6
- RFC 2740, OSPF for IPv6
- RFC 2893, Transition Mechanisms for IPv6 Hosts and Routers
- RFC 3019, IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
- RFC 3056, Connection of IPv6 Domains via IPv4 Clouds
- RFC 3122, Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification
- RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3363, Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)
- RFC 3364, Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)
- RFC 3446, Anycast Rendevous Point (RP) mechanism using Protocol Independant Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
- RFC 3484, Default Address Selection for IPv6
- RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3587, IPv6 Global Unicast Address Format
- RFC 3590, Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
- RFC 3596, DNS Extensions to Support IP Version 6
- RFC 3618, Multicast Source Discovery Protocol (MSDP)
- RFC 3775, Mobility Support in IPv6
- RFC 3810, IPv6 Multicast capabilities
- RFC 4022, Management Information Base for the Transmission Control Protocol (TCP)
- RFC 4087, IP Tunnel MIB

- RFC 4113, Management Information Base for the User Datagram Protocol (UDP)
- RFC 4649, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option
- draft-ietf-vrrp-ipv6-spec-08.txt, Virtual Router Redundancy Protocol for IPv6

Descriptions of management information bases (MIBs) in this document are based on information from the listed RFCs.

Nortel Ethernet Routing Switch 8600

Configuration — IPv6 Routing

Release: 7.0
Publication: NN46205-504
Document revision: 03.02
Document release date: 12 April 2010

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

www.nortel.com

NORTEL