

>THIS IS **THE WAY**

>THIS IS **NORTEL**

Nortel Multiservice Switch 7400/15000/20000

IP VPN Configuration Management

NN10600-803

Document status: Standard
Document issue: 7.1S1
Document date: October 2005
Product release: PCR7.1 and up
Job function: Operations
Type: NTP
Language type: U.S. English

Copyright © 2005 Nortel.
All Rights Reserved.

NORTEL the globemark design, and the NORTEL corporate logo are trademarks of Nortel.



Contents

What's new	6
FR Extended Burst Support	6
Inter-VRF RFC 2547	7
Multi-link PPP on Multiservice Switch 7400	7
RFC 2547 Fast Ethernet (FE) Trunking (port mode) and RFC 2547 Gigabit Ethernet (GE) trunking (VLAN)	7
RFC2764 support on 16p OC3/STM1 ATM GQM	7
VPN configuration	8
BGP/MPLS VPN configuration	10
Configuring the router and primary loopback	14
Configuring IP CPP on the RTR	16
Configuring EBGP and peers for address family ipv4Label	18
Changing an MD5 key on an authenticated BGP peer	21
Configuring BGP import policy	23
Configuring BGP and peers for address family ipv4MplsVpn	27
Configuring BGP export policy	30
Media configuration	32
Configuring Ethernet media in port mode	34
Configuring Ethernet media in VLAN mode	36
Configuring ATM media for single link congestion control	38
Configuring ATM media for multi link congestion control	40
Routing protocol configuration	43
Configuring OSPF as an IGP	44
Configuring ISIS as an IGP	46
MPLS configuration	48
Configuring LDP	50
Configuring alarm generation for MPLS transport LSPs	52
Configuring MD5 Authentication on an LDP neighbor	53
Changing an MD5 key on an authenticated LDP session	55
VRF and access configuration	58
Configuring a VRF	62



Configuring ATM media and feature set	67
Configuring PPP media and feature set for VRF in RFC2547 mode	70
Configuring Ethernet media and feature set	72
Creating a VRRP virtual router	74
Example of creating a VRRP virtual router associated with an Ethernet interface in port mode	77
Example of creating a VRRP virtual router associated with a VLAN on an Ethernet interface	80
Configuring frame relay media and feature set	82
Configuring EBGp	85
Changing an MD5 key on an authenticated EBGp peer	88
Configuring BGP route flood protection	90
Configuring BGP peer route flood protection	92
Configuring OSPF	94
Configuring static routing	96
Configuring RIP	97
Configuring a default static route in a scaled environment	99
Configuring the VRF export policy	101
Configuring IP CPP on the VRF	104
Configuring VRF route flood protection	106
<hr/>	
BGP/MPLS VPN configuration example	108
Example of a backbone configuration for PE node Multiservice Switch 1 (Multiservice Switch 7400 node)	110
Access Configuration for PE node Multiservice Switch 1 (Multiservice Switch 7400 node)	113
Example of a backbone configuration for PE node Multiservice Switch 2 (Multiservice Switch 15000 node)	116
Access Configuration for PE node Multiservice Switch 2 (Multiservice Switch 15000 node)	118
Example of configuring a P node on a Multiservice Switch 3 (Multiservice Switch 15000 node)	121
Example of configuring a BGP MED policy	124
Example of configuring a VRF policy	126
Example of configuring a route target export policy	128
<hr/>	
VCG-based IP VPN configuration	129
<hr/>	
VCG-based IP VPN core configuration	131
Configuring core media	134
Configuring VCG	136
Configuring a core protocol port	137
Configuring virtual media for tunnel endpoints	139
Configuring round-trip delay measurements	141
Example of configuring BGP on a VCG with dynamic tunnels	143



VCG-based IP VPN customer access configuration **146**

Configuring a customer virtual router 149

Configuring a dynamic tunnel 150

Configuring a static tunnel 153

Example of configuring a static tunnel 156

Configuring ARP entries 159

Procedure conventions **160**

Operational mode 160

Provisioning mode 161

Activating configuration changes 161



What's new

The following features were added to this document:

- [FR Extended Burst Support \(page 6\)](#)
- [Inter-VRF RFC 2547 \(page 7\)](#)
- [Multi-link PPP on Multiservice Switch 7400 \(page 7\)](#)
- [RFC 2547 Fast Ethernet \(FE\) Trunking \(port mode\) and RFC 2547 Gigabit Ethernet \(GE\) trunking \(VLAN\) \(page 7\)](#)
- [RFC2764 support on 16p OC3/STM1 ATM GQM \(page 7\)](#)

Other changes made to this document include the following:

Attention: To ensure that you are using the most current version of an NTP, check the current NTP list in NN10600-000 *Nortel Multiservice Switch 7400/15000/20000 What's New*.

- This document was renumbered from NN10600-582 to NN10600-803 as part of an ongoing effort to improve the organization of Nortel Multiservice Switch documentation.
- Updated the section [Configuring virtual media for tunnel endpoints \(page 139\)](#) to update information about the network address logical interface.
- Updated the section [Configuring Ethernet media in port mode \(page 34\)](#) to include information about configuring an Ethernet interface in port mode.
- Replaced obsolete request for comments (RFC) references with current RFC references.

FR Extended Burst Support

The following section was updated for this feature:

- [Configuring frame relay media and feature set \(page 82\)](#)



Inter-VRF RFC 2547

The following section was updated for this feature:

- [Configuring the VRF export policy \(page 101\)](#)

Multi-link PPP on Multiservice Switch 7400

The following section was updated for this feature:

- [Configuring PPP media and feature set for VRF in RFC2547 mode \(page 70\)](#)

RFC 2547 Fast Ethernet (FE) Trunking (port mode) and RFC 2547 Gigabit Ethernet (GE) trunking (VLAN)

The following sections were updated for this feature:

- [Configuring Ethernet media in port mode \(page 34\)](#)
- [Configuring Ethernet media in VLAN mode \(page 36\)](#)

RFC2764 support on 16p OC3/STM1 ATM GQM

The following sections were updated for this feature:

- [Configuring a static tunnel \(page 153\)](#)
- [Example of configuring a static tunnel \(page 156\)](#)



VPN configuration

Virtual private network (VPN) configuration allows for multiple customer virtual routers (VRs) in a single virtual network.

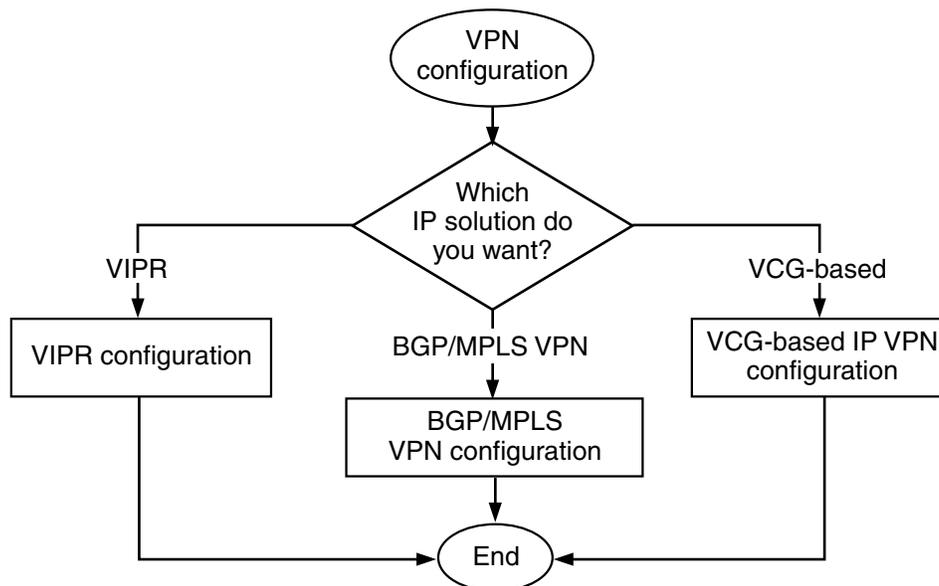
Prerequisites to VPN configuration

- Configure a management VR. For information on configuring a management VR, see NN10600-271 *Nortel Multiservice Switch 7400/15000/20000 Network Management Connectivity*.

VPN configuration tasks

The following work flow shows you the sequence of tasks you perform to configure a VPN. To link to any task, go to [VPN configuration task navigation \(page 9\)](#).

VPN configuration tasks





VPN configuration task navigation

- VIPR configuration. For information, see NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- [BGP/MPLS VPN configuration \(page 10\)](#)
- [VCG-based IP VPN configuration \(page 129\)](#)



BGP/MPLS VPN configuration

The border gateway protocol/multiprotocol label switching (BGP/MPLS) virtual private network (VPN) configuration allows you to configure the Provider Edge (PE), Provider (P), and Carrier's Carrier Customer Edge (CE') nodes in Nortel Multiservice Switch networks. For Carrier's Carrier, the CE' node also functions as a PE node. For information about these terms, and for conceptual and reference information about the BGP/MPLS VPN solution, see NN10600-802 *Nortel Multiservice Switch 7400/15000/20000 IP VPN Technology Fundamentals*

Prerequisites to BGP/MPLS VPN configuration

- Determine the media type prior to configuring software features. The decision you make to use ATM, or GigE media, affects the steps you take to configure the BGP/MPLS VPN.
- The task flow and procedures in this section describe configuring BGP/MPLS services only. Basic configuration at the P node, PE node or CE' node level (in this case, creating an instance of a logical processor type (LPT), and adding the services to the *featureList* component) must be performed first. Use the tasks and procedures in NN10600-550 *Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures* if you require supporting information or need to provision or reconfigure any node or nodal elements to support BGP/MPLS features.
 - For the PE node with a configuration that includes the VPN extender card and the CP card: add the *rfc2547bis*, *bgp*, and *ip* features to the VPN extender card feature list and add the *OamEnet*, *bgp*, and *ip* features to the CP card feature list.
 - For the PE node with a configuration that includes the CP card but no VPN extender card: add the *OamEnet*, *rfc2547bis*, *bgp*, and *ip* features to the CP card feature list.
 - For the PE node, include the *rfc2547bis* feature to the VRF access cards feature list.
 - For the P node, include the *OamEnet* and *ip* features to the CP card feature list.



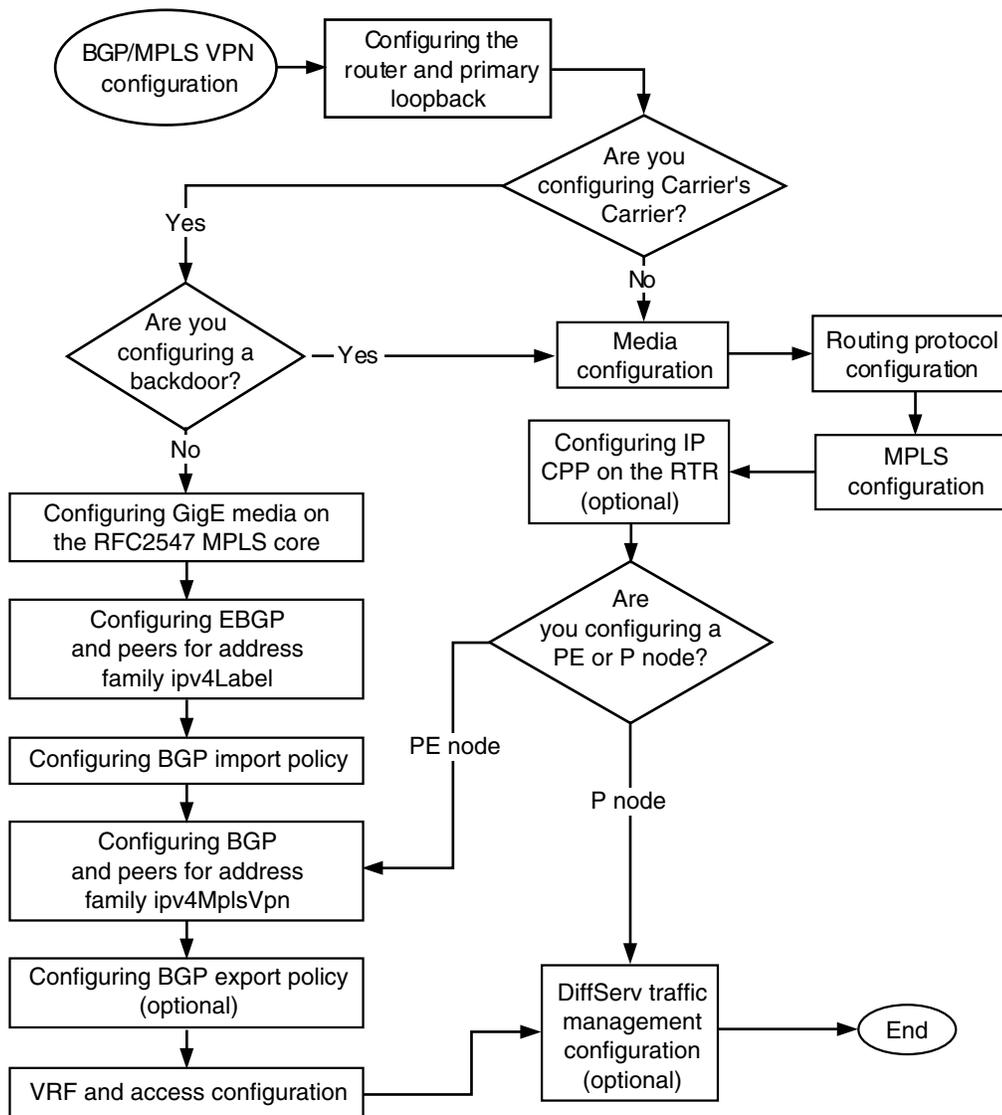
- For the P node, include the *mplsldp*, *atmmpe*, and *ip* features to the ATM card feature list.
- For the CE' node, include the *rfc2547bis* feature to the VRF access cards feature list.
- For the CE' node, include the *rfc2547bis* and *rfc2547bisCscCe* features to the VPN extender card feature list.
- For the CE' node, include the *rfc2547bisCscCe* feature to the GigE FP card feature list.

BGP/MPLS VPN configuration procedures

This task flow shows you the sequence of procedures you perform to configure a BGP/MPLS VPN. To link to any procedure, go to [BGP/MPLS VPN configuration procedure navigation \(page 12\)](#).



BGP/MPLS VPN configuration procedures



MSS 3541 001 AA

BGP/MPLS VPN configuration procedure navigation

- [Configuring the router and primary loopback \(page 14\)](#)
- [Media configuration \(page 32\)](#)
- [Routing protocol configuration \(page 43\)](#)
- [MPLS configuration \(page 48\)](#)
- [Configuring IP CPP on the RTR \(page 16\)](#)
- [Configuring GigE media on the RFC2547 MPLS core, see \[Configuring Ethernet media in port mode \\(page 34\\)\]\(#\) and \[Configuring Ethernet media in\]\(#\)](#)



[VLAN mode \(page 36\)](#) depending on whether you are configuring an Ethernet media in port mode or VLAN mode.

- [Configuring EBGP and peers for address family ipv4Label \(page 18\)](#)
- [Configuring BGP import policy \(page 23\)](#)
- [Configuring BGP and peers for address family ipv4MplsVpn \(page 27\)](#)
- [Configuring BGP export policy \(page 30\)](#)
- [VRF and access configuration \(page 58\)](#)
- DiffServ traffic management configuration. See to NN10600-809 *Nortel Multiservice Switch 7400/15000/20000 Layer 3 Traffic Management Configuration*.
- For examples of BGP/MPLS VPN configuration, refer to [BGP/MPLS VPN configuration example \(page 108\)](#).



Configuring the router and primary loopback

Configure a router to operate as a P node, PE node or CE' node in order to provide IGP connectivity between them. The P node router is a backbone router which is not connected to any CE devices. The PE is connected to one or more CE devices and handles all VPN routing information. Configure a mandatory instance of Loopback interface with mode primaryLoopback. The IP address of this component is called the primaryLoopback address. The primaryLoopback address is used in the RFC 2547 solution by MPLS and BGP control plane as follows:

- LDP-DU as the transport layer next hop when establishing LSP tunnels between PE nodes used to transport VPN traffic
- BGP next hop when distributing VPN routing information between PE nodes

Procedure steps

Step	Action
1	Add the <i>Router</i> component. add Rtr/<rtr_name>
2	Link the router to the VPN extender card or the CP card. set Rtr/<rtr_name> Vrp lp/<n>
3	Add the loopback interface IP address. add -s Rtr/<rtr_name> Interface/<ip_address> Loopback
4	Set the netmask. This must be 32 bits. set Rtr/<rtr_name> Interface/<ip_address> netMask 255.255.255.255
5	Set the <i>mode</i> attribute to primaryLoopback. set Rtr/<rtr_name> Interface/<ip_address> Loopback mode primaryLoopback

--End--

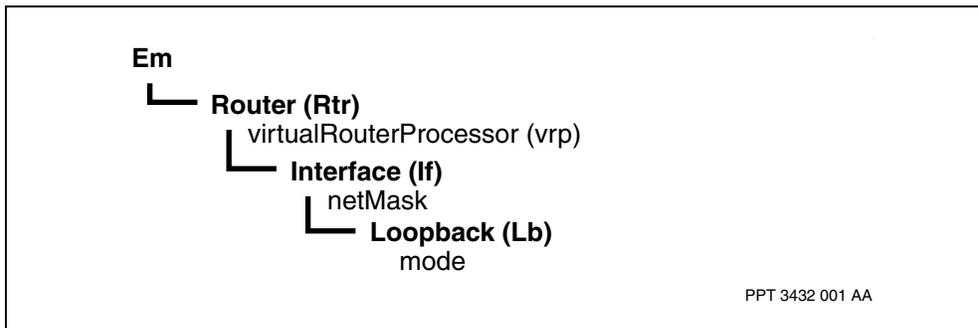


Variable definitions

Variable	Value
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived.
<mask>	is the network mask to be used with the IP address. Must be 32 bits in the case of a loopback interface.
<n>	is the number of the LP. The router can be linked to the VpnXc card or CP card. CPs must be Lp/0.
<rtr_name>	is the name of the router.

Procedure job aid

Router and primary loopback component hierarchy





Configuring IP CPP on the RTR

Configure control plane protection (CPP) on the RTR to protect Nortel Multiservice Switch nodes against certain denial of service (DoS) attacks on the control plane by monitoring the flow rate of IP packets destined for local IP destination addresses (DAs).

Attention: CPP is supported on PQC-based FPs only.

Prerequisites

- See the section on CPP in the *NN10600-800 Nortel Multiservice Switch 7400/15000/20000 IP Technology Fundamentals*.
- The procedure in this section describes configuring CPP software and services only. Basic configuration at the node level (in this case, creating an instance of a logical processor type (LPT), and adding the *ip* and *ipCpp* services to the *featureList* attribute) must be performed first. Use the tasks and procedures in *NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures* if you require supporting information or need to provision or reconfigure any node or nodal elements to support the CPP feature.

Procedure steps

Step	Action
1	Add a <i>Cpp</i> component as a subcomponent of the <i>Rtr</i> component. add Rtr/<rtr_name> cpp
2	Configure the number of packets per second before discard occurs. set Rtr/<rtr_name> cpp packetsPerSecond <packets_per_second>
3	Configure the isolation time period. set Rtr/<rtr_name> cpp isolationTime <isolation_time>
4	Configure the grace period. set Rtr/<rtr_name> cpp gracePeriod <grace_period>
5	Configure the CPP mode. set Rtr/<rtr_name> cpp mode <cpp_mode>

--End--

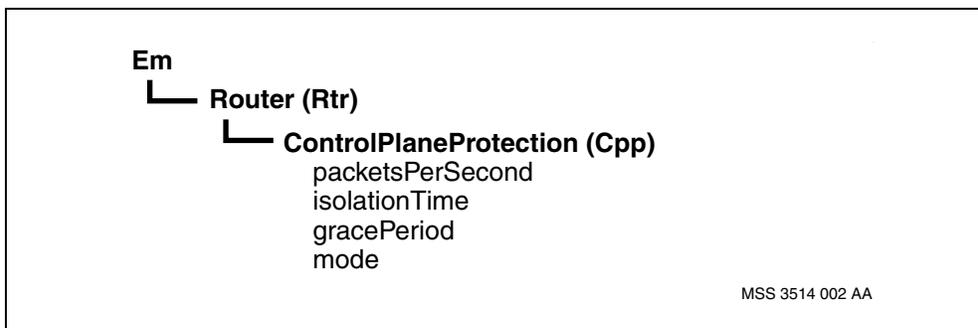


Variable definitions

Variable	Value
<cpp_mode>	is the CPP operational mode: study, protect or disabled. Use study to determine an acceptable traffic rate. Once you learn the rate created and have the appropriate configuration, use protect. Use disabled to pre-configure the feature without enabling the monitoring process.
<grace_period>	is the period over which the average flow rate is measured to ensure that the exceeded traffic flow rate still exceeds the maximum allowed rate. A value of zero in protect mode means that isolation occurs immediately after an excessive flow is detected.
<isolation_time>	is the amount of time over which traffic will be discarded once isolation has begun. A value of zero indicates to permanently discard traffic until the card is cleared by an operator.
<packets_per_second>	is the flow rate, in packets per second, for the VR's DA, that must be exceeded on a single DA before discard processing occurs.
<rtr_name>	is the name of the router.

Procedure job aid

RTR IP CPP component hierarchy





Configuring EBGp and peers for address family ipv4Label

Configure the exterior border gateway protocol (EBGP) for the CE' node and add one peer for each remote PE' node that is directly connected.

EBGP with address family ipv4Label is replacing:

- the interior gateway protocol (IGP) for primary loopback address distribution
- the label distribution protocol (LDP) for transport label distribution

Optionally, configure MD5 authentication on a BGP peer connection to provide protection of BGP neighbor relationships. Change an MD5 key on an authenticated BGP peer using the procedure [Changing an MD5 key on an authenticated BGP peer \(page 21\)](#).

Prerequisites

- If configuring MD5 authentication, use different MD5 key values for each BGP peer. A longer MD5 key will be more difficult to break, however, the longer the key used, the greater the impact on performance. A key length of between 12 and 24 characters should be sufficiently secure without having too great an impact on performance.

Procedure steps

Step	Action
1	Add the <i>Bgp</i> component. add Rtr/<rtr_name> Bgp
2	Set the <i>localAs</i> attribute. set Rtr/<rtr_name> Bgp localAs <local_as_value>
3	Set the <i>bgpIdentifier</i> attribute. set Rtr/<rtr_name> Bgp bgpIdentifier <ip_address>
4	Add the BGP peer. add Rtr/<rtr_name> Bgp Peer/<peer_address> The <i>Descriptor</i> subcomponent is automatically added.
5	Optionally, configure MD5 authentication on a BGP peer connection. Set the MD5 key value under the <i>Descriptor</i> . set Rtr/<rtr_name> Bgp Peer/<ip_addr> Desc md5Key <ASCII_string>
6	Set the <i>LocalAddressConfigured (lac)</i> attribute. set Rtr/<rtr_name> Bgp Peer/<peer_address> Desc lac <lac_ip_address>



- 7 Set the autonomous system that is changed for the BGP peer.
**set Rtr/<rtr_name> Bgp Peer/<peer_address> Desc peerAs
<peer_as_value>**
- 8 Set the address family for the node you are configuring.
**set Rtr/<rtr_name> Bgp Peer/<peer_address> Desc
addressFamily ipv4Label**
- 9 Disable AS_PATH loop detection.
**set Rtr/<rtr_name> Bgp Peer/<peer_address> Desc
asPathCheck disabled**

--End--

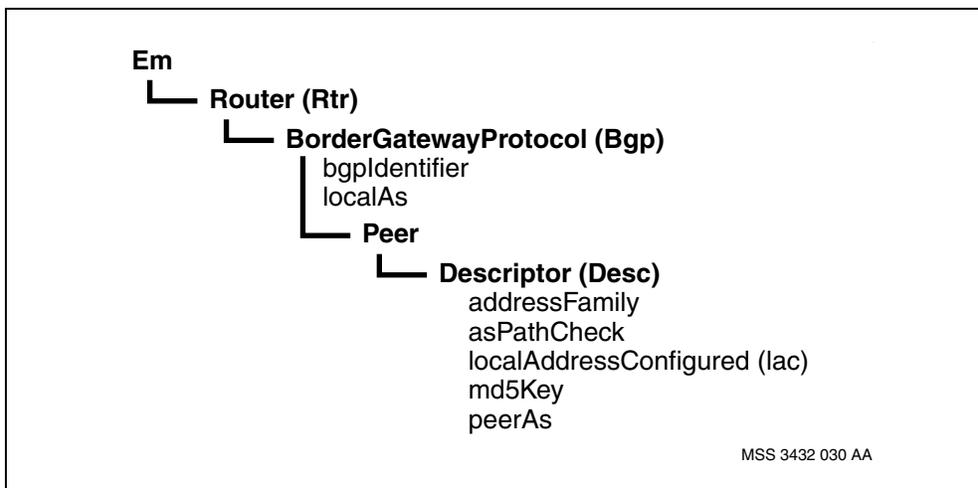


Variable definitions

Variable	Value
<ASCII_string>	is the MD5 key value, 1-255 ASCII characters in length. Any printable ASCII character is allowed. If a space or other non-alphabetic or numeric character is used within the key, then the whole key must be included in quotes. For this reason a " character is the only printable ascii character not allowed as part of a key. A null string indicates that MD5 authentication is not to be used on the connection to this peer.
<ip_address>	is the IP address that matches the primary loopback address.
<lac_ip_address>	is the IP address that matches the CE' interface that is directly connected to the VRF PE' interface.
<local_as_value>	is the value of the autonomous system for the CE' node.
<peer_address>	is the IP address of the VRF PE' interface that is directly connected to the CE' node.
<peer_as_value>	is the value of the autonomous system for the PE' node.
<rtr_name>	is the name of the router.

Procedure job aid

EBGP and peers for address family ipv4Label component hierarchy





Changing an MD5 key on an authenticated BGP peer

Transition MD5 keys without having to terminate the BGP neighbor session for which the key is being changed, if you have optionally configured MD5 authentication on a BGP peer.

When changing keys on a BGP session between a Multiservice Switch node and a non-Multiservice Switch, change the key on the Multiservice Switch node to minimize the outage time.

A longer MD5 key will be more difficult to break, however, the longer the key used, the greater the impact on performance. A key length of between 12 and 24 characters should be sufficiently secure without having too great an impact on performance.

It is recommended that different MD5 key values be used for each BGP-4 peer.

Procedure steps

Step	Action
1	Set the <i>keyTransitionDelay</i> attribute on the local and remote router, for all BGP peers. set Rtr/<rtr_name> Bgp keyTransitionDelay <n>
2	Alternatively, set the <i>keyTransitionDelay</i> attribute on the local and remote router, for a specific peer's <i>Descriptor</i> . set Rtr/<rtr_name> Bgp Peer/<ip_addr> Desc keyTransitionDelay <n>
3	Set the new MD5 key value on the local and remote router. set Rtr/<rtr_name> Bgp Peer/<ip_addr> Desc md5Key <ASCII_string>

--End--

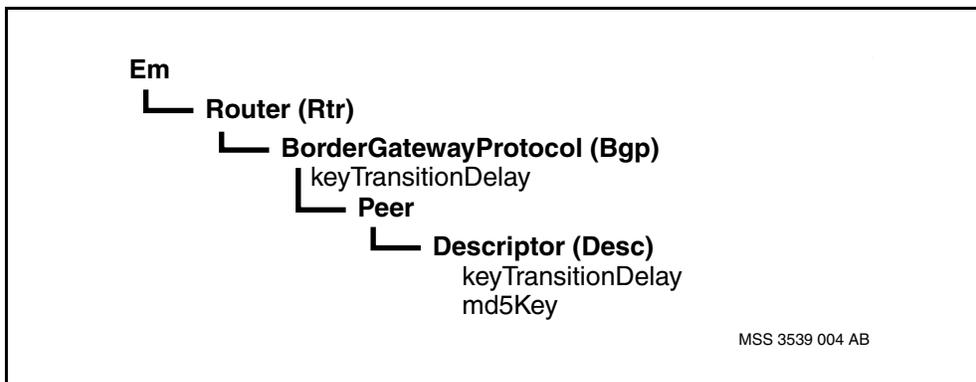


Variable definitions

Variable	Value
<ASCII_string>	is the MD5 key value, 1-255 ASCII characters in length.
<ip_addr>	is a 32-bit address assigned to the interface from which the routing information is derived.
<n>	is the amount of time the operator has to provision both the local and remote ends with the new key, without losing service. for the <i>Bgp</i> component, the value is 1 to 20160 (minutes), default is 10 minutes. for the <i>Descriptor</i> component, the value is “sameAsBgp, 1 to 20160 (minutes)”, default is “sameAsBgp”.
<rtr_name>	is the name of the router.

Procedure job aid

BGP-4 component hierarchy for changing an MD5 key on an authenticated BGP peer





Configuring BGP import policy

Configure the border gateway protocol (BGP) import policy to decide if certain labeled routes learned from the EBGP peer are to be ignored or used on the CE' node. If no import policy is provisioned, BGP does not use any routes received from its EBGP peer. If multiple import policies are provisioned, the one with the most specific match applies.

Procedure steps

Step	Action
1	Add BGP import policy. add Rtr/<rtr_name> Bgp Import/<import>
2	Optionally, set the <i>addressFamily</i> (<i>af</i>) attribute to match the labeled EBGP addresses only. By default, the addressFamily is set to all. set Rtr/<rtr_name> Bgp Import/<import> af ipv4Label
3	Set the action to take upon a policy match. set Rtr/<rtr_name> Bgp Import/<import> usage <usage_flag>
4	Add the network component and set the prefix and length attributes to filter routers based on specific network addresses. add Rtr/<rtr_name> Bgp Import/<import> Net/<network> prefix <prefix>, length <length>
5	Specify the AS number of the EBGP peer from which routes are learned. set Rtr/<rtr_name> Bgp Import/<import> peerAs <asNo>
6	Specify the IP address of the EBGP peer from which routes are learned. set Rtr/<rtr_name> Bgp Import/<import> peerIpAddress <addr>
7	Specify the AS that originated the routes learned over the EBGP peer. set Rtr/<rtr_name> Bgp Import/<import> originAs <or_asNo>
8	Specify a regular expression that identifies AS paths from which EBGP accepts route updates if you do not want to use the default value. set Rtr/<rtr_name> Bgp Import/<import> asExpr <path_expr>
9	Specify a regular expression that identifies community paths from which EBGP peer accepts route updates if you do not want to use a default value. set Rtr/<rtr_name> Bgp Import/<import> comExpr <com_expr>



- 10 If you have configured an AS path and community path expression for the import policy, specify a preference for the policy.

```
set Rtr/<rtr_name> Bgp Import/<import> exprPref <pref>
```

When the expression attributes of two import policies match the same AS or community, EBGP uses the preference metric to select a preferred policy. A higher value indicates a higher preference.
- 11 Specify the protocol that originated the routes learned over the EBGP peer.

```
set Rtr/<rtr_name> Bgp Import/<import> originProtocol <protocol>
```
- 12 If required, override the route preference by changing attribute *ebgpRtePref* for BGP external routes.

```
set Rtr/<rtr_name> Bgp Import/<import> ebgpRtePreference <ebgp_override>
```
- 13 Specify the community number that EBGP inserts in the community path attribute for routes that match the criteria of this import policy.

```
set Rtr/<rtr_name> Bgp Import/<import> appCom <com_no>
```

--End--

Variable definitions

Variable	Value
<addr>	is the IP address of the EBGP peer from which the routes are learned. If you set this value to 0.0.0.0, the policy matches any IP address.
<asNo>	specifies the autonomous system number to which the EBGP peer belongs. If you set this value to 0, the policy matches any AS number.
<com_expr>	is a regular expression identifying community paths to match.
<com_no>	is the community number added to the community path attribute.
<ebgp_override>	is the override route preference. Attribute default is <i>sameAsBgp</i> , which means use the value of attribute <i>defaultEbgpRtePref</i> for the route preference. To prefer BGP external routes over OSPF internal routes, the recommended setting for <i>ebgpRtePreference</i> is 6.
<import>	is an instance that describes a BGP import policy.
<length>	is specifying the length of the network <i>prefix</i> attribute.
<network>	is an instance that describes a network address.

(1 of 2)



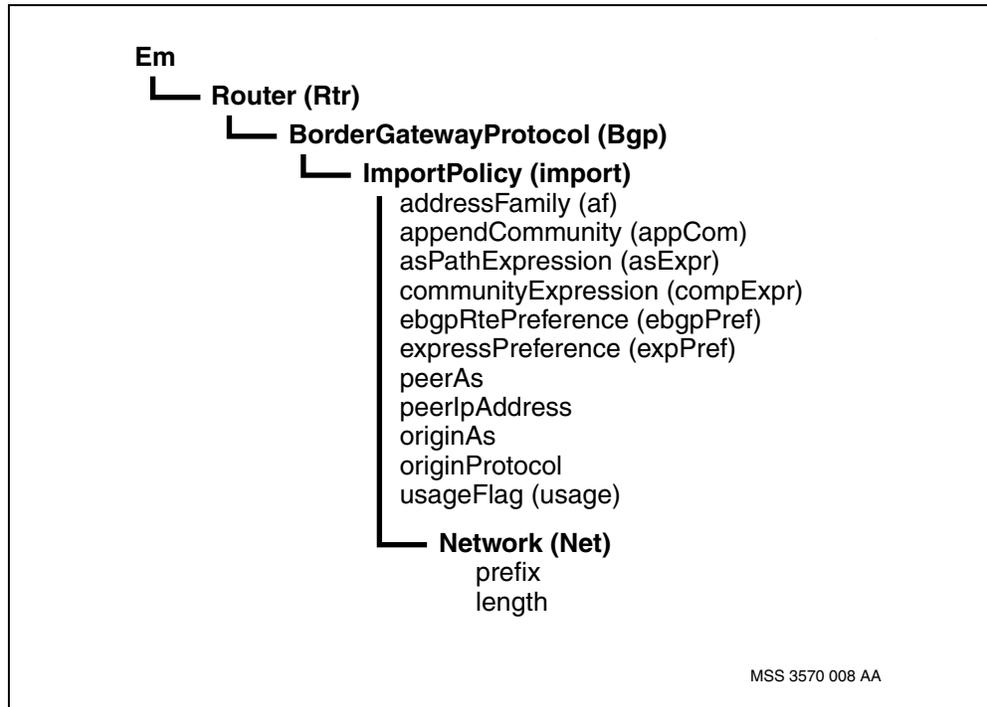
Variable	Value
<or_asNo>	is the number of the AS that originated the learned routes. If you set this value to 0, the policy matches any AS number.
<path_expr>	a regular expression identifying AS paths to match.
<pref>	is the relative preference of a path-based policy.
<prefix>	is specifying the network prefix.
<protocol>	identifies the protocol that originated the routes.
<rtr_name>	is the name of the router.
<usage_flag>	is the action to take on importing routes. To accept labeled routes, set the value of the <i>usageFlag</i> attribute to use. To prevent the use of labeled routes, set the value of the <i>usageFlag</i> attribute to ignore. The default value is use.

(2 of 2)



Procedure job aid

BGP import policy component hierarchy





Configuring BGP and peers for address family ipv4MplsVpn

Configure the interior border gateway protocol (IBGP) or the exterior border gateway protocol (EBGP) for address family ipv4MplsVpn.

Configure the IBGP for the PE or CE' node and add one peer for each remote PE or CE' node respectively in the network. For inter-autonomous systems (inter-ASs), configure the EBGP peers for the PE or CE' node and add one peer for each remote PE or CE' node in the network. Using the BGP protocol, VPN IPv4 routes are distributed between the BGP peers.

Optionally, configure MD5 authentication on a BGP peer connection to provide protection of BGP neighbor relationships. You can change an MD5 key on an authenticated BGP peer using the procedure [Changing an MD5 key on an authenticated BGP peer \(page 21\)](#).

Prerequisites

- If configuring MD5 authentication, use different MD5 key values for each BGP peer. A longer MD5 key will be more difficult to break, however, the longer the key used, the greater the impact on performance. A key length of between 12 and 24 characters should be sufficiently secure without having too great an impact on performance.
- Try to use a key length of between 12 and 24 characters, which should be sufficiently secure without having too great an impact on performance. A longer MD5 key will be more difficult to break, however, the longer the key used, the greater the impact on performance.

Procedure steps

Step	Action
1	Add the <i>Bgp</i> component. add Rtr/<rtr_name> Bgp
2	Set the <i>localAs</i> attribute. set Rtr/<rtr_name> Bgp localAs <local_as_value>
3	Set the <i>bgpIdentifier</i> attribute. set Rtr/<rtr_name> Bgp bgpIdentifier <ip_address>
4	Add the BGP peer. add Rtr/<rtr_name> Bgp Peer/<peer_address> The <i>Descriptor</i> subcomponent is automatically added.
5	Optionally, configure MD5 authentication on a BGP peer connection. Set the MD5 key value under the <i>Descriptor</i> .



```
set Rtr/<rtr_name> Bgp Peer/<ip_addr> Desc md5Key  
<ASCII_string>
```

- 6 Set the *LocalAddressConfigured (lac)* attribute.

```
set Rtr/<rtr_name> Bgp Peer/<peer_address> Desc lac  
<lac_ip_address>
```

- 7 Set the autonomous system identifier for the BGP peer.

```
set Rtr/<rtr_name> Bgp Peer/<peer_address> Desc peerAs  
<peer_as_value>
```

- 8 Set the address family for the node you are configuring.

```
set Rtr/<rtr_name> Bgp Peer/<peer_address> Desc  
addressFamily ipv4MplsVpn
```

--End--

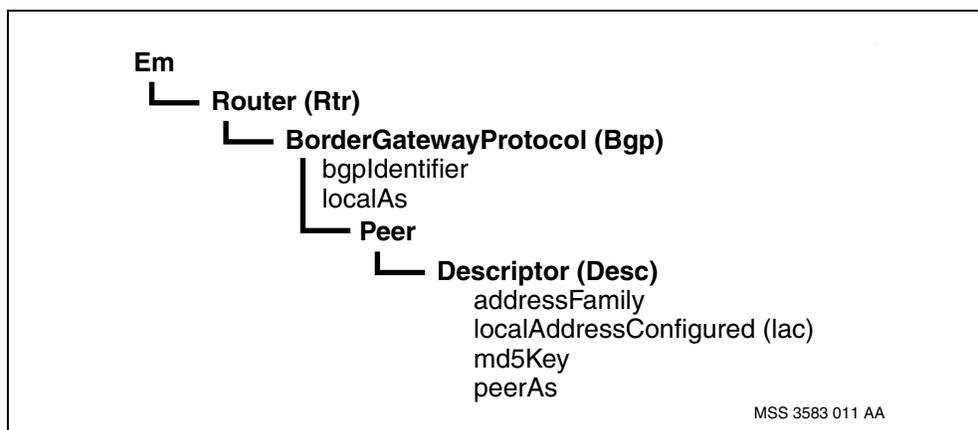


Variable definitions

Variable	Value
<ASCII_string>	is the MD5 key value, 1-255 ASCII characters in length.
<ip_address>	is the IP address that matches the local primary loopback address.
<lac_ip_address>	is the IP address that matches the local primary loopback address.
<local_as_value>	is the value of the autonomous system for the PE or CE' node.
<peer_address>	is the primary loopback address of the peer of the remote PE or CE' node.
<peer_as_value>	is the value of the autonomous system for the remote PE or CE' node. Note that for IBGP, the localAS value and the peerAS value must be the same.
<rtr_name>	is the name of the router.

Procedure job aid

BGP and peers for address family ipv4MplsVpn component hierarchy





Configuring BGP export policy

Optionally, you can configure a border gateway protocol (BGP) export policy on the PE node to either block or send certain routes to its peers. You can decide to filter VPN IPv4 routes based on the values of the network address, the remote peer IP address, and the route target.

Procedure steps

Step	Action
1	<p>By default, BGP advertises all routes in the <i>MplsVpnRibEntry</i> component to its peers. Optionally, you can configure an export policy on the router to either block or send certain routes to its peers. To start configuring the export policy, add the <i>ExportPolicy</i> component.</p> <pre>add -s Rtr/<rtr_name> Bgp Export/<export></pre>
2	<p>Set the <i>RouteTarget</i> attribute to filter routes based on route targets.</p> <pre>set Rtr/<rtr_name> Bgp Export/<export> Rt <route_target></pre> <p>To apply a BGP export policy to a set of IP addresses associated with a VRF, you must set the <i>RouteTarget</i> attribute to include all the route target values that have the <i>mode</i> attribute set to export for that VRF.</p>
3	<p>Set the <i>addressFamily</i> attribute to apply this export policy to VPN IPV4 routes.</p> <pre>set Rtr/<rtr_name> Bgp Export/<export> af ipv4MplsVpn</pre>
4	<p>Add the <i>Network</i> component and set the <i>prefix</i> and <i>length</i> attributes to filter routes based on specific network addresses.</p> <pre>add Rtr/<rtr_name> Bgp Export/<export> Net/<network> prefix <prefix>, length <length></pre>
5	<p>Set the <i>advertiseStatus</i> attribute to specify the action to take on a matched policy.</p> <pre>set Rtr/<rtr_name> Bgp Export/<export> advertise <advertise></pre>
6	<p>Set the <i>peerIpAddress</i> attribute to specify the peer that this policy applies to.</p> <pre>set Rtr/<rtr_name> Bgp Export/<export> peerIpAddress <peer_ip_address></pre>
7	<p>Repeat this procedure for all the PE nodes and Route Reflectors with which this PE node will peer.</p>

--End--

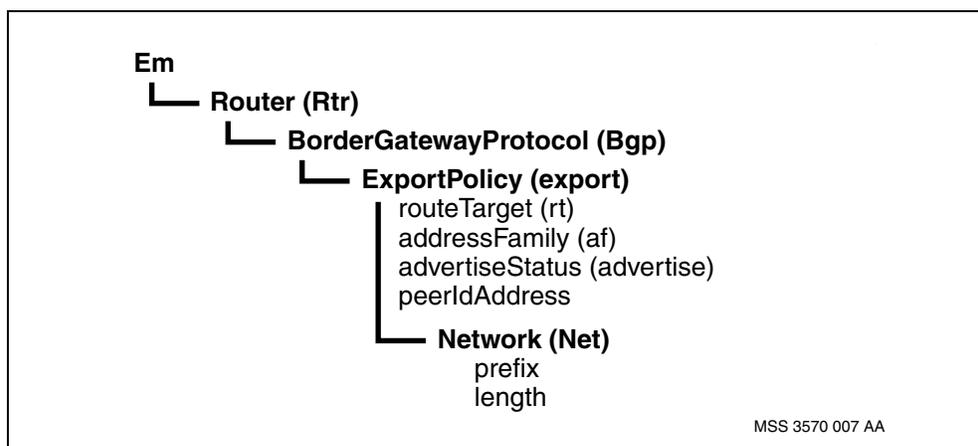


Variable definitions

Variable	Value
<advertise>	is the advertise status for exporting routes. The status is block or send. The default is send.
<export>	is an instance that describes a BGP export policy.
<length>	is specifying the length of the network <i>prefix</i> attribute.
<network>	is an instance that describes a network address.
<peer_ip_address>	is specifying the IP address of the peer that the routes are advertised to.
<prefix>	is specifying the network prefix. The length of the network prefix is determined by the <i>length</i> attribute under the same <i>Network</i> component.
<route_target>	is specifying a list of routes for which the export policy applies to.
<rtr_name>	is the name of the router.

Procedure job aid

BGP export policy component hierarchy





Media configuration

The media configuration is used to encapsulate forwarded IP packets into the underlying layer 2 specific media interface (for example, an Ethernet frame).

Prerequisites to media configuration

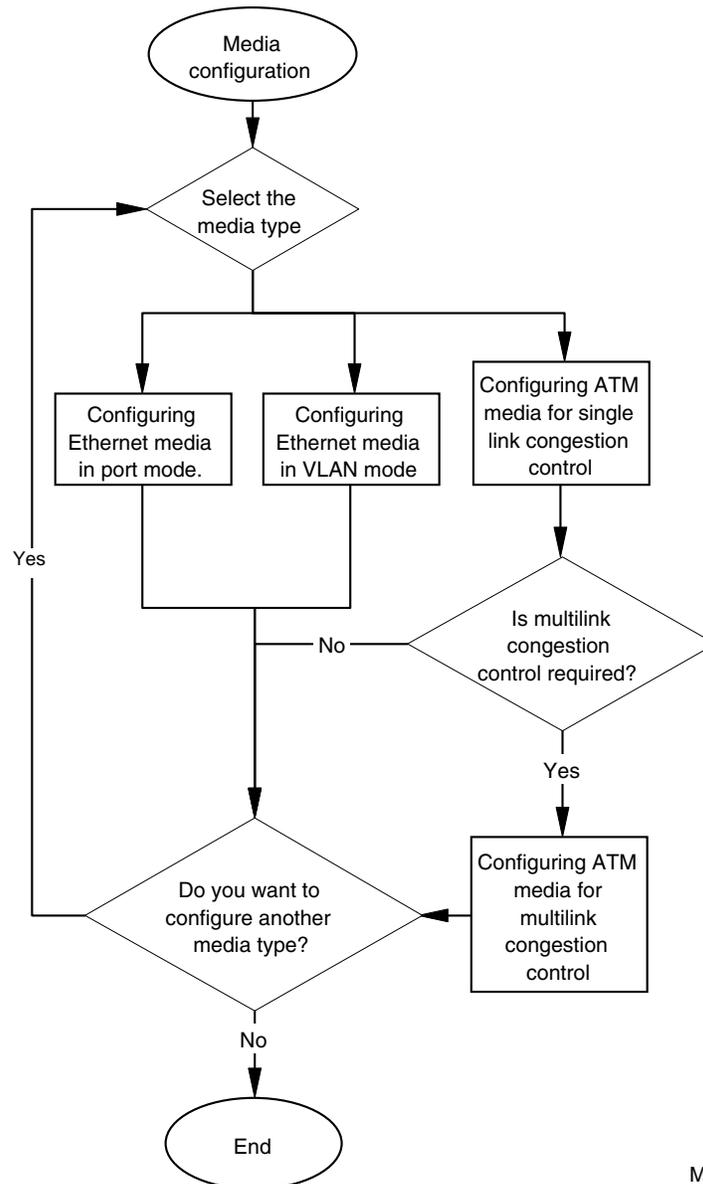
- Determine the media type prior to configuring software features. The decision you make to use ATM, or GigE media, affects the steps you take to configure the BGS/MPLS VPN.

Media configuration procedures

This task flow shows you the sequence of procedures you perform to configure media. To link to any procedure, go to [Media configuration procedure navigation \(page 33\)](#).



Media configuration procedures



MSS 4004 003 AA

Media configuration procedure navigation

- [Configuring Ethernet media in port mode \(page 34\)](#)
- [Configuring Ethernet media in VLAN mode \(page 36\)](#)
- [Configuring ATM media for single link congestion control \(page 38\)](#)
- [Configuring ATM media for multi link congestion control \(page 40\)](#)



Configuring Ethernet media in port mode

Configure Ethernet media in port mode to define logical connectivity for BGP/MPLS VPN tunnels. These links use LDP-DU to signal MPLS LSPs. Packets transmitted on the LSPs will be differentiated by multiple levels of drop precedence and scheduling class.

Prerequisites

- You must configure an Ethernet interface in port mode. For more information, see NN10600-821 *Nortel Multiservice Switch 7400/15000/20000 Operations: Ethernet Services*.

Procedure steps

Step	Action
1	Add the <i>EnetApplication</i> component. add Rtr/<rtr_name> Interface/<ip_address> Enet
2	Link to the LanApplication. set Rtr/<rtr_name> Interface/<ip_address> Enet linkToEnetIf La/<la_name>
3	Set the maximum frame size for the Router on the Ethernet interface. set Lp/<lp_id> Ethernet/<eth> maxFrameSize <maxFrameSize>

--End--

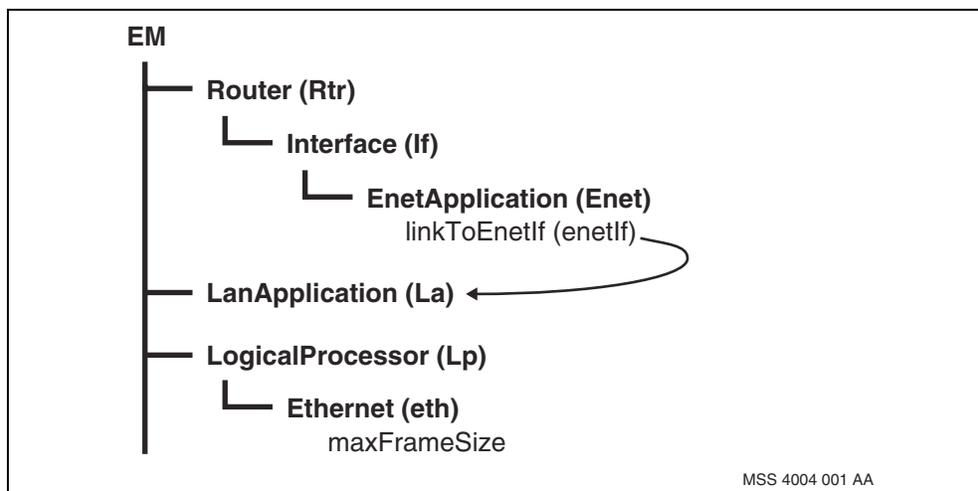


Variable definitions

Variable	Value
<eth>	is the instance number of an Ethernet port corresponding to a physical port a card.
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived.
<la_name>	is the identifier assigned to the LanApplication.
<lp_id>	is the identifier assigned to the Ethernet LP.
<maxFrameSize>	is a value between 1519 and 1600 bytes. The default value is 1518 bytes for standard Ethernet frames. A value greater than the default, up to 1600 bytes, supports jumbo frames.
<rtr_name>	is the name of the router.

Procedure job aid

Ethernet media in port mode component hierarchy





Configuring Ethernet media in VLAN mode

Configure Ethernet media in Virtual Lan (VLAN) mode to define logical connectivity for BGP/MPLS VPN tunnels. These links use LDP-DU to signal MPLS LSPs. Packets transmitted on the LSPs will be differentiated by multiple levels of drop precedence and scheduling class.

Prerequisites

- You must configure an Ethernet interface in VLAN mode. For more information, see NN10600-821 *Nortel Multiservice Switch 7400/15000/20000 Operations: Ethernet Services*.

Procedure steps

Step	Action
1	Add the <i>EnetApplication</i> component. <code>add Rtr/<rtr_name> Interface/<ip_address> Enet</code>
2	Link to the LanApplication. <code>set Rtr/<rtr_name> Interface/<ip_address> Enet linkToEnetIf La/<la_name> vlan/<vlan_name></code>
3	Set the maximum frame size for the Router on the Ethernet interface. <code>set Lp/<lp_id> Ethernet/<eth> maxFrameSize <maxFrameSize></code>

--End--

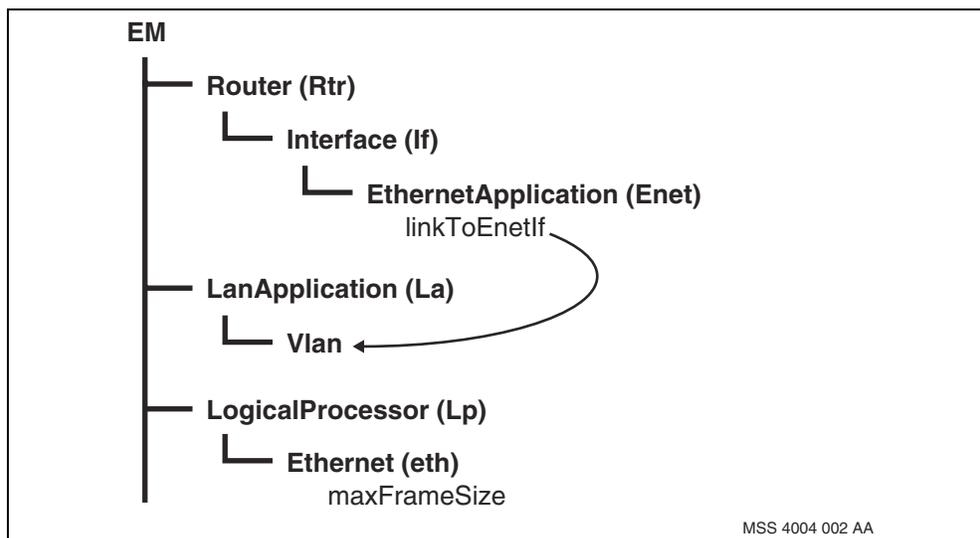


Variable definitions

Variable	Value
<eth>	is the instance number of an Ethernet port corresponding to a physical port a card.
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived.
<la_name>	is the identifier assigned to the LanApplication.
<lp_id>	is the identifier assigned to the Ethernet LP.
<maxFrameSize>	is a value between 1519 and 1600 bytes. The default value is 1518 bytes for standard Ethernet frames. A value greater than the default, up to 1600 bytes, supports jumbo frames.
<rtr_name>	is the name of the router.
<vlan_name>	is the identifier assigned to the VLAN.

Procedure job aid

Ethernet media in Vlan mode component hierarchy





Configuring ATM media for single link congestion control

Configure ATM media for single link congestion control to define physical connectivity for BGP/MPLS VPN tunnels. These links use LDP-DU to signal MPLS LSPs. Packets transmitted on the LSPs will be differentiated by multiple levels of drop precedence.

Prerequisites

- For more information on *AtmIf* component configuration, see NN10600-710 *Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*

Procedure steps

Step	Action
1	Set the LPT feature list to include the ATM card feature set. <pre>set Sw Lpt/<lpt_name> featureList atmmppe</pre>
2	Activate changes. See Activating configuration changes (page 161) .
3	Add <i>ATMMPE</i> media set to use LLC encapsulation. This is the default setting. <pre>add -s Rtr/<rtr_name> Interface/<ip_address> AtmMpe</pre>
4	Set the <i>netmask</i> attribute. <pre>set Rtr/<rtr_name> Interface/<ip_address> netmask <ip_mask></pre>
5	Add the Nailed Up Endpoint <pre>add -s AtmIf/<atmif_id> Vcc/<vpi.vci> nep</pre>
6	Link the <i>AtmConnection</i> subcomponent, which is added automatically with DiffServ connection class 0 when the <i>atmMpe</i> component is created, to an ATM VCC that is configured with the ATM UBR service category. <pre>set Rtr/<rtr_name> Interface/<ip_address> AtmMpe Ac/<ac_id> AtmConnection AtmIf/<atmif_id> Vcc/<vpi.vci> Nep set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm atmServiceCategory ubr</pre>
7	Enable packet-wise discard. <pre>set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard enabled</pre>

--End--

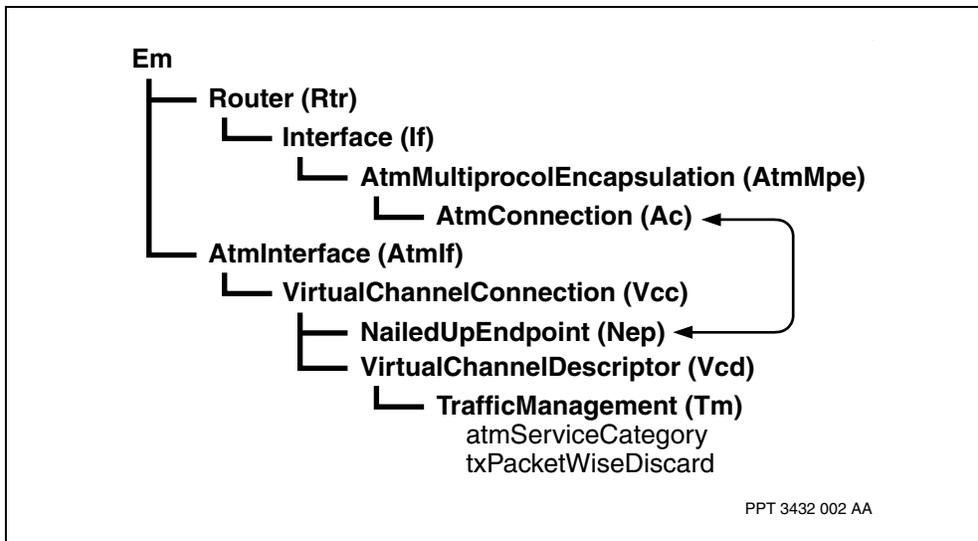


Variable definitions

Variable	Value
<ac_id>	is the instance value of the atm connections. Any mnemonic (for example, AC/1).
<atmif_id>	is the instance value of the <i>AtmIf</i> component.
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived.
<ip_mask>	is the netmask of the IP address. This value cannot be 32 bits for an interface.
<rtr_name>	is the name of the router.
<vpi.vci>	is the identifier assigned to the VP and VC of the virtual channel.

Procedure job aid

ATM media for single link congestion control component hierarchy





Configuring ATM media for multi link congestion control

Configuring ATM media for multi link congestion control allows packets transmitted on the LSPs to be differentiated by multiple levels of drop precedence and by the multi link congestion control configuration of the ATM links.

At least one ATM connection must be created. Nortel Multiservice Switch systems support up to four ATM connections between hops in IP and MPLS networks. This provides four unique emission priorities when transmitting from the Multiservice Switch to the next node, and allows for individual service differentiation on separate links in the ATM network. To enable this capability, up to three more ATM connections may be added, one for each of the four DiffServ connection class values. For more information on differentiated service, see NN10600-809 *Nortel Multiservice Switch 7400/15000/20000 Layer 3 Traffic Management Configuration*.

Prerequisites

- For more information on *AtmIf* component configuration, see NN10600-710 *Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*

Procedure steps

Step	Action
1	Configure the COS value. <pre>set Rtr/<rtr_name> Interface/<ip_address> AtmMpe Ac/ <ac_id> IpCos/<ipcos_value></pre>
2	Add an ATM connection with DiffServ connection class 1 and link it to an ATM VCC that has an ATM nrtVBR service category. <pre>set Rtr/<rtr_name> Interface/<ip_address> AtmMpe Ac/ <ac_id> AtmConnection AtmIf/<atmif_id> Vcc/<vpi.vci> Nep set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd tm atmServiceCategory nrtvbr</pre>
3	Set the traffic management parameter of the ATM connection. This parameter is used to derive the OSPF metric value for this interface. <pre>set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm txTrafficDescType <desc_type> set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm txTrafficDescParm 1 <desc_parm></pre>
4	Enable packet-wise discard. <pre>set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard enabled</pre>



- 5 Add an ATM connection with DiffServ connection class 2 and link it to an ATM VCC that has an ATM rtVBR service category.
- ```
set Rtr/<rtr_name> Interface/<ip_address> AtmMpe Ac/
<ac_id> AtmConnection AtmIf/<atmif_id> Vcc/<vpi.vci> Nep
set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm
atmServiceCategory rtvbr
```
- 6 Enable packet-wise discard.
- ```
set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm  
txPacketWiseDiscard enabled
```
- 7 Add an ATM connection with DiffServ connection class 3 and link it to an ATM VCC that has an ATM CBR service category.
- ```
set Rtr/<rtr_name> Interface/<ip_address> AtmMpe Ac/
<ac_id> AtmConnection AtmIf/<atmif_id> Vcc/<vpi.vci> Nep
set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm
atmServiceCategory cbr
```
- 8 Enable packet-wise discard.
- ```
set AtmIf/<atmif_id> Vcc/<vpi.vci> Vcd Tm  
txPacketWiseDiscard enabled
```

--End--

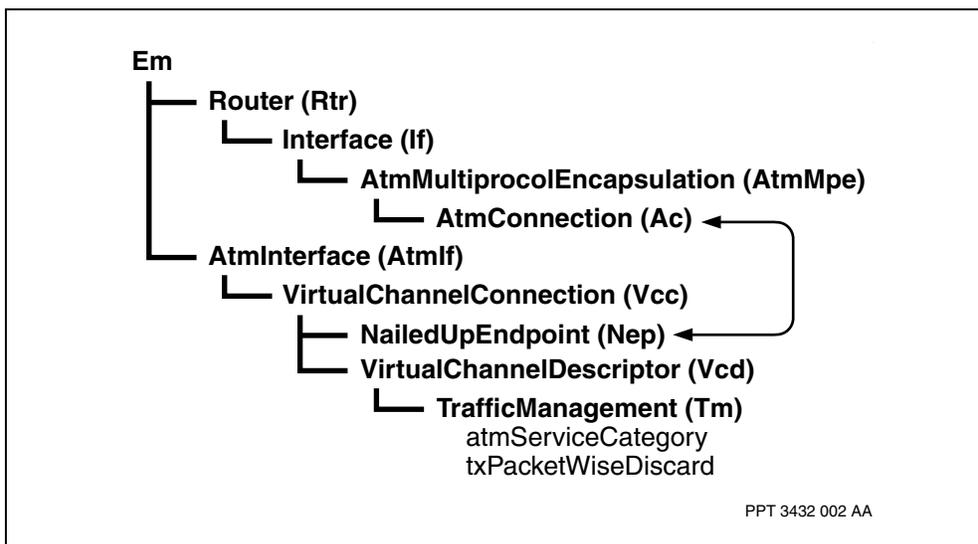


Variable definitions

Variable	Value
<ac_id>	is the instance value of the atm connection. Any mnemonic (for example, AC/1).
<atmif_id>	is the instance value of the <i>AtmIf</i> component.
<desc_parm>	is the vector of five traffic parameters whose meanings are defined by the <i>txTrafficDescType</i> attribute. The instance value is the peak cell rate (PCR) setting in cell/second.
<desc_type>	is the instance value specifies the type of traffic management which is applied to the transmit direction of this connection. Values: 3 to 8.
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived.
<ip_mask>	is the IP address of the netmask.
<ipcos_value>	is the value assigned to the COS. It is recommended that the IP COS values 0, 1, 2, 3 correlate directly with ATM service categories UBR, nrtVBR, rtVBR, CBR.
<rtr_name>	is the name of the router.
<vpi.vci>	is the identifier assigned to the VP and VC of the virtual channel.

Procedure job aid

ATM media for multi link congestion control component hierarchy





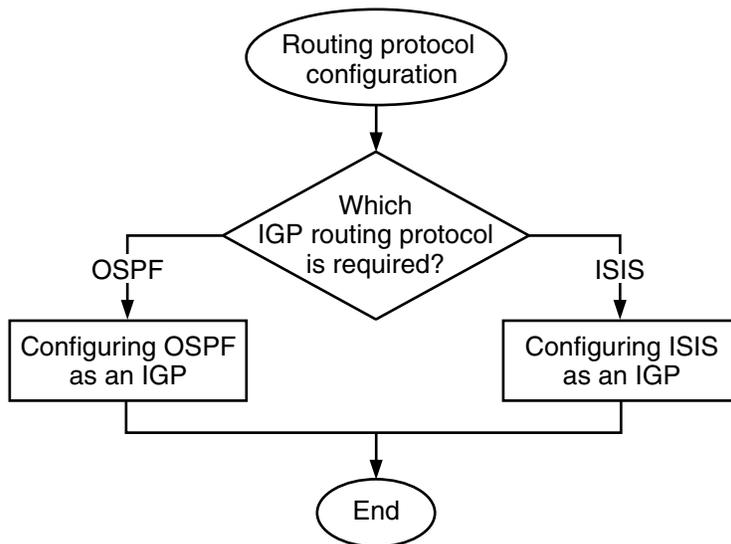
Routing protocol configuration

The routing protocol configuration is used to set up IP address reachability information to allow for a source IP host to direct traffic to a destination IP host.

Routing protocol configuration procedures

This task flow shows you the sequence of procedures you perform to configure a routing protocol. To link to any procedure, go to [Routing protocol configuration procedure navigation \(page 43\)](#).

Routing protocol configuration procedures



MSS 3541 004 AA

Routing protocol configuration procedure navigation

- [Configuring OSPF as an IGP \(page 44\)](#)
- [Configuring ISIS as an IGP \(page 46\)](#)



Configuring OSPF as an IGP

Configure Open Shortest Path First (OSPF) as the Interior Gateway Protocol (IGP) and configure a passive OSPF interface on the primary loopback interface so that the loopback address is visible to the IGP running in the backbone.

Prerequisites

- Identify the primaryLoopback IP address. For more information, see [Configuring the router and primary loopback \(page 14\)](#).

Procedure steps

Step	Action
1	Add the <i>OSPF</i> component and set the <i>AreaEntry</i> component. <code>add -s Rtr/<rtr_name> Ospf AreaEntry/<area_id></code>
2	Set the OSPF routerId to match the primaryLoopback address. <code>set Rtr/<rtr_name> Ospf routerId <ip_address></code>
3	Add the OSPF interface under the primaryLoopback interface and set the type to passive. <code>add -s Rtr/<rtr_name> Interface/<ip_address> Ospfif ifType passive</code>
4	Add OSPF on other interfaces, for other media types (ATM or GigE). The OSPF is added on other interfaces to be able to reach the loopback interface. <code>add -s Rtr/<rtr_name> Interface/<ip_address> Ospfif ifType <interface_type></code>

--End--

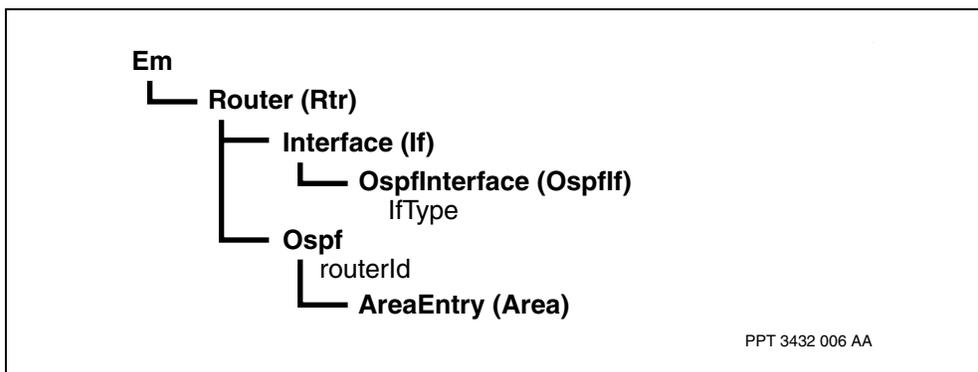


Variable definitions

Variable	Value
<area_id>	is a 32-bit address that contains the information about various areas that the router is connected to. This address uses the dotted decimal notation of an IP address, however it is not an IP address. The backbone area is always set to 0.0.0.0.
<interface_type>	is the type of this OSPF interface (pointToPoint, broadcast, etc.).
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived.
<rtr_name>	is the name of the router.

Procedure job aid

OSPF as an IGP component hierarchy





Configuring ISIS as an IGP

Configure the Intermediate System to Intermediate System (ISIS) as the Interior Gateway Protocol (IGP) running in the backbone and configure a passive ISIS interface on the primary loopback interface so that the loopback address is visible to the IGP running in the backbone.

Procedure steps

Step	Action
1	Add the <i>ISIS</i> protocol under the Router. add Rtr/<rtr_name> Isis
2	Add the <i>Network Entity Title (Net)</i> component. add Rtr/<rtr_name> Isis Net/<net_instance>
3	Add the <i>IsisLevel</i> component. add Rtr/<rtr_name> Isis IsisLevel/<level> Once ISIS is added at the router level, an ISIS interface must be added for each interface on which you want to use ISIS as an IGP.
4	Add the <i>IsisInterface</i> component. add -s Rtr/<rtr_name> Interface/<ip_address> IsisIf Once an instance of the <i>IsisInterface</i> component is added, at least one <i>Level</i> subcomponent must be added.
5	Add the <i>IsisIf Level</i> component. add -s Rtr/<rtr_name> Interface/<ip_address> IsisIf Level/<if_level>
6	Set the <i>IsisIf</i> component to passive mode for the primaryLoopback interface to make it visible to the IGP. set Rtr/<rtr_name> If/<ip_address> IsisIf passive yes

--End--

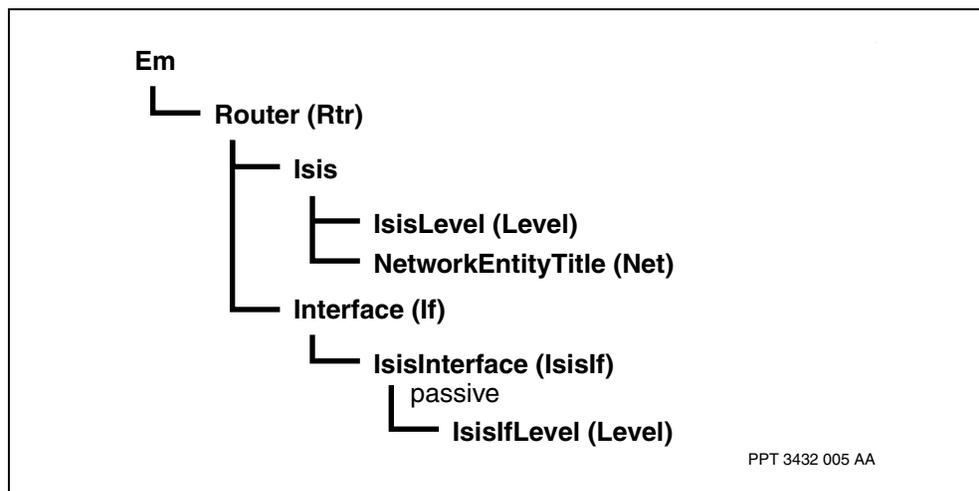


Variable definitions

Variable	Value
<if_level>	represents the ISIS Level functionality that is associated with a single logical port. Level/1 only is supported.
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived.
<level>	represents the ISIS protocol level specific capability under the router ISIS component. Level/1 only is supported
<net_instance>	is the value assigned to the <i>NetworkEntityTitle</i> component that identifies the ISIS router. The <i>NetworkEntityTitle</i> component consists of three parts: Area Address, System Identifier, and Network Selector (NSEL). Multiservice Switch systems support up to 3 NETs. On a router, all provisioned NETs must have the same System Identifier.
<rtr_name>	is the name of the router.

Procedure job aid

ISIS as an IGP component hierarchy





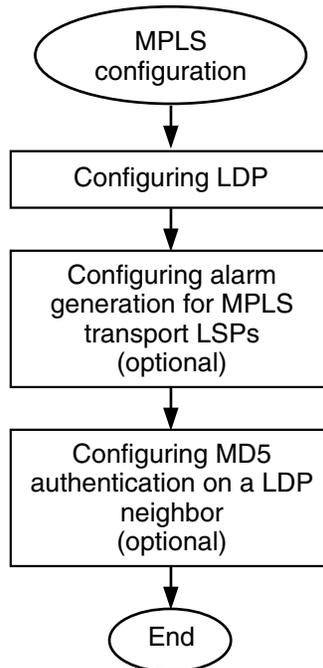
MPLS configuration

The label distribution protocol (LDP) configuration is used to trigger the exchange of MPLS labels for all the neighbor nodes.

MPLS configuration procedures

This task flow shows you the sequence of procedures you perform to configure the MPLS-related components. To link to any procedure, go to [MPLS configuration procedure navigation \(page 48\)](#).

MPLS configuration procedures



MSS 3541 003 AA

MPLS configuration procedure navigation

- [Configuring LDP \(page 50\)](#)



- [Configuring alarm generation for MPLS transport LSPs \(page 52\)](#)
- [Configuring MD5 Authentication on an LDP neighbor \(page 53\)](#). This is an optional procedure that is done on an installed system, and is not part of initial system configuration.



Configuring LDP

Configure the Label Distribution Protocol (LDP) on the node to trigger the exchange of MPLS labels for all the neighbor nodes. This enables label switching of VPN traffic through tandem nodes in the backbone network.

Procedure steps

Step	Action
1	Add MPLS LDP. add Rtr/<rtr_name> Ldp
2	Optionally, configure the LSR capability for the LDP component. set Rtr/<rtr_name> Ldp lsrCapability <lsr_capability>
3	Add an LDP interface on each interface that defines the adjacency. The interface can be ATM or Gigabit Ethernet, and is not required under any loopback interface. add Rtr/<rtr_name> If/<ip_address> LdpIf

--End--

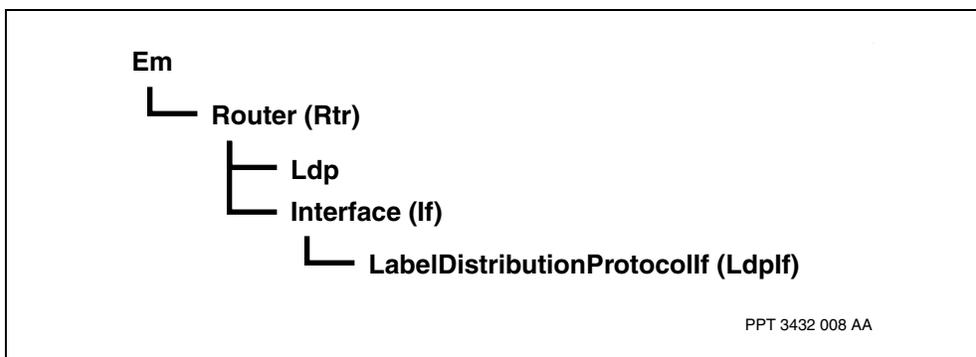


Variable definitions

Variable	Value
<ip_address>	is a 32-bit address assigned to the interface from which the routing information is derived. Each LDP interface is created on the same interface as the corresponding OSPF or ISIS interface.
<lsr_capability>	is the value that determines whether the switch has only Label Edge Router (LER) capabilities, or both LER and tandeming Label Switch Router (LSR) capabilities. For LER and LSR use <i>lerLsr</i> , for LER only, use <i>lerOnly</i> . By default, the value is <i>lerOnly</i> on a Multiservice Switch 7400, and <i>lerLsr</i> on a Multiservice Switch 15000 or Multiservice Switch 20000.
<rtr_name>	is the name of the router.

Procedure job aid

LDP component hierarchy





Configuring alarm generation for MPLS transport LSPs

Optionally, configure the MPLS component on the node to provide the capability of generating an alarm when an MPLS transport LSP is unavailable for one or more BGP next hops. This is an indication that there is no BGP/MPLS VPN datapath from the node that has generated the alarm to one or more BGP next hops. The alarm is cleared when all BGP next hops are again reachable by an MPLS transport LSP.

Procedure steps

Step	Action
1	Add MPLS. <code>add Rtr/<rtr_name> Mpls</code>
--End--	

Variable definitions

Variable	Value
<rtr_name>	is the name of the router.

Procedure job aid

Mpls transport LSPs component hierarchy





Configuring MD5 Authentication on an LDP neighbor

Configure MD5 authentication on an LDP neighbor to provide protection of neighbor relationships.

To change an MD5 key on an authenticated LDP neighbor, use the procedure [Changing an MD5 key on an authenticated LDP session \(page 55\)](#).

If an LDP MD5 Authentication alarm is raised, the operator can isolate the source of the issue using the Neighbor operational attributes described in [LDP neighbor operational attributes \(page 57\)](#).

Prerequisites

- A different MD5 key value is used for each LDP neighbor. A longer MD5 key is more difficult to break, however, the longer the key used, the greater the impact on performance. A key length of between 12 and 24 characters should be sufficiently secure without having too great an impact on performance

Procedure steps

Step	Action
1	Add the LDP neighbor. <code>add Rtr/<rtr_name> Ldp Nbr/<ip_addr>, <LabelSpaceId></code> For provisioned LDP neighbors, the <i>LabelSpaceId</i> must be 0 (zero). The <i>Descriptor</i> subcomponent is automatically created.
2	Set the MD5 key under the <i>Descriptor</i> component. <code>set Rtr/<rtr_name> Ldp Nbr/<ip_addr>, <LabelSpaceId> Desc md5Key <ASCII_string></code>

--End--

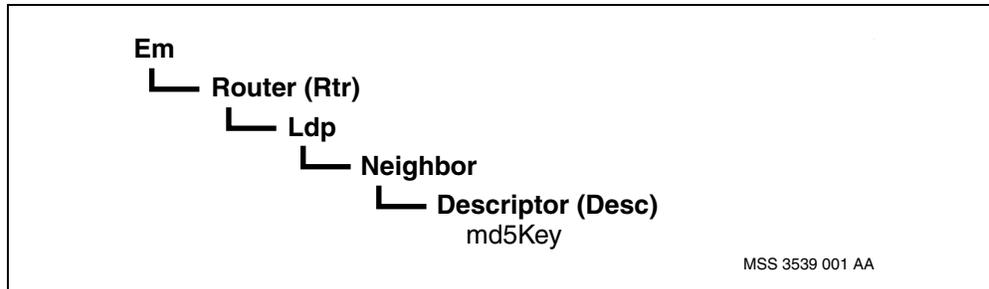


Variable definitions

Variable	Value
<ASCII_string>	is the MD5 key value, 0-69 ASCII characters. A null string indicates that MD5 authentication is not to be used on the connection to this neighbor. Any printable ascii character is allowed. If a space is used within the key, then the whole key must be included in quotes. For this reason a " character is the only printable ascii character not allowed as part of a key.
<ip_addr>	is the IP address.
<LabelSpaceId>	is the value for the LabelSpaceId element, value 0-65535. For provisioned LDP neighbors, the LabelSpaceId must be 0 (zero).
<rtr_name>	is the name of the router.

Procedure job aid

LDP component hierarchy for MD5 authentication on an LDP neighbor





Changing an MD5 key on an authenticated LDP session

Transition MD5 keys without having to terminate the LDP neighbor session for which the key is being changed.

Use a different MD5 key value be used for each LDP neighbor.

When changing keys on a LDP session between a Multiservice Switch node and a non-Multiservice Switch, change the key on the Multiservice Switch node, to minimize the outage time.

A longer MD5 key will be more difficult to break, however, the longer the key used, the greater the impact on performance. A key length of between 12 and 24 characters should be sufficiently secure without having too great an impact on performance.

Procedure steps

Step	Action
1	Set the <i>keyTransitionDelay</i> attribute on the local router to a value (in minutes) sufficient to complete the changes at both ends of the connection. <code>set Rtr/<rtr_name> Ldp Nbr/<ip_addr>, <LabelSpaceId> Desc keyTransitionDelay <n></code>
2	Set the <i>keyTransitionDelay</i> attribute on the remote end. <code>set Rtr/<rtr_name> Ldp Nbr/<ip_addr>, <LabelSpaceId> Desc keyTransitionDelay <n></code>
3	Set the new MD5 key value on the local router. <code>set Rtr/<rtr_name> Ldp Nbr/<ip_addr>, <LabelSpaceId> Desc md5Key <ASCII_string></code>
4	Set the new MD5 key value on the remote router, if the remote router is also a Multiservice Switch. <code>set Rtr/<rtr_name> Ldp Nbr/<ip_addr>, <LabelSpaceId> Desc md5Key <ASCII_string></code>

--End--

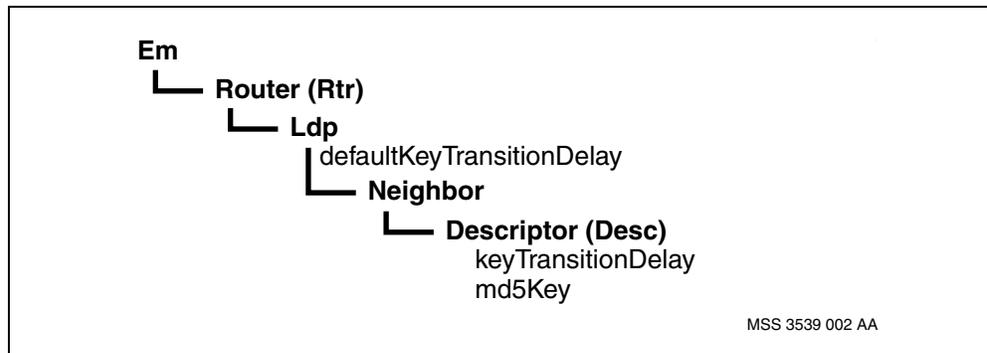


Variable definitions

Variable	Value
<ASCII_string>	is the MD5 key value, 0-69 ASCII characters.
<ip_addr>	is the IP address.
<LabelSpaceId>	is the value for the LabelSpaceId element, value 0-65535. For provisioned LDP neighbors, the LabelSpaceId must be 0 (zero).
<n>	is the value for the <i>keyTransitionDelay</i> . This is the time that can elapse before the local router transitions to using the new key for transmission (the new key value is immediately accepted for reception). This delay equates to the amount of time the operator has to provision both the local and remote ends with the new key, without losing service. The value can be inherited from the <i>Ldp</i> component's <i>keyTransitionDelay</i> attribute by setting the value to <i>sameAsLdp</i> . Range: <i>sameAsLdp</i> , 1 to 65535 (minutes), the default is <i>sameAsLdp</i> .
<rtr_name>	is the name of the router.

Procedure job aid

LDP component hierarchy for changing an MD5 key on an authenticated LDP session





LDP neighbor operational attributes

Attribute	Description
authenticationType	is the attribute that indicates which type of authentication is used on the TCP connection to the specified Neighbor. Values are none and md5.
badAuthenticationPkts	is the attribute that indicates the number of TCP packets have been received from the specified Neighbor which were authenticated incorrectly. When this counter is increasing could mean that the Neighbor is configured with a different key or a hacker is attempting disrupt the LDP connection and is injecting packets authenticated using a different key.
noAuthenticationPkts	is the attribute that indicates the number of TCP packets have been received from the specified Neighbor which were unauthenticated when authentication was expected. When this counter is increasing it could mean that the Neighbor is not configured to use authentication or a hacker is attempting to disrupt the LDP connection and is injecting unauthenticated packets.
unexpectedAuthenticationPkts	is the attribute that indicates the number of TCP packets have been received from the specified Neighbor which were authenticated when authentication was not expected. When this counter is increasing it could mean that the Neighbor is configured to use authentication or a hacker is attempting to disrupt the LDP connection and is injecting authenticated packets.



VRF and access configuration

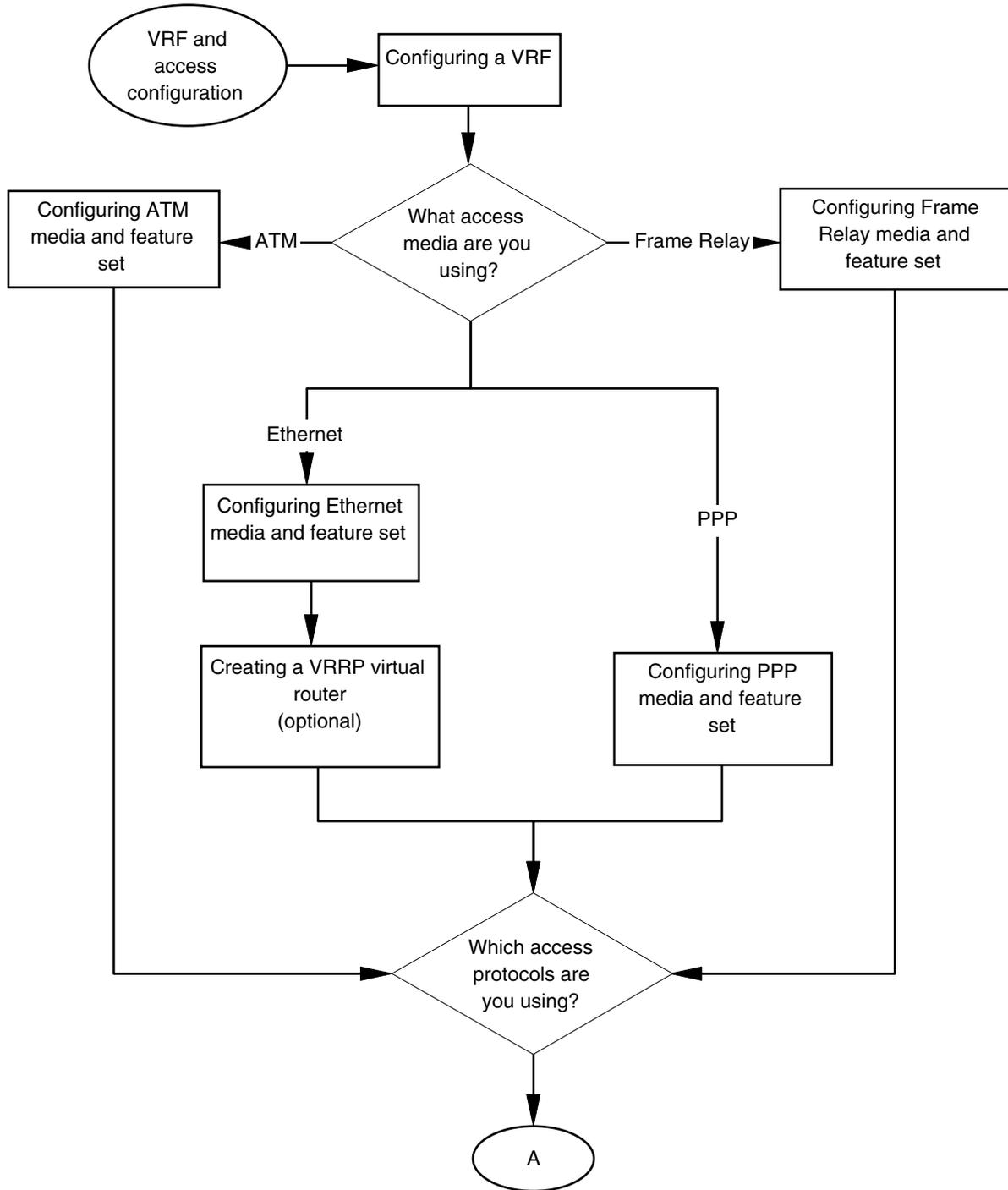
Configure VPN route forwarders (VRFs) and access interfaces on the node. The VRF is the entity that groups together the routing information learned from several connected sites. A local site can belong to one or more VPNs.

VRF and access configuration procedures

This task flow shows you the sequence of procedures you perform to configure the VRF and the access on the node. To link to any procedure, go to [VRF and access configuration procedure navigation \(page 61\)](#).



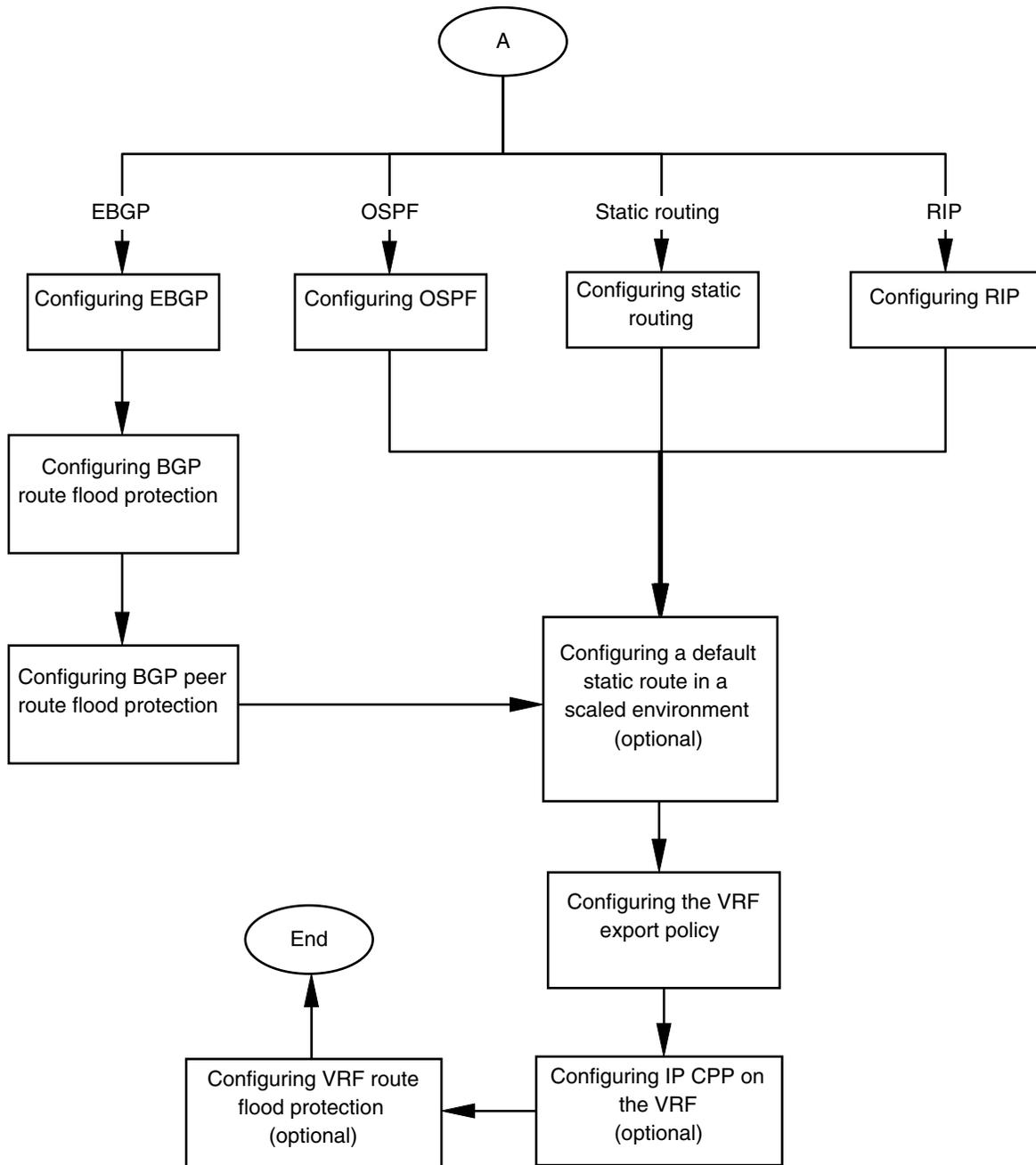
VRF and access configuration procedures



MSS 3541 006 AB



VRF and access configuration procedures (continued)



MSS 4002 033 AA



VRF and access configuration procedure navigation

- [Configuring a VRF \(page 62\)](#)
- [Configuring ATM media and feature set \(page 67\)](#)
- [Configuring PPP media and feature set for VRF in RFC2547 mode \(page 70\)](#)
- [Configuring Ethernet media and feature set \(page 72\)](#)
- [Creating a VRRP virtual router \(page 74\)](#)
- [Configuring frame relay media and feature set \(page 82\)](#)
- [Configuring EBGp \(page 85\)](#)
- [Configuring BGP route flood protection \(page 90\)](#)
- [Configuring BGP peer route flood protection \(page 92\)](#)
- [Configuring OSPF \(page 94\)](#)
- [Configuring static routing \(page 96\)](#)
- [Configuring RIP \(page 97\)](#)
- [Configuring a default static route in a scaled environment \(page 99\)](#)
- [Configuring the VRF export policy \(page 101\)](#)
- [Configuring IP CPP on the VRF \(page 104\)](#)
- [Configuring VRF route flood protection \(page 106\)](#)



Configuring a VRF

Configuring a VPN route forwarder (VRF), with its own unique route distinguisher, allows two different VPNs, with no site in common, to use IPv4 address spaces that overlap with each other. Configuring route targets under the *Vrf* component defines VPN memberships for local sites connected into the PE node, so that two or more customer sites can communicate. In Nortel Multiservice Switch systems, the VRF associates all routes that lead to a particular site with one or more target VPNs.

Procedure steps

Step	Action
1	Add a <i>VpnRouteForwarder</i> component. <code>add Rtr/<rtr_name> Vrf/<vrf_name></code>
2	Add the VRF's applicable Route Distinguisher. <code>add Rtr/<rtr_name> Vrf/<vrf_name> Rd/<rd_value></code>
3	Add the <i>RouteTarget</i> component. <code>add Rtr/<rtr_name> Vrf/<vrf_name> Rt/<rt_value></code>
4	Set the <i>mode</i> attribute for the <i>RouteTarget</i> component. <code>set Rtr/<rtr_name> Vrf/<vrf_name> Rt/<rt_value> mode <mode></code>
5	Specify the route preference for routes received from another VRF from a remote PE node, if you do not want to use the default value. <code>set Rtr/<rtr_name> Vrf/<vrf_name> defaultRemoteBgpMplsIRtePref <route_pref></code>
6	Specify the route preference for routes received from another VRF from the same PE node, if you do not want to use the default value. <code>set Rtr/<rtr_name> Vrf/<vrf_name> defaultLocalBgpMplsIRtePref <route_pref></code>
7	Increase the <i>importRoutesDiscardLimit</i> , if you do not want to use the default value.

Attention: The default *importRoutesDiscardLimit* value of 3000 routes can quickly be exceeded on Import Spoke and Export Hub VRFs, which results in routes being discarded and ultimately traffic loss. It is highly recommended that this value be provisioned to the maximum allowed value for the Import Spoke and Export Hub VRFs.

```
set Rtr/<rtr_name> Vrf/<vrf_name>
importRoutesDiscardLimit <discard_limit>
```



- 8 If you have increased `importRoutesDiscardLimit`, increase the corresponding `importRoutesAlarmLimit`.

Attention: The value chosen for `importRoutesDiscardLimit` must be greater than the `importRoutesAlarmLimit` value in order for CHECK PROV to pass.

```
set Rtr/<rtr_name> Vrf/<vrf_name>
importRoutesAlarmLimit <alarm_limit>
```

- 9 Increase the `exportRoutesDiscardLimit`, if you do not want to use the default value.

Attention: The default `exportRoutesDiscardLimit` value of 500 routes can quickly be exceeded on Import Spoke and Export Hub VRFs, which results in routes being discarded and ultimately traffic loss. It is highly recommended that this value be provisioned to the maximum allowed value for the Import Spoke and Export Hub VRFs.

```
set Rtr/<rtr_name> Vrf/<vrf_name>
exportRoutesDiscardLimit <discard_limit>
```

- 10 If you have increased `exportRoutesDiscardLimit`, increase the corresponding `exportRoutesAlarmLimit`.

Attention: The value chosen for `exportRoutesDiscardLimit` must be greater than the `exportRoutesAlarmLimit` value in order for CHECK PROV to pass.

```
set Rtr/<rtr_name> Vrf/<vrf_name>
exportRoutesAlarmLimit <alarm_limit>
```

- 11 If you have increased the `importRoutesDiscardLimit` and `exportRoutesDiscardLimit` values, you must also increase the `ipRoutesPoolCapacity` for the FPs on which the VRFs reside (PQC-based FPs only). Add the `FrameCoreResourceControl` (Fcr) and `Pqc` subcomponents to the LP (this will automatically add the `Ov` subcomponent under `Pqc`).

```
add -s Lp/<lp_number> Eng Fcr Pqc
```

- 12 Increase the `ipRoutesPoolCapacity` value to accommodate the higher `discardLimit` values.

Attention: The default `ipRoutesPoolCapacity` value of 4096 routes will quickly be exceeded if the `importRoutesDiscardLimit` and `exportRoutesDiscardLimit` values are increased and the number of routes on the card is increased accordingly. The `ipRoutesPoolCapacity` must be increased to accommodate the higher number of allowed routes.



```
set Lp/<lp_number> Eng Fcrc Pqc Ov ipRoutesPoolCapacity
<pool_capacity>
```

13 Add the *Interface* component.

```
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address>
```

14 Set the *netMask* attribute.

```
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address>
netMask <mask>
```

15 Add the media to the VRF interfaces.

If you are adding an ATM media to the VRF for each access link to a CE device, complete this command:

```
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
```

If you are adding the loopback interface to verify the PE to PE node connections without any CE device connected, complete this command:

```
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> Lb
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address>
netmask 255.255.255.255
```

16 If you are adding the loopback interface to verify the PE to PE node connections without any CE device connected, complete these commands:

```
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> Lb
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address>
netmask 255.255.255.255
```

--End--

Variable definitions

Variable	Value
<alarm_limit>	is the alarm limit value, which ranges from 1 to 65535.
<discard_limit>	is the discard limit value, which ranges from 1 to 65535.
<ip_address>	is the 32-bit address assigned to this interface.
<mask>	is the network mask to be used with the IP address.
<mode>	identifies the mode. Values are both, import, and export. Default is both.
<pool_capacity>	is the pool capacity limit value, which ranges from 0 to 100 000. The default value is 4096.
<route_pref>	is the route preference value.

(1 of 2)



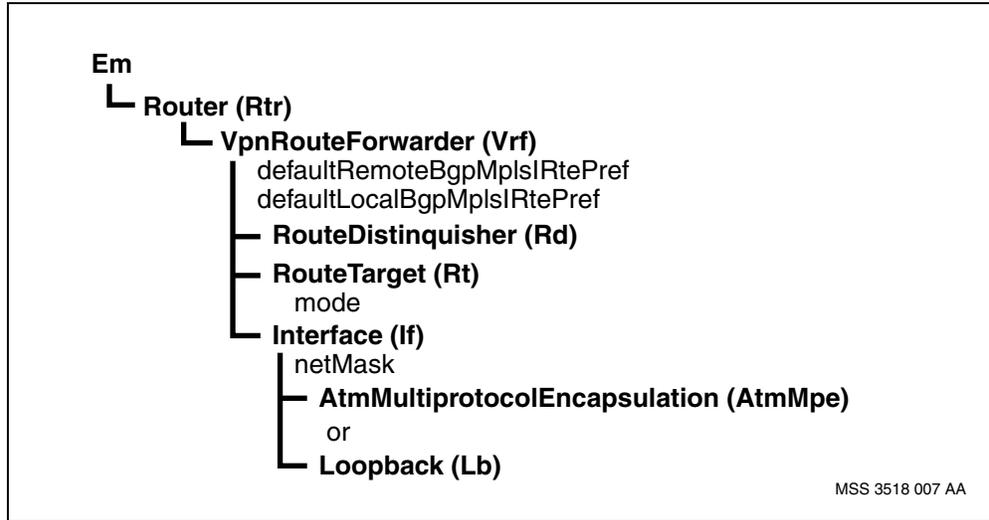
Variable	Value
<rd_value>	specifies the route distinguisher for the VRF. The syntax can be in the form of Type 0 or Type 1. Type 0 is a 2-byte AS number and a 4-byte number assigned by the SP (AS:xxxx). Type 1 is a 4-byte ipv4 address and a 2-byte number assigned by the SP (ipv4:xx). The RD must be unique on the PE node.
<rtr_name>	is the name of the router.
<rt_value>	identifies the VPN. For two or more customer sites to talk, they must have at least one route target in common. The syntax can be in the form of Type 0 or Type 1. Type 0 is a 2-byte AS number and a 4-byte number assigned by the SP (AS:xxxx). Type 1 is a 4-byte ipv4 address and a 2-byte number assigned by the SP (ipv4:xx).
<vrf_name>	is the name of the VPN route forwarder.

(2 of 2)



Procedure job aid

VRF component hierarchy





Configuring ATM media and feature set

Configure ATM Multiprotocol Encapsulation (AtmMpe) media for a VRF Interface instance to define ATM connectivity between the PE node and the CE route. The AtmMpe media enables IP data traffic to be received and transmitted over AAL5 using RFC 2684 encapsulation methods. IP over ATM is a supported access media for BGP/MPLS VPN. The following mode/encapsulations are supported:

- direct (single AC subcomponent under AtmMpe linked to IP interface)
- VCC-bundle (multiple AC subcomponents under the AtmMpe) for PVC or SPVC
- IP over ATM SPVC between ATM UNI and ATM MPE
- IP bridge termination over ATM (LLC-SNAP encapsulation for Ethernet frames)

Prerequisites

For NPVC, you must do the following:

- Configure the *AtmIf* component. See NN10600-710 *Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*

For SPVC, you must do the following:

- Configure the required ATM routing components. See NN10600-710 *Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*.
- Configure the *Pnni* component under the *AtmRouting* and *AtmInterface* components. See NN10600-710 *Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*.

Procedure steps

Step	Action
1	Configure the feature set on ATM supported access cards. set Sw Lpt/<lp_name> featureList rfc2547bis atmMpe ip
2	Configure the ip routes pool capacity on a Multiservice Switch 7400 or Multiservice Switch 15000 ATM access LP. add -s Lp/<lp_number> eng fcrc pqc set Lp/<lp_number> eng fcrc pqc ov ipRoutesPoolCapacity 64000
3	Set the ATM connection for direct mode (single AC subcomponent). set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe Ac/<ac_id> atmConnection AtmIf/<n> Vcc/<vpi.vci> Nep



- 4 Set the ATM connection for VCC-bundle mode (multiple AC subcomponents).

```
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id1> atmConnection AtmIf/<n> Vcc/<vpi.vci1> Nep
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id2> atmConnection AtmIf/<n> Vcc/<vpi.vci2> Nep
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id3> atmConnection AtmIf/<n> Vcc/<vpi.vci3> Nep
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id4> atmConnection AtmIf/<n> Vcc/<vpi.vci4> Nep
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id1> ipCos 0
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id2> ipCos 1
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id3> ipCos 2
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id4> ipCos 3
```

- 5 Set the ATM connection for IP over ATM SPVC mode.

When CPE is setting up the SPVC connection:

```
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
stp
add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id> dstpvc
```

When the VRF is setting up the SPVC connection:

```
add -s Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address>
AtmMpe Ac/<ac_id> SourcePvc
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
Ac/<ac_id> SourcePvc remoteAddress <remote_NSAP>,
remoteConnectionIdentifier <remote_ConnID>
```

- 6 Set the ATM connection for IP bridge termination over ATM mode.

```
add -s Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address>
AtmMpe Ac/<ac_id> atmConnection AtmIf/<n> Vcc/<vpi.vci>
Nep
set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe
encapType llcBridgeEncap, maxTransmissionUnit 1500
```

--End--

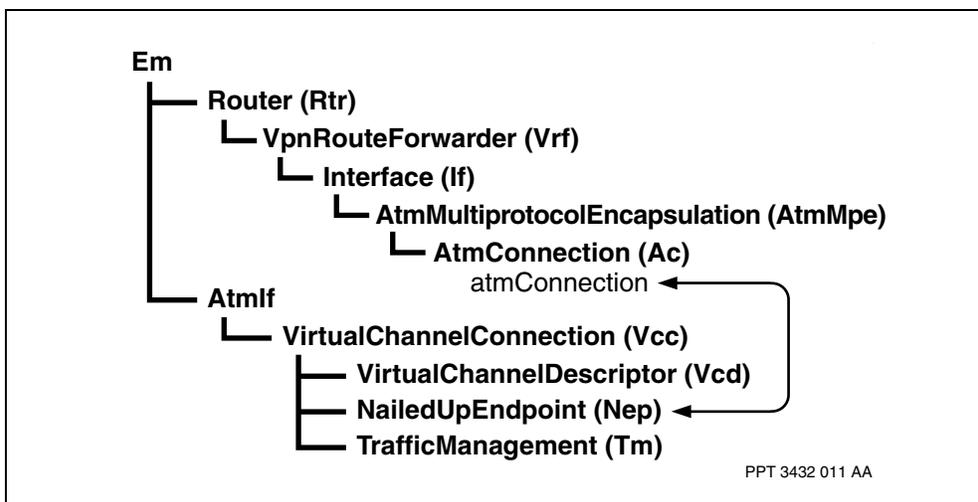


Variable definitions

Variable	Value
<ac_id>	is the instance value of the atm connection component under AtmMpe. Any mnemonic (for example, AC/1).
<atmif_id>	is the instance value of the <i>AtmIf</i> component.
<ip_address>	is the 32-bit address assigned to this interface.
<lp_number>	is the number assigned to the LP.
<lpt_name>	is the name assigned to the software Lpt for this Lp.
<remote_ConnID>	is the remote VCI value (assuming VPI 0) if the SPVC terminates on an AtmIf, or the AC instance value if the SPVC terminates into a remote AtmMpe.
<remote_NSAP>	is the ATM NSAP address of the remote (called end) ATM interface of the SPVC connection.
<rtr_name>	is the name of the router.
<vpi.vci>	is the identifier assigned to the VP and VC of the virtual channel. It is a good practice to assign the vci value of the atm connection to the ac_id (example: set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe Ac/40 atmConnection AtmIf/<n> Vcc/0.40 Nep. It is the ac_id that is displayed in the ARP table for the IP address mapping to the layer 2 attribute (inverse ARP).

Procedure job aid

ATM media and feature set component hierarchy





Configuring PPP media and feature set for VRF in RFC2547 mode

Configure PPP media and feature set for VRF in RFC2547 mode in order to carry IP over PPP.

Prerequisites

- Required PPP (single-link or multi-link) interfaces are configured. For more information about PPP interface configuration, see NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- Hardware connections for the PPP interface are configured.

Procedure steps

Step	Action
1	Add rfc2547bis to the feature set. <code>set sw lpt/<lpt_name> featurelist rfc2547bis</code>
2	Set the Vrf interface netmask. <code>set Rtr/<rtr_name> vrf/<vrf_name> If/<ip_address> netmask <netmask></code>
3	If the netmask is a 32-bit mask, configure the Vrf interface link destination address. <code>set Rtr/<rtr_name> vrf/<vrf_name> If/<ip_address> linkDestinationAddress <remote_ip_address></code>
4	Add a PPP media application to the Router Vrf interface. <code>add -s Rtr/<rtr_name> vrf/<vrf_name> If/<ip_address> PppApplication</code>
5	Link the application to the corresponding PPP media interface that is under the root component. <code>set Rtr/<rtr_name> vrf/<vrf_name> If/<ip_address> PppApplication linkToMedia ppp/<ppp_instance></code>
--End--	

Variable definitions

Variable	Value
<ip_address>	is the Internet Protocol address for the interface.
<lpt_name>	is the label for the interface.
(1 of 2)	



Variable	Value
<netmask>	is the is the interface netmask.
<ppp_instance>	is the instance number of the PPP media interface.
<remote_ip_address>	is the IP address configured at the other end of this PPP interface.
<rtr_name>	is the name of the router.
<vrf_name>	is the name of the VPN route forwarder.
(2 of 2)	



Configuring Ethernet media and feature set

Configure the Ethernet media (port or virtual LAN [VLAN]) to carry IP over Ethernet.

For more information on the Ethernet media, refer to the chapter on Multiservice Switch IP fundamentals in NN10600-800 *Nortel Multiservice Switch 7400/15000/20000 IP Technology Fundamentals*.

Prerequisites

- To configure an Ethernet interface in port mode or VLAN mode, see NN10600-821 *Nortel Multiservice Switch 7400/15000/20000 Operations: Ethernet Services*.

Procedure steps

Step	Action
1	Add <i>EnetApplication</i> component as the media interface. <code>add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> Enet</code>
2	Link the <i>EnetApplication</i> component to the Ethernet media in port mode. <code>set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> Enet linkToEnetIf La/<la_number></code> or <code>set La/<la_number> enetConnection Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> Enet</code>
3	Link the <i>EnetApplication</i> component to the Ethernet media in VLAN mode. <code>set Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> Enet linkToEnetIf La/<la_number> Vlan/<vlan_number></code> or <code>set La/<la_number> Vlan/<vlan_number> enetConnection Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> Enet</code>

--End--

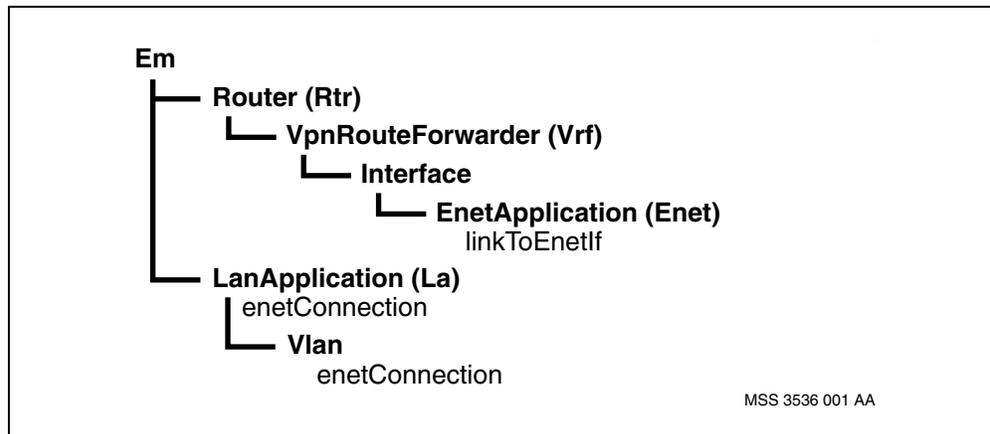


Variable definitions

Variable	Value
<ip_address>	is the 32-bit address assigned to this interface.
<la_number>	is the number of the <i>LanApplication</i> instance.
<rtr_name>	is the name of the router.
<vlan_number>	is the identifier of the <i>vlan</i> instance.
<vrf_name>	is the name of the VPN route forwarder.

Procedure job aid

Ethernet media and feature set component hierarchy





Creating a VRRP virtual router

Create a virtual router redundancy protocol (VRRP) virtual router to provide VPN route forwarder (VRF) redundancy.

Optionally, set the VRRP advertisement interval on both the master and backup VRRP virtual routers (VRs) through the *advertisementInterval* attribute. The master and backup VRRP VRs require the same value.

Procedure steps

Step	Action
1	Add the <i>Vrrp</i> component to the Ethernet interface. The VRRP virtual router (VR) is the master. <pre>add Rtr/<router_A> Vrf/<vrf_name> If/ <interface_address> Vrrp/<vrrp_name></pre>
2	Set the <i>ipAddresses</i> attribute for the VRRP VR with which it is associated. <pre>set Rtr/<router_A> Vrf/<vrf_name> If/ <interface_address> Vrrp/<vrrp_name> ipAddresses <ipaddress></pre>
3	Set the <i>priority</i> attribute of the master VRRP VR. If the master VRRP VR owns the IP address of the VRF, set the priority to 255. <pre>set Rtr/<router_A> Vrf/<vrf_name> If/<ip_address> Vrrp/ <vrrp_name> priority <priority_value></pre>
4	Add the <i>Vrrp</i> component to the Ethernet interface. The VRRP VR is a backup. <pre>add Rtr/<router_B> Vrf/<vrf_name> If/ <interface_address> Vrrp/<vrrp_name></pre>
5	Set the <i>ipAddresses</i> attribute of VRRP VR. <pre>set Rtr/<router_B> Vrf/<vrf_name> If/ <interface_address> Vrrp/<vrrp_name> ipAddresses <ipaddress></pre>
6	Set the <i>priority</i> attribute of the backup VRRP VR. <pre>set Rtr/<router_B> Vrf/<vrf_name> If/ <interface_address> Vrrp/<vrrp_name> priority <priority_value></pre> <p>When you have multiple backup VRRP VRs, it is very important to set the priority because it defines which backup VRRP VR is active when the master VRRP VR has a failure.</p>



- 7 Optionally, set the *advertisementInterval* attribute on the master VRRP VR. Ensure that the *advertisementInterval* attribute value is the same for the backup and master VRRP VRs.

```
set Rtr/<router_A> Vrf/<vrf_name> If/  
<interface_address> Vrrp/<vrrp_name>  
advertisementInterval <ad_inter>
```

- 8 Optionally, set the *advertisementInterval* attribute on the backup VRRP VR. Ensure that the *advertisementInterval* attribute value is the same for the backup and master VRRP VRs.

```
set Rtr/<router_B> Vrf/<vrf_name> If/  
<interface_address> Vrrp/<vrrp_name>  
advertisementInterval <ad_inter>
```

- 9 Activate the changes. See [Activating configuration changes \(page 161\)](#).

--End--

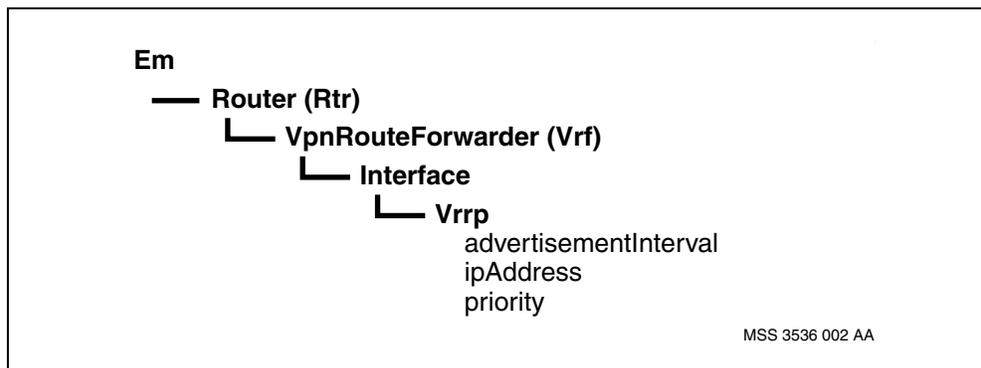


Variable definitions

Variable	Value
<ad_inter>	is the advertisement interval time in seconds.
<interface_address>	is the 32-bit address assigned to this interface.
<ipaddress>	specifies one or more IP addresses associated with the <i>Vrrp</i> instance. Typically, this IP address is the same as the IP addresses of the master VRRP VR.
<priority_value>	is a decimal value between 1 and 255. The higher priority is for the master VRRP VR.
<router_A>	is an instance name of a Multiservice Switch RTR on node A.
<router_B>	is an instance name of a Multiservice Switch RTR on node B.
<vrf_name>	is the name of the VPN route forwarder.
<vrrp_name>	is instance name of the VRRP VR.

Procedure job aid

VRRP virtual router component hierarchy





Example of creating a VRRP virtual router associated with an Ethernet interface in port mode

Prior to starting this example procedure, ensure that Nodes 1 and 2 have the *LanApplication* component in port mode. For more information about Configuring an Ethernet interface in port mode, see NN10600-821 *Nortel Multiservice Switch 7400/15000/20000 Operations: Ethernet Services*.

Procedure steps

Step	Action
1	Set the <i>featureList</i> attribute to include <i>ipvrrp</i> . <pre>set sw Lpt/ethernet featureList ipvrrp</pre>
2	Activate the changes without ending your provisioning session. See Activating configuration changes (page 161) .

For Node 1, complete the following steps:

- 3 Add the *Vrrp 1* component to the Ethernet interface. The VRRP virtual router (VR) is the master.

```
add Rtr/1 Vrf/1 If/<interface_address> Vrrp/1
```
- 4 Set the *ipAddresses* attribute that the VRRP VR is associated with.

```
set Rtr/1 Vrf/1 If/<interface_address> Vrrp/1 ipAddresses <ipaddress_1B>
```
- 5 This VRRP VR is the master because it owns the IP address set in [step 4](#). Set the *priority* attribute of the master VRRP VR to 255.

```
set Rtr/1 Vrf/1 If/<interface_address> Vrrp/1 priority 255
```

For Node 2, complete the following steps:

- 6 Add the *Vrrp* component to Ethernet interface. The VRRP virtual router (VR) is the backup.

```
add Rtr/1 Vrf/1 If/<interface_address> Vrrp/1
```
- 7 Set the *ipAddresses* attribute that the VRRP VR is associated with.

```
set Rtr/1 Vrf/1 If/<interface_address> Vrrp/1 ipAddresses <ipaddress_1B>
```
- 8 This VRRP VR does not own the IP address set in [step 7](#) because it is the backup VRRP VR. Set the *priority* attribute of the backup VRRP VR to a value less than 255.

```
set Rtr/1 Vrf/1 If/<interface_address> Vrrp/1 priority <priority_value>
```
- 9 Activate configuration changes. See [Activating configuration changes \(page 161\)](#).



--End--

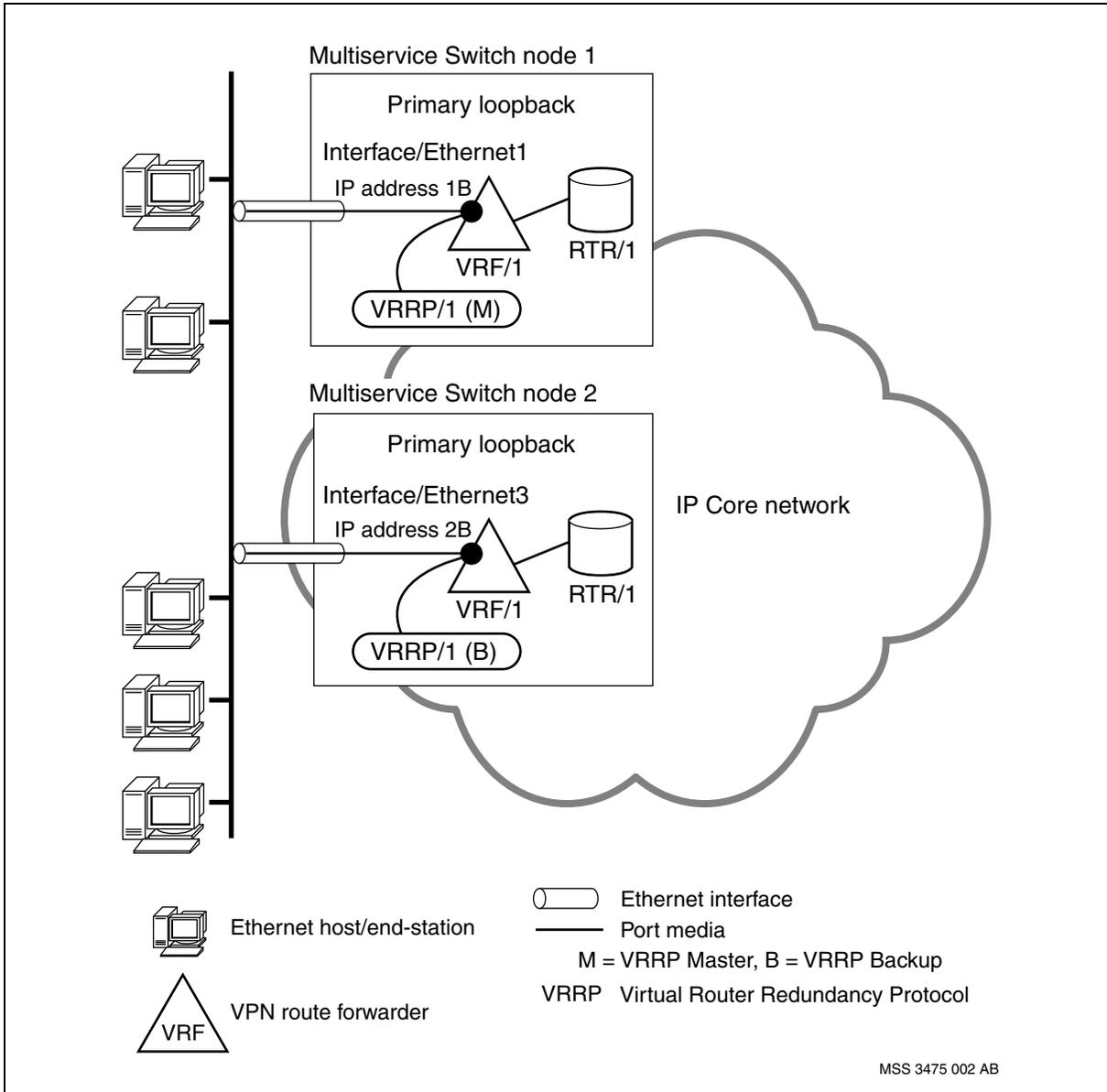
Variable definitions

Variable	Value
<ipaddress_1B>	is the IP address of the master VRRP VR.
<priority_value>	is a decimal value between 1 and 255. The higher priority is for the master VRRP VR.



Procedure job aid

Example figure for creating a VRRP virtual router associated with an Ethernet interface in port mode





Example of creating a VRRP virtual router associated with a VLAN on an Ethernet interface

Prior to starting this example procedure, ensure that Nodes 3 and 4 have the *LanApplication* component in VLAN mode. For more information about Configuring an Ethernet interface in VLAN mode, see NN10600-821 *Nortel Multiservice Switch 7400/15000/20000 Operations: Ethernet Services*.

Procedure steps

Step	Action
------	--------

For Node 3, complete the following steps:

- 1 Add the *Vrrp 4* component to the interface. The VRRP virtual router (VR) is the master.
`add Rtr/1 Vrf/1 If/<interface_address> Vrrp/4`
- 2 Set the *ipAddresses* attribute that the VRRP VR is associated with.
`set Rtr/1 Vrf/1 If/<interface_address> Vrrp/4 ipAddresses <ipAddress_3B>`
- 3 This VRRP VR is the master because it owns the IP address set in [step 2](#). Set the *priority* attribute of the master VRRP VR to 255.
`set Rtr/1 Vrf/1 If/<interface_address> Vrrp/4 priority 255`
- 4 Activate the changes without ending your provisioning session. See [Activating configuration changes \(page 161\)](#).

For Node 4, complete the following steps:

- 5 Add the *Vrrp 4* component to the interface. The VRRP VR is a backup.
`add Rtr/1 Vrf/1 If/<interface_address> Vrrp/4`
- 6 Set the *ipAddresses* attribute that the VRRP VR is associated with.
`set Rtr/1 Vrf/1 If/<interface_address> Vrrp/4 ipAddresses <ipAddress_3B>`
- 7 This VRRP VR does not own the IP address set in [step 6](#) because it is the backup VRRP VR. Set the *priority* attribute of the backup VRRP VR to a value less than 255.
`set Rtr/1 Vrf/1 If/<interface_address> Vrrp/4 priority <priority_value>`
- 8 Activate configuration changes. See [Activating configuration changes \(page 161\)](#).

--End--

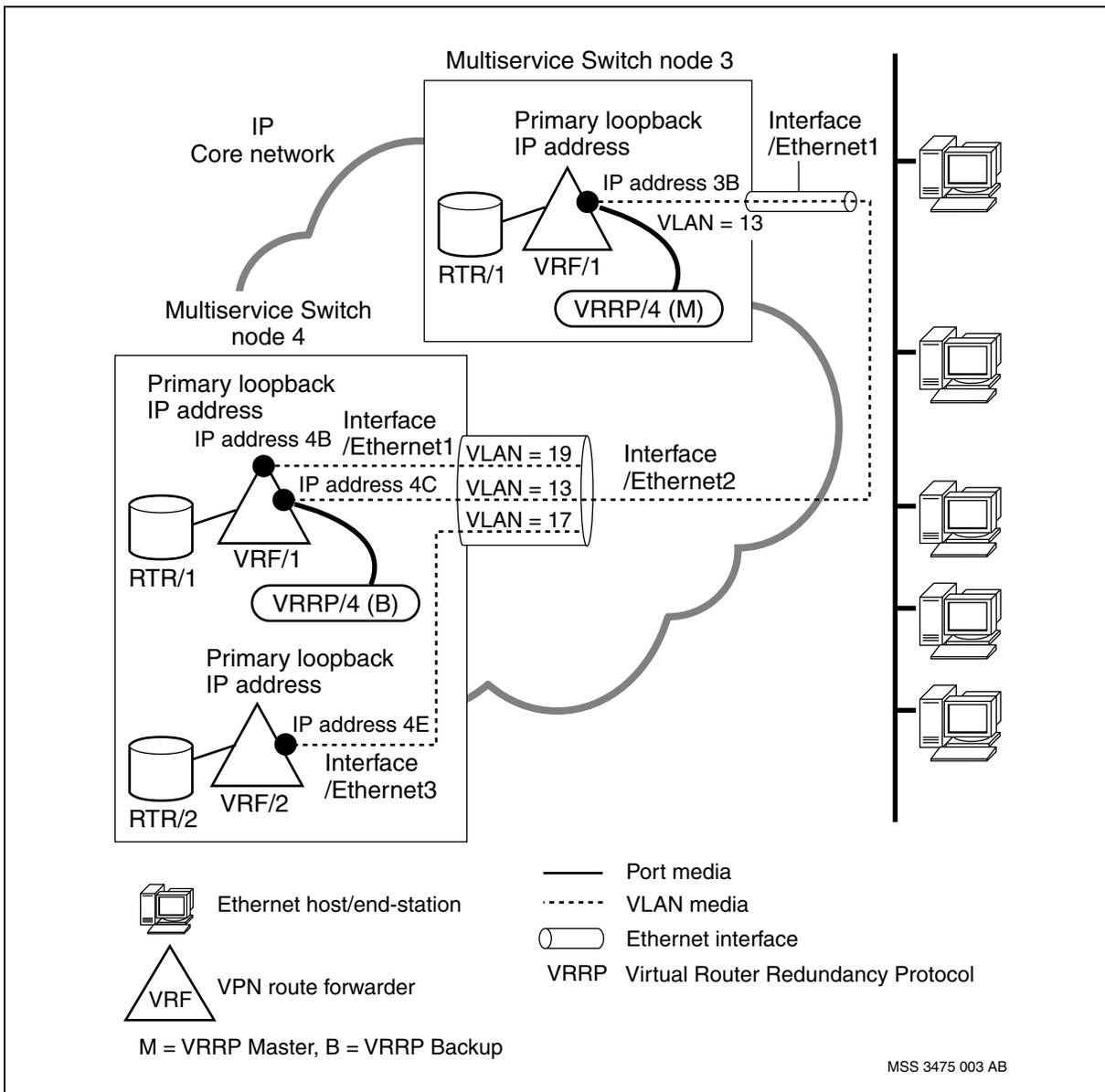


Variable definitions

Variable	Value
<ipaddress_3B>	is the IP address of the master VRRP VR.
<priority_value>	is a decimal value between 1 and 255. The higher priority is for the master VRRP VR.

Procedure job aid

Example figure for creating a VRRP virtual router associated with a VLAN on an Ethernet interface





Configuring frame relay media and feature set

Configure frame relay media for a VRF Interface instance to define Frame relay physical connectivity between the CE and the PE node. Frame relay access to a VRF can be achieved through a direct connection over an existing channel (Ip Optimized direct) or through a backhaul scenario (DPRS trunk). You can use a software configuration with a vframer component or for enhanced quality of service, use a hairpin configuration.

Prerequisites

- A *FrUni Dci IpConn* component must be provisioned and linked to the *IpDci* media. This configuration allows for direct Frame relay access to an IP VPN network. For more information about configuring Frame relay, see NN10600-901 *Nortel Multiservice Switch 7400/15000/20000 Frame Relay Configuration Management*.

Procedure steps

Step	Action
1	Configure the feature set (frUniAllDprs, is for backhaul access only). <pre>set Sw Lpt/<lpt_name> featureList rfc2547bis frUniIpOptimized, ip, frUniAllDprs</pre>
2	Add the Ip Optimized DLCI media to the VRF interface. <pre>add Rtr/<rtr_name> Vrf/<vrf_name> If/<ip_address> IpODlci Frc/<frc></pre>
3	Set the numberOfEmissionsQs attribute to 4. <pre>set Fruni/<fruni_inst> numberOfEmissionsQs 4</pre> <p>Regardless of the number of DLCIs being used, it is recommended that the numberOfEmissionsQs attribute be set to 4, so that 4 emission queues are available instead of the default 2.</p>
4	Set the emission queue size. <pre>set FrUni/<FrUni_inst> doubleEmissionQSize <QSize_value></pre> <p>If <QSize_value> is yes, the FrUni must be linked to a real framer.</p>
5	Link the Ip Optimized DLCI media to the Ip Connection under the appropriate Fruni and Dci (ipOptimized direct). <pre>set Rtr/<rtr_name> vrf/<vrf_name> If/<ip_address> IpODlci Frc/<frc> linkToFrDlci Fruni/<fruni_inst> Dci/ <dci> IpConnection</pre>
6	Add the DPRS Fruni component for CE connectivity. <pre>add FrUni/<fruni_inst></pre>



- 7 Remove the physical framer and add the virtual framer for the software connection.

```
del FrUni/<fruni_inst> framer  
add FrUni/<fruni_inst> Vframer
```
- 8 Link the IP optimized FrUni to the DPRS FrUni (direct call) and associate it with a frame relay based LP.

```
set FrUni/<fruni_inst> Vframer otherVirtualFramer FrUni/  
<fruni_inst> VFramer  
set FrUni/<fruni_inst> Vframer logicalProcessor Lp/  
<lpt_name>
```
- 9 Set the DPRS FrUni for remote signalling onto a remote Multiservice Switch node for CE connectivity. This DLCI will signal the remote X121 FrUni DLCI through the DPRS backbone

```
add FrUni/<fruni_inst> Dlci/<dlci> dc
```
- 10 If rate enforcement and LMI is required, it should be applied on this FrUni, facing the DPRS core.

```
set FrUni/<fruni_inst> Dlci/<dlci> Sp rateEnforcement on  
set FrUni/<fruni_inst> lmi proc itu (or ansi)
```
- 11 Set the DP to DE mapping.

```
set FrUni/<fruni_inst> Dlci/<dlci> IpConn dpToDeMapLevel  
<level>
```
- 12 For the hairpin scenario, link the framer to an existing physical port.

```
add FrUni/<fruni_inst>  
set FrUni/<fruni_inst> Vframer logicalProcessor Lp/  
<lpt_name> port/<port>  
add FrUni/<fruni_inst> Dlci/<dlci> dc  
set FrUni/<fruni_inst> Dlci/<dlci> Sp rateEnforcement on  
set FrUni/<fruni_inst> lmi proc itu (or ansi)  
set FrUni/<fruni_inst> Dlci/<dlci> IpConn dpToDeMapLevel  
<level>
```

--End--

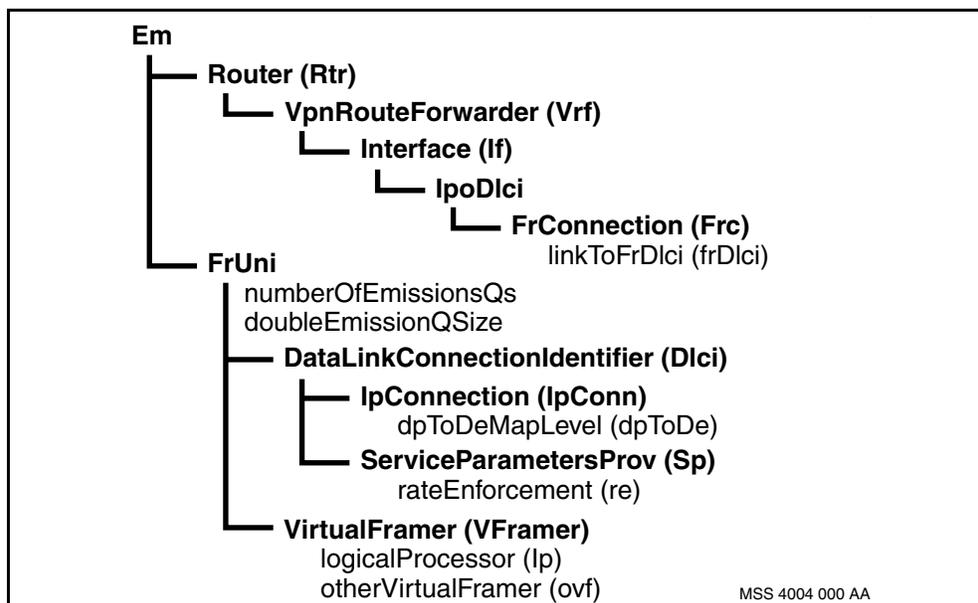


Variable definitions

Variable	Value
<dlci>	is the highest DLCI value permitted for a permanent connection.
<frc>	is the name assigned to the FR connection.
<fruni_inst>	is the instance number of the FR UNI. The instance value must be unique.
<ip_address>	is the 32-bit address assigned to this interface.
<level>	is NotApplicable (default), high, medium or low.
<lpt_name>	is the name assigned to the software Lpt for this Lp.
<port>	is the port number.
<QSize_value>	is the value of the <i>doubleEmissionQSize</i> attribute. The default value is no, a value of yes will double the emission queue size. This attribute is only compatible with the 8-port V.11, 4-port E1, and 4-port E1Ch FPs. When the FrUni is linked to a virtual framer, the value must be no or a semantic check error will occur.
<rtr_name>	is the name of the router.

Procedure job aid

Frame relay and feature set component hierarchy





Configuring EGBP

Configure external border gateway protocol (EGBP) as the access protocol to exchange IP address prefixes between the CE router and the PE router. EGBP provides the benefit of having low routing overhead to support it and gives access to powerful policy control mechanisms.

Optionally, configure MD5 authentication on an EGBP peer connection to provide protection of EGBP neighbor relationships. Change an MD5 key on an authenticated EGBP peer using the procedure [Changing an MD5 key on an authenticated EGBP peer \(page 88\)](#).

Procedure steps

Step	Action
1	Add BGP on the VRF, and set the <i>localAs</i> and <i>BGPIdentifier</i> attributes. <pre>add -s Rtr/<rtr_name> Vrf/<vrf_name> Bgp localAs <as_value> bgpIdentifier <ip_address></pre>
2	Add the EGBP peer over a VRF access interface. <pre>add -s Rtr/<rtr_name> Vrf/<vrf_name> Bgp Peer/<Peer> Desc peerAs <value></pre>
3	Configure the <i>removePrivateAs</i> attribute to learn the IP address from the remote VPN site. <pre>set Rtr/<router> Vrf/<vrf_name> Bgp Peer/<Peer> Desc remPrivate enabled</pre>
4	Optionally, configure MD5 authentication on a BGP peer connection. Set the MD5 key value under the <i>Descriptor</i> . <pre>Set Rtr/<rtr_name> Vrf/<vrf_name> Bgp Peer/<ip_addr> Desc md5Key <ASCII_string></pre>
5	Optionally, add the BGP export policy, setting the <i>protocol</i> attribute value to <i>bgpMplsInternal</i> . <pre>add -s Rtr/<rtr_name> Vrf/<vrf_name> Bgp Export/ <export_policy_number> protocol bgpMplsInternal</pre>
6	Enable the multi-hop EGBP route distribution on a peer if you want to allow the distribution of routes across multiple hops between BGP peers that belong to different autonomous systems (AS). <pre>set Rtr/<rtr_name> Vrf/<vrf_name> Bgp Peer/<Peer> Desc multiHopEbgp <multihop_ebgp></pre>
7	Set the <i>peerIpAddress</i> attribute. <pre>set Rtr/<rtr_name> Vrf/<vrf_name> Bgp Export/ <export_policy_name> peerIpAddress <peer_ip_address></pre>



- 8** Optionally, set the Multi Exit Discriminator (MED) value.
- ```
set Rtr/<rtr_name> Vrf/<vrf_name> Bgp Export/
<export_policy_name> med <med_value>
```
- 

**--End--**

---

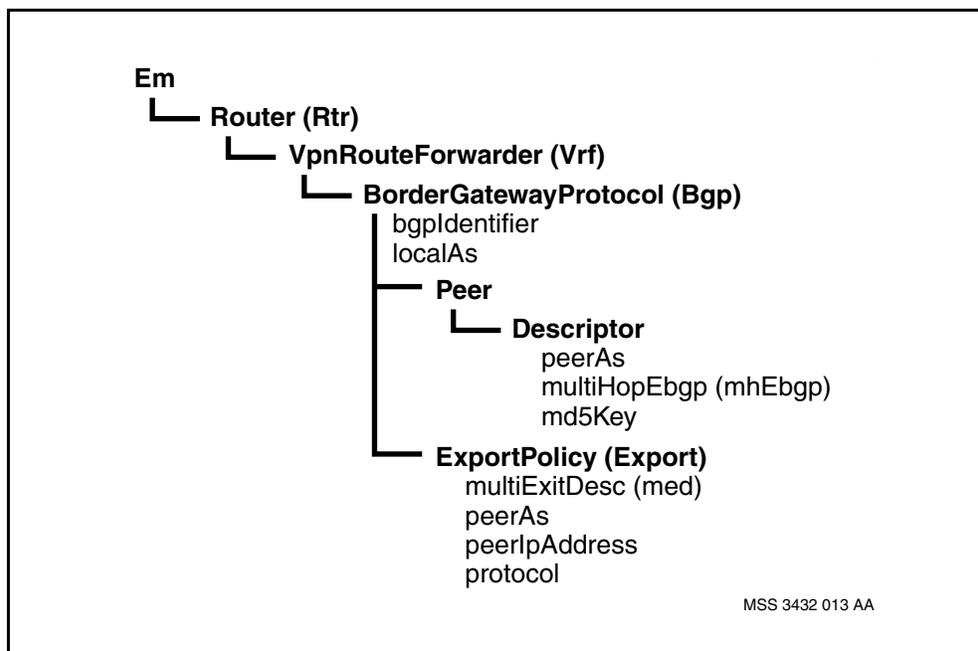


### Variable definitions

| Variable                | Value                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ASCII_string>          | is the MD5 key value, 1-255 ASCII characters in length.                                                                                                          |
| <as_value>              | is a value assigned to the Autonomous System. Note that the localAS value and the peerAS value must be different. The VRF AS and the router AS must be the same. |
| <export_policy_number > | is the numeric designation assigned to the export policy.                                                                                                        |
| <ip_address>            | is the IP address of the BGP Identifier.                                                                                                                         |
| <med_value>             | is the value assigned to the multi exit discriminator.                                                                                                           |
| <multihop_ebgp>         | is identifying whether the multihop EBGp route distribution capability is disabled or enabled on a BGP peer.                                                     |
| <peer>                  | is the IP address of the BGP peer.                                                                                                                               |
| <peer_ip_address>       | is the IP address of the peer.                                                                                                                                   |
| <rtr_name>              | is the name of the router.                                                                                                                                       |
| <vrf_name>              | is the name of the VPN route forwarder.                                                                                                                          |

### Procedure job aid

#### EBGP component hierarchy





## Changing an MD5 key on an authenticated EBGp peer

Transition MD5 keys without having to terminate the BGP session for which the key is being changed, if you have optionally configured MD5 authentication on a BGP peer.

When changing keys on a BGP session between a Multiservice Switch node and a non-Multiservice Switch, change the key on the Multiservice Switch node to minimize the outage time.

A longer MD5 key will be more difficult to break, however, the longer the key used, the greater the impact on performance. A key length of between 12 and 24 characters should be sufficiently secure without having too great an impact on performance.

It is recommended that different MD5 key values be used for each BGP peer.

## Procedure steps

---

| Step | Action                                                                                                                                                                                                                                                      |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Set the <i>keyTransitionDelay</i> attribute on the local and remote router, for all BGP peers.<br><br><b>Set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Bgp keyTransitionDelay &lt;n&gt;</b>                                                                 |
| 2    | Alternatively, set the <i>keyTransitionDelay</i> attribute on the local and remote router, for a specific peer's <i>Descriptor</i> .<br><br><b>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Bgp peer/&lt;ip_addr&gt; Desc keyTransitionDelay &lt;n&gt;</b> |
| 3    | Set the new MD5 key value on the local and router.<br><br><b>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Bgp peer/&lt;ip_addr&gt; Desc md5Key &lt;ASCII_string&gt;</b>                                                                                    |

---

--End--

---

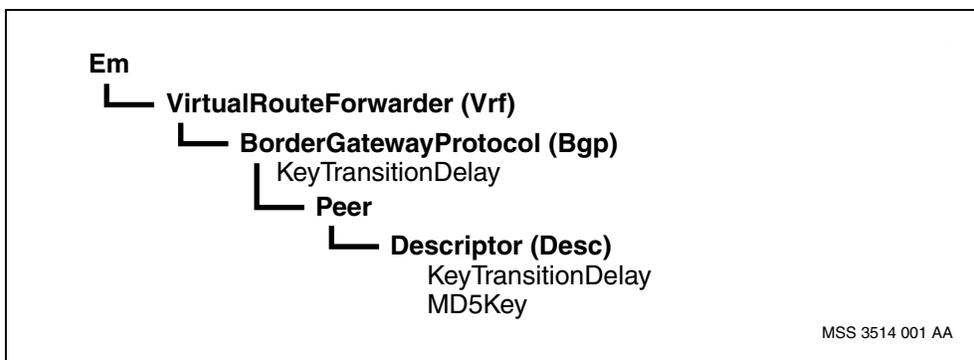


## Variable definitions

| Variable       | Value                                                                                                                                                                                                                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ASCII_string> | is the MD5 key value, 1-255 ASCII characters in length.                                                                                                                                                                                                                                                                                 |
| <ip_addr>      | is a 32-bit address assigned to the interface from which the routing information is derived.                                                                                                                                                                                                                                            |
| <n>            | is the amount of time the operator has to provision both the local and remote ends with the new key, without losing service.<br>for the <i>Bgp</i> component, the value is 1 to 20160 (minutes), default is 10 minutes.<br>for the <i>Descriptor</i> component, the value is "sameAsBgp, 1 to 20160 (minutes)", default is "sameAsBgp". |
| <rtr_name>     | is the name of the router.                                                                                                                                                                                                                                                                                                              |

## Procedure job aid

### Component hierarchy for changing an MD5 key on an authenticated BGP peer





## Configuring BGP route flood protection

Optionally, configure the border gateway protocol (BGP) route flood protection to control the maximum number of IPv4 learned routes imported by all BGP sessions connected to a specific RFC2547 VPN route forwarder (VRF).

The variables *bgpImportRouteLimit* and *bgpImportRouteDiscardLimit* have default values of zero, meaning that there is no user provisioned value and BGP route flood protection is not enforced.

### Procedure steps

---

| Step | Action                                                                                                                                                        |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Set the Bgp import alarm limit.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Bgp<br/>bgpImportRouteLimit &lt;import_alarm_limit&gt;</pre>            |
| 2    | Set the Bgp import discard limit.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Bgp<br/>bgpImportRouteDiscardLimit &lt;import_discard_limit&gt;</pre> |

---

--End--

---

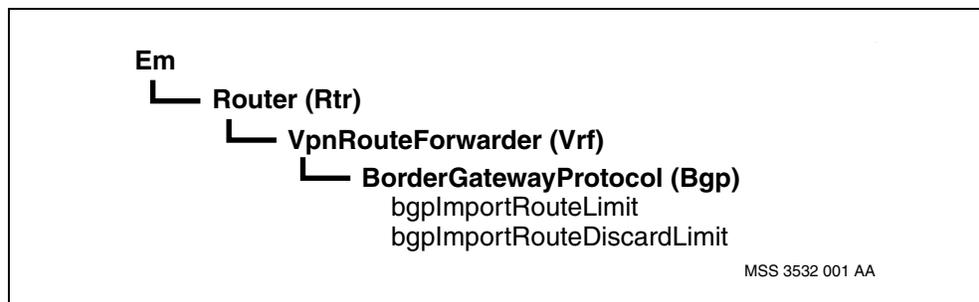


## Variable definitions

| Variable               | Value                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <import_alarm_limit>   | specifies a limit to control the maximum number of imported BGP Ipv4 Unicast routes that will be processed until an alarm is generated. This limit is chosen based on the requirements of various network configurations. The default value of zero implies that there is no limit set. In such a configuration, no alarm is generated and default behavior is expected. This attribute is critical under BGP.                                     |
| <import_discard_limit> | specifies a limit to control the maximum number of imported BGP Ipv4 Unicast routes that will be processed until an alarm is generated and subsequent routes are discarded. This limit is chosen based on the requirements of various network configurations. The default value of zero implies that there is no limit set. In such a configuration, no alarm is generated and default behavior is expected. This attribute is critical under BGP. |
| <rtr_name>             | is the name of the router.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <vrf_name>             | is the name of the VPN route forwarder.                                                                                                                                                                                                                                                                                                                                                                                                            |

## Procedure job aid

### BGP route flood protection component hierarchy





## Configuring BGP peer route flood protection

Optionally, configure the border gateway protocol (BGP) peer route flood protection to control the maximum number of IPv4 learned routes imported by a specific customer edge (CE) BGP session connected to an RFC2547 VPN route forwarder (VRF).

The variables *bgpPeerRouteLimit* and *bgpPeerRouteDiscard* have default values of zero, meaning that there is no user provisioned value and BGP per peer route flood protection is not enforced.

### Procedure steps

---

| Step | Action                                                                                                                                                                                                |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Set the Bgp peer import alarm limit.<br><br><code>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Bgp peer/<br/>&lt;peer_address&gt; desc bgpPeerRouteLimit<br/>&lt;import_alarm_limit&gt;</code>       |
| 2    | Set the Bgp peer import discard limit.<br><br><code>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Bgp peer/<br/>&lt;peer_address&gt; desc bgpPeerRouteDiscard<br/>&lt;import_discard_limit&gt;</code> |

---

--End--

---

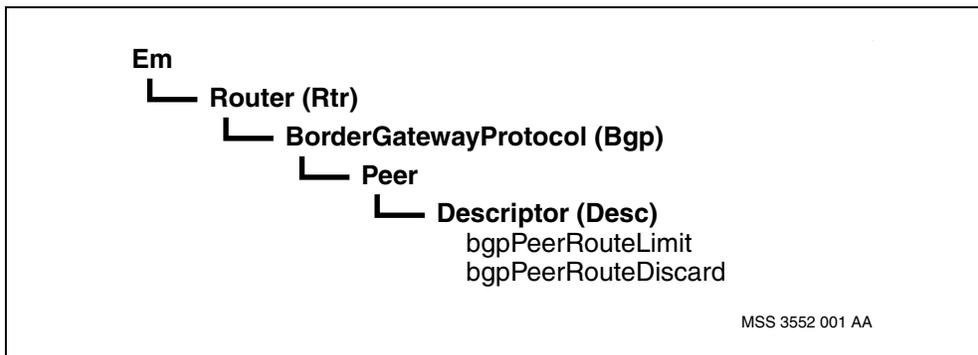


## Variable definitions

| Variable               | Value                                                                                                                                                                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <import_alarm_limit>   | specifies a limit to control the maximum number of imported BGP Ipv4 Unicast routes that will be processed by one peer until an alarm is generated. This limit is chosen based on the requirements of various network configurations. This attribute is optional but critical under BGP peer.                                     |
| <import_discard_limit> | specifies a limit to control the maximum number of imported BGP Ipv4 Unicast routes that will be processed by one peer until an alarm is generated and subsequent routes are discarded. This limit is chosen based on the requirements of various network configurations. This attribute is optional but critical under BGP peer. |
| <peer_address>         | is the IP address of the peer.                                                                                                                                                                                                                                                                                                    |
| <rtr_name>             | is the name of the router.                                                                                                                                                                                                                                                                                                        |
| <vrf_name>             | is the name of the VPN route forwarder.                                                                                                                                                                                                                                                                                           |

## Procedure job aid

### BGP peer route flood protection component hierarchy





---

## Configuring OSPF

Configure Open Shortest Path First (OSPF) as the access protocol to exchange IP address prefixes between the CE router and the PE router. Although EBGP is the recommended access routing protocol, OSPF is also supported.

---

**Attention:** This procedure assumes a point-to-point link.

---

---

**Attention:** To support the equal cost multi-path (ECMP) on egress, all access links on the associated VRF must reside on the same functional processor (FP).

---

### Procedure steps

---

| Step | Action                                                                                                                                                                                                                                                          |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add the <i>Ospf</i> component, and set the <i>routerId</i> , <i>redistributeIbgp</i> , and <i>asBr</i> attribute values.<br><br><code>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Ospf routerId &lt;router_id&gt;, redistributeIbgp true, asbr true</code> |
| 2    | Add the OSPF area.<br><br><code>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Ospf Area/&lt;area_id&gt;</code>                                                                                                                                               |
| 3    | Add the OSPF export policy and set the <i>protocol</i> attribute.<br><br><code>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Ospf Export/&lt;export_policy_number&gt; protocol bgpMplsInternal</code>                                                        |
| 4    | If required, change the default for the equal cost multi-path (ECMP) setting.<br><br><code>add Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Ospf ecmpStatus &lt;ecmp&gt;</code>                                                                                    |
| 5    | Add point-to-point OSPF on an existing interface.<br><br><code>add Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; If/&lt;ip_address&gt; Ospfif ifType pointToPoint</code>                                                                                            |

---

--End--

---

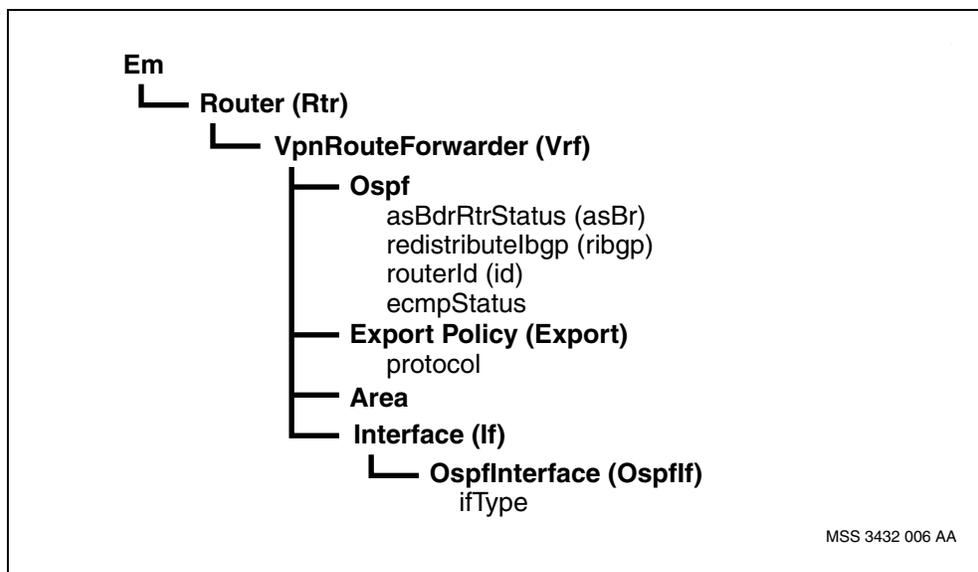


## Variable definitions

| Variable               | Value                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------------|
| <area_id>              | is the 32-bit IP address for the OSPF area in which the router is located.                          |
| <ecmp>                 | is the attribute that specifies if equal cost multi-path (ECMP) is enabled for OSPF learned routes. |
| <export_policy_number> | is the numeric designation assigned to the export policy.                                           |
| <router_id>            | is the IP address that uniquely identifies the router in an autonomous system.                      |
| <rtr_name>             | is the name of the router.                                                                          |
| <vrf_name>             | is the name of the VPN route forwarder.                                                             |

## Procedure job aid

### OSPF component hierarchy





## Configuring static routing

Configure static routing to allow the PE router to forward IP traffic to the CE router in cases where dynamic routing protocols are not being used between the CE and PE routers. This might also be done to address specific cases even when a dynamic routing protocol is in use.

### Procedure steps

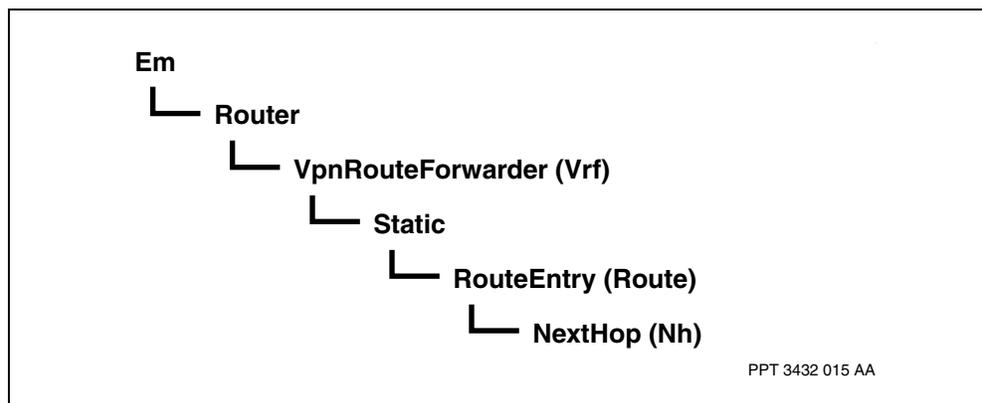
| Step    | Action                                                                                                                                                  |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1       | Add a static route.<br><br><pre>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Static RouteEntry/ &lt;ip_address&gt; Nexthop/&lt;ip_address&gt;</pre> |
| --End-- |                                                                                                                                                         |

### Variable definitions

| Variable     | Value                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------|
| <ip_address> | is the next hop IP address of the static route. The next hop IP address must belong to a local subnet that exists on the VRF. |
| <rtr_name>   | is the name of the router.                                                                                                    |
| <vrf_name>   | is the name of the VPN route forwarder.                                                                                       |

### Procedure job aid

#### Static routing component hierarchy





## Configuring RIP

Configure Routing Information Protocol (RIP) to exchange the set of address prefixes between the CE router and the PE router. Although EIGRP is the recommended access routing protocol, RIP is also supported.

### Procedure steps

---

| Step | Action                                                                                                                                                                                                            |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add the <i>Rip</i> component.<br><br><code>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Rip<br/>redistributeIbgp true</code>                                                                                  |
| 2    | Add <i>RipIf</i> component under the router interface.<br><br><code>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; If/&lt;ip_address&gt;<br/>Ripif</code>                                                       |
| 3    | Add the <i>Export</i> component and set the <i>protocol</i> attribute.<br><br><code>add -s Rtr/&lt;rtr_name&gt; vrf/&lt;vrf_name&gt; Rip Export/<br/>&lt;export_policy_number&gt; protocol bgpMplsInternal</code> |

---

--End--

---

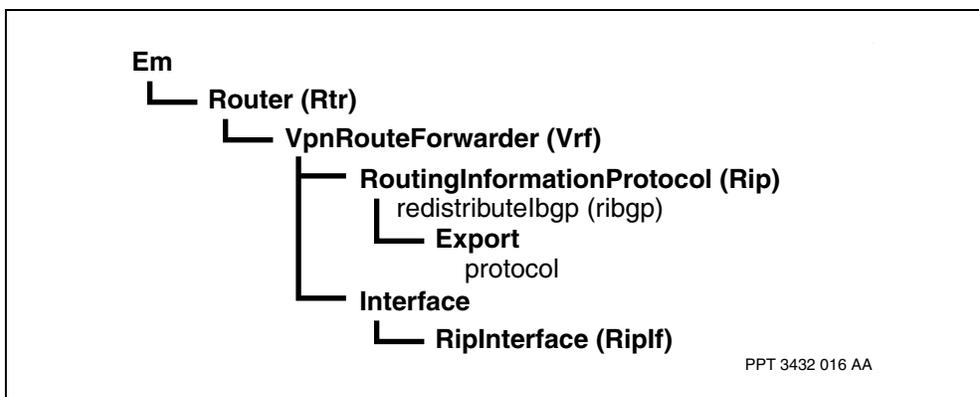


### Variable definitions

| Variable               | Value                                                     |
|------------------------|-----------------------------------------------------------|
| <export_policy_number> | is the numeric designation assigned to the export policy. |
| <ip_address>           | is the ip address of the interface.                       |
| <rtr_name>             | is the name of the router.                                |
| <vrf_name>             | is the name of the VPN route forwarder.                   |

### Procedure job aid

#### RIP component hierarchy





## Configuring a default static route in a scaled environment

Configure a default static route in a scale environment to prevent Forwarding Tables and MvRibs from growing to very large sizes without impacting reachability. Depending on scalability requirements (for example a large number of spokes) it is preferable to disable the dynamic routing protocol between the Export Hub and the Hub Site, and replace it with a default static route.

### Procedure steps

---

| Step | Action                                                                                                                                                                                                      |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add a default static route on your Export Hub which points to the Hub Site.<br><b>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;EH_vrf_name&gt; Static RouteEntry/0.0.0.0,0.0.0.0,0 Nexthop/&lt;nh_ip_address&gt;</b> |
| 2    | Disable dynamic routing between the Export Hub and the Hub Site (if using OSPF for dynamic routing).<br><b>del Rtr/&lt;rtr_name&gt; Vrf/&lt;EH_vrf_name&gt; If/&lt;if_ip_address&gt; OspfIf</b>             |

---

--End--

---

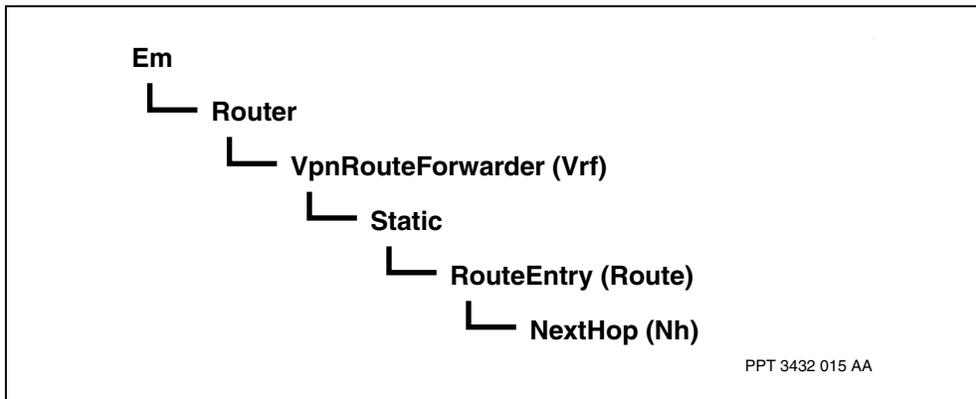


### Variable definitions

| Variables       | Value                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <EH_vrf_name>   | is the name of the VPN route forwarder. In this case, the Export Hub VRF.                                                                  |
| <if_ip_address> | is the IP address of the OSPF interface on the Export Hub which is connected to the Hub Site.                                              |
| <nh_ip_address> | is the next hop IP address of the static route. In this case, it must be the IP address of the Hub Site port connected to your Export Hub. |
| <rtr_name>      | is the name of the router.                                                                                                                 |

### Procedure job aid

#### Default static routing in a scaled environment component hierarchy





## Configuring the VRF export policy

Configure the VPN route forwarder (VRF) export policy to optionally control the redistribution of locally learned routes to remote PEs.

### Procedure steps

| Step | Action                                                                                                                                                                                                                                                                                                                                                   |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add the VRF export policy.<br><pre>add Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt;</pre>                                                                                                                                                                                                                          |
| 2    | Set the protocol.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt; protocol &lt;protocol&gt;</pre>                                                                                                                                                                                                         |
| 3    | Set the local preference value.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt; localPreference &lt;pref_value&gt;</pre>                                                                                                                                                                                  |
| 4    | Add the <i>Network</i> component, and set its prefix and length.<br><pre>add -s Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt; Network/&lt;net&gt; prefix<br/>&lt;net_prefix&gt;, length &lt;net_length&gt;</pre>                                                                                                    |
| 5    | Set the export advertiseStatus mode.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt; advertiseStatus &lt;mode&gt;</pre>                                                                                                                                                                                   |
| 6    | Optionally, set a regular expression to identify the AS path.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt; asPathExpression<br/>&lt;path_regularExpress&gt;</pre>                                                                                                                                      |
| 7    | Optionally, set a regular expression to identify the community.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt; communityExpression<br/>&lt;com_regularExpress&gt;</pre>                                                                                                                                  |
| 8    | If you configured a value in step 6 and step 7, you can optionally set the policy preference. The preference is used to break the tie if the matching criteria of two or more policies is the same.<br><pre>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt; Export/<br/>&lt;export_policy_number&gt; expressPreference<br/>&lt;express_prefValue&gt;</pre> |

--End--



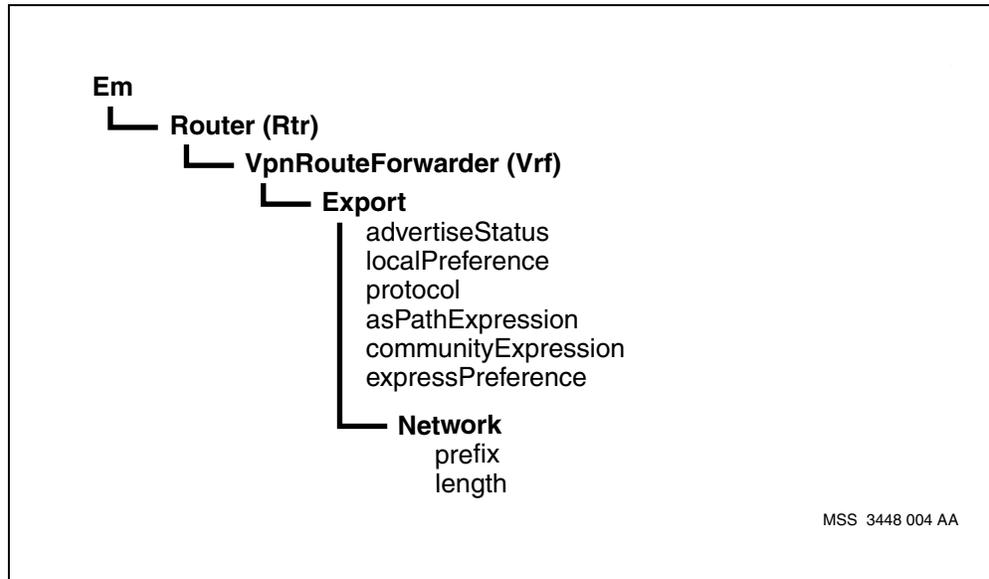
## Variable definitions

| Variable               | Value                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <com_regularExpress>   | is the expression that matches the route's community path attribute.                                                                                                                                                                                                                     |
| <export_policy_number> | is the numeric designation assigned to the export policy. Value is from 0 to 65535.                                                                                                                                                                                                      |
| <express_prefValue>    | is the attribute that specifies the relative preference of the policy which uses the keys asPathExpression and communityExpression.                                                                                                                                                      |
| <mode>                 | is send or block. The default is send.                                                                                                                                                                                                                                                   |
| <net>                  | is the identifier assigned to network. The network prefix, under the VRF export policy, can be used to further refine a filtering policy or to leak a specific subnet from the local VRF to remote PEs when all the remaining local prefixes are being blocked by a more generic policy. |
| <net_length>           | is the value assigned to the network length. Values from 1 to 32. Default is <system supplied>.                                                                                                                                                                                          |
| <net_prefix>           | is the value assigned to the network IP prefix.                                                                                                                                                                                                                                          |
| <path_regularExpress>  | is the expression that matches the route's AS path attribute.                                                                                                                                                                                                                            |
| <pref_value>           | is the value of localPreference. Values from 0 to 4294967295. Default is 0.                                                                                                                                                                                                              |
| <protocol>             | is the policy applies to routes learned from the specified protocol. Values all, rip, ospfInternal, ospfExternal, staticLocal, staticRemote, bgpExternal. Default is all.                                                                                                                |
| <rtr_name>             | is the name of the router.                                                                                                                                                                                                                                                               |
| <vrf_name>             | is the name of the VPN route forwarder.                                                                                                                                                                                                                                                  |



## Procedure job aid

### VRF export policy component hierarchy





## Configuring IP CPP on the VRF

Configure control plane protection (CPP) on the VRF to protect Nortel Multiservice Switch nodes against certain denial of service (DoS) attacks on the control plane by monitoring the flow rate of IP packets destined for local IP destination addresses (DAs).

---

**Attention:** CPP is supported on PQC-based FPs only.

---

### Prerequisites

- See the section on CPP in *NN10600-800 Nortel Multiservice Switch 7400/15000/20000 IP Technology Fundamentals*.
- The procedure in this section describes configuring CPP software and services only. Basic configuration at the node level (in this case, creating an instance of a logical processor type (LPT), and adding the *ip* and *ipCpp* services to the *featureList* attribute) must be performed first. Use the tasks and procedures in *NN10600-550 Nortel Multiservice Switch 7400/15000/20000 Common Configuration Procedures* if you require supporting information or need to provision or reconfigure any node or nodal elements to support the CPP feature.

### Procedure steps

---

| Step | Action                                                                                                                                                                    |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add a <i>Cpp</i> component as a subcomponent of the <i>Rtr</i> component.<br><b>add Rtr/&lt;rtr_name&gt; vrf/&lt;vrf_name&gt; cpp</b>                                     |
| 2    | Configure the number of packets per second before discard occurs.<br><b>set Rtr/&lt;rtr_name&gt; vrf/&lt;vrf_name&gt; cpp packetsPerSecond &lt;packets_per_second&gt;</b> |
| 3    | Configure the isolation time period.<br><b>set Rtr/&lt;rtr_name&gt; vrf/&lt;vrf_name&gt; cpp isolationTime &lt;isolation_time&gt;</b>                                     |
| 4    | Configure the grace period.<br><b>set Rtr/&lt;rtr_name&gt; vrf/&lt;vrf_name&gt; cpp gracePeriod &lt;grace_period&gt;</b>                                                  |
| 5    | Configure the CPP mode.<br><b>set Rtr/&lt;rtr_name&gt; vrf/&lt;vrf_name&gt; cpp mode &lt;cpp_mode&gt;</b>                                                                 |

---

--End--

---

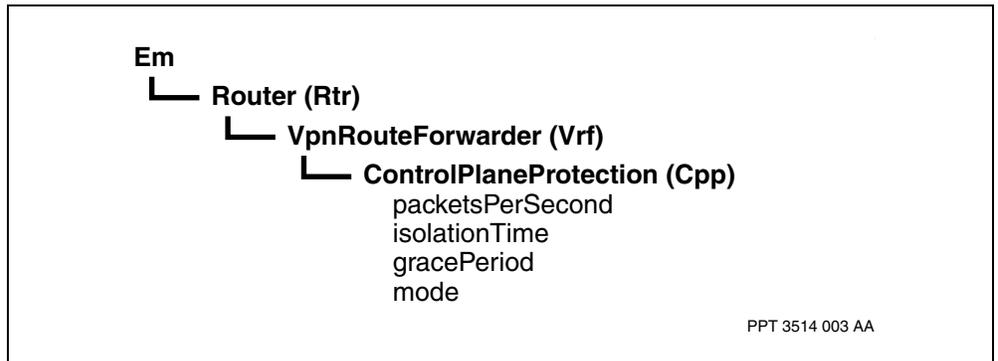


### Variable definitions

| Variable             | Value                                                                                                                                                                                                                                                                               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <cpp_mode>           | is the CPP operational mode: study, protect or disabled. Use study to determine an acceptable traffic rate. Once you learn the rate created and have the appropriate configuration, use protect. Use disabled to pre-configure the feature without enabling the monitoring process. |
| <grace_period>       | is the period over which the average flow rate is measured to ensure that the exceeded traffic flow rate still exceeds the maximum allowed rate. A value of zero in protect mode means that isolation occurs immediately after an excessive flow is detected.                       |
| <isolation_time>     | is the amount of time over which traffic will be discarded once isolation has begun. A value of zero indicates to permanently discard traffic until the card is cleared by an operator.                                                                                             |
| <packets_per_second> | is the flow rate, in packets per second, for the VR's DA, that must be exceeded on a single DA before discard processing occurs.                                                                                                                                                    |
| <rtr_name>           | is the name of the router.                                                                                                                                                                                                                                                          |
| <vrf_name>           | is the name of the VPN route forwarder.                                                                                                                                                                                                                                             |

### Procedure job aid

#### VRF IP CPP component hierarchy





## Configuring VRF route flood protection

Optionally, configure the VPN route forwarder (VRF) route flood protection to control the maximum number of IPv4 learned routes to be:

- exported from the VRF routing table to the router VPN routing information database
- imported into the VRF routing table from the router VPN routing information database

### Procedure steps

---

| Step | Action                                                                                                                                                        |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Set the VRF import alarm limit.<br><br><code>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt;<br/>importRoutesAlarmLimit &lt;import_alarm_limit&gt;</code>       |
| 2    | Set the VRF import discard limit.<br><br><code>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt;<br/>importRoutesDiscardLimit &lt;import_discard_limit&gt;</code> |
| 3    | Set the VRF export alarm limit.<br><br><code>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt;<br/>exportRoutesAlarmLimit &lt;export_alarm_limit&gt;</code>       |
| 4    | Set the VRF export discard limit.<br><br><code>set Rtr/&lt;rtr_name&gt; Vrf/&lt;vrf_name&gt;<br/>exportRoutesDiscardLimit &lt;export_discard_limit&gt;</code> |

---

--End--

---

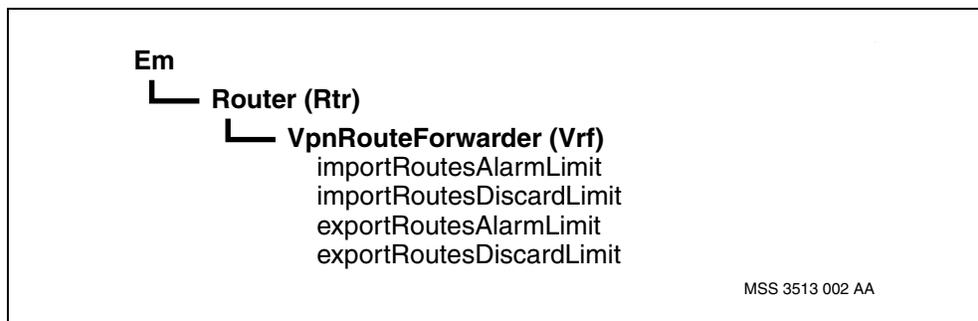


### Variable definitions

| Variable               | Value                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <export_alarm_limit>   | specifies the alarm threshold of number of routes to be exported from this VRF's routing table to the VPN routing database of the <i>Router</i> component. When the number of routes exported from this VRF reaches this limit, an alarm is generated and the VRF will continue exporting routes. |
| <export_discard_limit> | specifies the maximum number of routes to be exported from this VRF's routing table to the VPN routing database of the <i>Router</i> component. When the number of routes exported from this VRF reaches this limit, an alarm is generated and the VRF will stop exporting routes.                |
| <import_alarm_limit>   | specifies the alarm threshold of number of VPN routes to be imported to this VRF's routing table from the <i>Router</i> component. When the number of routes imported to this VRF reaches this limit, an alarm is generated and the VRF will continue importing routes.                           |
| <import_discard_limit> | specifies the maximum number of VPN routes to be imported to this VRF's routing table from the <i>Router</i> component. When the number of routes imported to this VRF reaches this limit, an alarm is generated and the VRF will stop importing routes.                                          |
| <rtr_name>             | is the name of the router.                                                                                                                                                                                                                                                                        |
| <vrf_name>             | is the name of the VPN route forwarder.                                                                                                                                                                                                                                                           |

### Procedure job aid

#### VRF route flood protection component hierarchy





---

## BGP/MPLS VPN configuration example

---

This section provides examples of configuring BGP/MPLS VPN. The diagram [Example figure for a BGP/MPLS VPN network configuration \(page 109\)](#) represents the network being used in these examples. In these example procedures, the Layer 1 and Layer 2 provisioning steps (for example, AtmIf, La, FrUni, etc.) are not described.

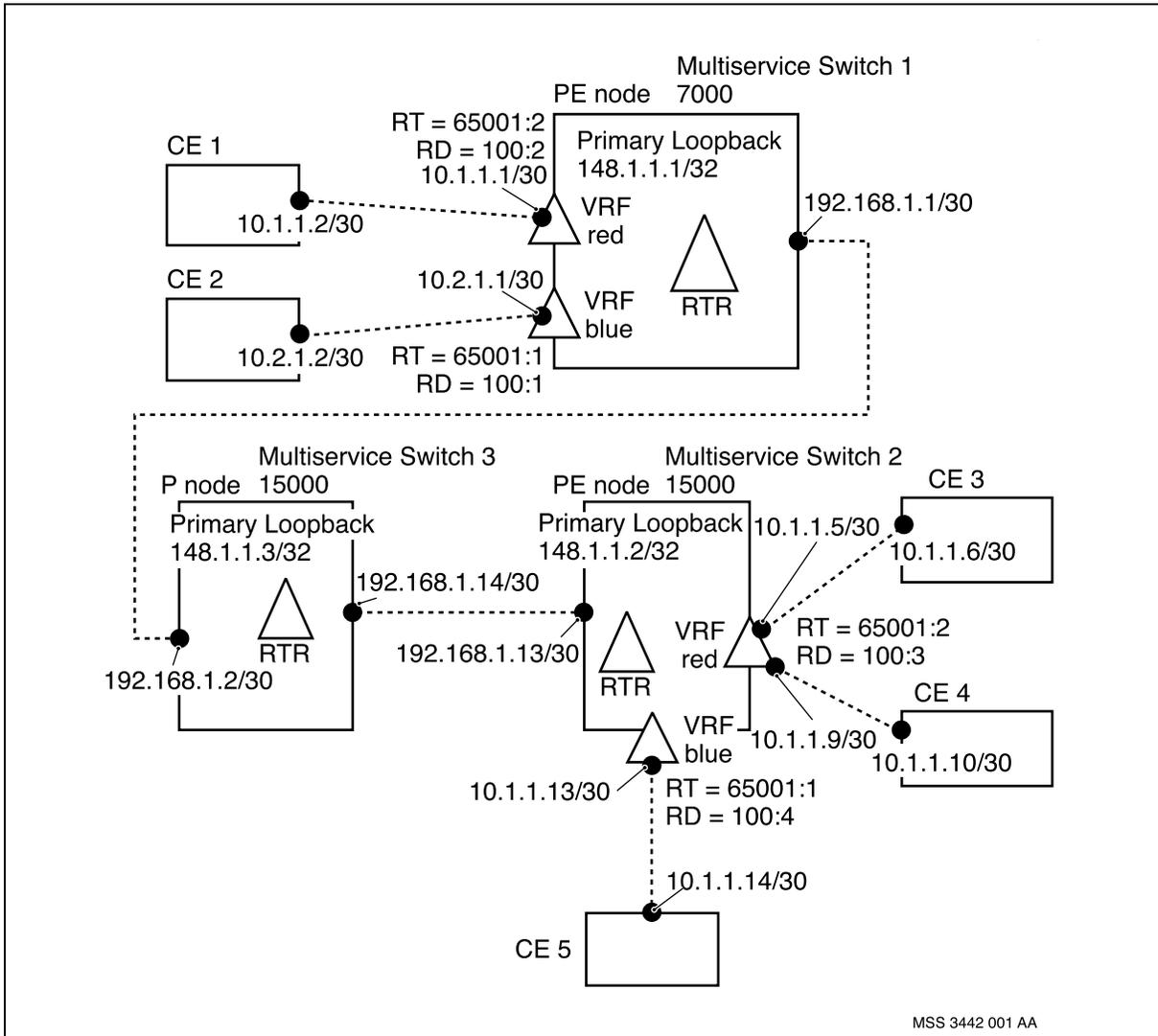
---

**Attention:** The following are example procedures. The values you use in your configuration can differ from the values shown here. Consult your network engineer to ensure the values you are using are accurate for your configuration.

---



**Example figure for a BGP/MPLS VPN network configuration**



MSS 3442 001 AA

**BGP/MPLS VPN configuration example navigation**

- [Example of a backbone configuration for PE node Multiservice Switch 1 \(Multiservice Switch 7400 node\) \(page 110\)](#)
- [Example of a backbone configuration for PE node Multiservice Switch 2 \(Multiservice Switch 15000 node\) \(page 116\)](#)
- [Example of configuring a P node on a Multiservice Switch 3 \(Multiservice Switch 15000 node\) \(page 121\)](#)
- [Example of configuring a BGP MED policy \(page 124\)](#)
- [Example of configuring a VRF policy \(page 126\)](#)
- [Example of configuring a route target export policy \(page 128\)](#)



---

## Example of a backbone configuration for PE node Multiservice Switch 1 (Multiservice Switch 7400 node)

### Procedure steps

| Step | Action                                                                                                                                                                                                                                                                                                                                                                         |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure RFC 2547 features.<br><pre>set sw lpt/CP featureList ! OamEnet bgp ip set sw lpt/VPNXC featureList ! rfc2547bis bgp ip set sw lpt/atm_trunk featureList ! mplsLdp atmmpc ip atmtrunks  check prov activate prov confirm prov</pre>                                                                                                                                   |
| 2    | For ATM PQC cards:<br><pre>add -s lp/&lt;atm_lp&gt; eng arc ov MulticastBranchesCapacity &lt;existing prov number + 4000&gt; add -s lp/&lt;atm_lp&gt; eng fcrc pqc set lp/&lt;atm_lp&gt; eng fcrc pqc ov ipRoutesPoolCapacity 64000 add -s lp/&lt;atm_lp&gt; eng fcrc ov subConnectionPoolCapacity 4096</pre>                                                                  |
| 3    | Configure the Router and the Primary Loopback Interface.<br><pre>add router/RTR1 VRP lp/&lt;VpnXc_LP&gt; add router/RTR1 If/148.1.1.1 netmask 255.255.255.255 add router/RTR1 If/148.1.1.1 loopback mode primaryLoopback</pre>                                                                                                                                                 |
| 4    | Configure AtmMpc Media for four emission priorities.<br><pre>add router/RTR1 If/192.168.1.1 netmask 255.255.255.252 add router/RTR1 If/192.168.1.1 atmMpc add atmif/&lt;x&gt; vcc/&lt;n.m1&gt; nep set router/RTR1 If/192.168.1.1 atmMpc Ac/1 atmConnection AtmIf/&lt;x&gt; Vcc/&lt;n.m1&gt; nep set AtmIf/&lt;x&gt; Vcc/&lt;n.m1&gt; Vcd Tm txPacketWiseDiscard enabled</pre> |



- 
- 5 Add an ATM connection with DiffServ connection class 1 and link it to an ATM VCC that is configured with the ATM nrtVBR service category.
- ```
add router/RTR1 If/192.168.1.1 atmMpe Ac/2 ipCos 1
set router/RTR1 If/192.168.1.1 atmMpe Ac/2 atmConnection
AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory
nrtvbr
set AtmIf/<x> Vcc/<n.m> Vcd Tm txPacketWiseDiscard
enabled
```
- 6 Add an ATM connection with DiffServ connection class 2 and link it to an ATM VCC that is configured with the ATM rtVBR service category.
- ```
add router/RTR1 If/192.168.1.1 atmMpe Ac/3 ipCos 2
set router/RTR1 If/192.168.1.1 atmMpe Ac/3 atmConnection
AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory
rtvbr
set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard
enabled
```
- 7 Add an ATM connection with DiffServ connection class 3 and link it to an ATM VCC that is configured with the ATM CBR service category.
- ```
add router/RTR1 If/192.168.1.1 atmMpe Ac/4 ipCos 3
set router/RTR1 If/192.168.1.1 atmMpe Ac/4 atmConnection
AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory
rtvbr
set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard
enabled
```
- 8 Configure OSPF as IGP.
- ```
add -s router/RTR1 ospf area/0.0.0.0
set router/RTR1 ospf routerId 148.1.1.1
add router/RTR1 If/148.1.1.1 ospfif ifType passive
```
- 9 Configure OSPF Interfaces.
- ```
add router/RTR1 If/192.168.1.1 ospfif ifType
pointToPoint
```
- 10 If you want ISIS as IGP, complete the following commands and [step 11](#):
- ```
add -s router/RTR1 isis Level/1
add router/RTR1 isis Net/47.0001.1480.0100.1001.00
```



- ```
add -s router/RTR1 If/148.1.1.1 isisif Level/1
set router/RTR1 If/148.1.1.1 isisif passive yes
```
- 11 Configure ISIS Interfaces.
- ```
add -s router/RTR1 If/192.168.1.1 isisif Level/1
```
- 12 Configure BGP.
- ```
add -s router/RTR1 Bgp localAs 1
set router/RTR1 Bgp bgpIdentifier 148.1.1.1
add -s router/RTR1 Bgp peer/148.1.1.2 desc peerAs 1
set router/RTR1 bgp peer/148.1.1.2 desc addressFamily
ipv4mplsvpn, lac 148.1.1.1
```
- 13 Configure LDP.
- ```
add router/RTR1 ldp
add router/RTR1 If/192.168.1.1 ldpif
```
- 14 Confirm configuration.
- ```
check prov
activate prov
confirm prov
```

--End--



Access Configuration for PE node Multiservice Switch 1 (Multiservice Switch 7400 node)

Procedure steps

Step	Action
1	Configure RFC 2547 feature set on access. <pre>set sw lpt/atm_access featureList ! rfc2547bis atmmpc ip check prov activate prov confirm prov</pre>
2	For ATM PQC cards: <pre>add -s lp/<atm_lp> eng fcrc pqc set lp/<atm_lp> eng fcrc pqc ov ipRoutesPoolCapacity 64000</pre>
3	Configure VRF. <pre>add -s router/RTR1 vrf/RED rd/100:2 add router/RTR1 vrf/RED rt/65001:2 add -s router/RTR1 vrf/BLUE rd/100:1 add router/RTR1 vrf/BLUE rt/65001:1</pre>
4	Configure Interfaces on VRF. <pre>add router/RTR1 vrf/RED If/10.1.1.1 netmask 255.255.255.252 add router/RTR1 vrf/BLUE If/10.2.1.1 netmask 255.255.255.252</pre>
5	Configure ATM access media for VPN RED. <pre>add router/RTR1 vrf/RED If/10.1.1.1 atmMpc</pre>
6	Link the Ac/1 subcomponent to an ATM VCC that is configured with the ATM UBR service category. <pre>set router/RTR1 vrf/RED if/10.1.1.1 atmMpc Ac/1 atmConnection AtmIf/x Vcc/<vpi.vci> nep set AtmIf/x Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard enabled</pre>
7	Link the Ac/2 subcomponent to an ATM VCC that is configured with the ATM nrtVBR service category. <pre>add router/RTR1 vrf/RED If/10.1.1.1 atmMpc Ac/2 ipCos 1</pre>



```
set router/RTR1 vrf/RED If/10.1.1.1 atmMpe Ac/2
atmConnection AtmIf/x Vcc/<vpi.vci> nep

set AtmIf/x Vcc/<vpi.vci> vcd tm atmServiceCategory
nrtvbr

set AtmIf/x Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard
enabled
```

- 8 Link the Ac/3 subcomponent to an ATM VCC that is configured with the ATM rtVBR service category.

```
add router/RTR1 vrf/RED If/10.1.1.1 atmMpe Ac/3 ipCos 2

set router/RTR1 vrf/RED If/10.1.1.1 atmMpe Ac/3
atmConnection AtmIf/x Vcc/<vpi.vci> nep

set AtmIf/x Vcc/<vpi.vci> vcd tm atmServiceCategory
rtvbr

set AtmIf/x Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard
enabled
```

- 9 Link the Ac/4 subcomponent to an ATM VCC that is configured with the ATM CBR service category.

```
add router/RTR1 vrf/RED If/10.1.1.1 atmMpe Ac/4 ipCos 3

set router/RTR1 vrf/RED If/10.1.1.1 atmMpe Ac/4
atmConnection AtmIf/x Vcc/n.m4 nep

set AtmIf/x Vcc/<vpi.vci> vcd tm atmServiceCategory cbr

set AtmIf/x Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard
enabled
```

- 10 Configure ATM access media for VPN BLUE. The same set of commands shown in [step 5](#) is required to configure ATM media on interface/10.2.1.1 for VPN BLUE. Exchange each instance of vrf/RED with vrf/BLUE.

- 11 Configure routing protocols on VRF.

- 12 Add EBGP on the VRF RED media.

```
add -s router/RTR1 vrf/RED bgp localAs 1, bgpIdentifier
10.1.1.1

add -s router/RTR1 vrf/RED bgp peer/10.1.1.2 desc peerAs
65101

add router/RTR1 vrf/RED bgp export/0 protocol
bgpMplsInternal
```

- 13 Add OSPF on the VRF BLUE media. This example assumes a point-to-point link.

```
add router/RTR1 vrf/BLUE ospf routerId 10.2.1.1, asbr
true, redistributeIbgp true

add router/RTR1 vrf/BLUE ospf area/0.0.0.0
```



```
add router/RTR1 vrf/BLUE ospf export/0 protocol
bgpMplsInternal

add router/RTR1 vrf/BLUE If/10.2.1.1 ospfif ifType
pointToPoint
```

14 Confirm configuration.

```
check prov
activate prov
confirm prov
```

--End--



Example of a backbone configuration for PE node Multiservice Switch 2 (Multiservice Switch 15000 node)

Procedure steps

Step	Action
1	Configure RFC 2547 features. <pre>set sw lpt/CP featureList ! OamEnet bgp ip set sw lpt/VPNXC featureList ! rfc2547bis bgp ip atmmp set sw lpt/gige_trunk featureList ! mplsLdp ip check prov activate prov confirm prov</pre>
2	Configure the Router and the Primary Loopback Interface. <pre>add router/RTR2 vrp lp/<VpnXc> add router/RTR2 If/148.1.1.2 netmask 255.255.255.255 add router/RTR2 If/148.1.1.2 loopback mode primaryLoopback</pre>
3	Configure GigE media. <pre>add router/RTR2 If/192.168.1.13 netmask 255.255.255.252 add router/RTR2 If/192.168.1.13 enet linkToEnetIf La/n</pre>
4	Configure OSPF as an IGP. <pre>add -s router/RTR2 ospf area/0.0.0.0 set router/RTR2 ospf routerId 148.1.1.2 add router/RTR2 If/148.1.1.2 ospfif ifType passive</pre>
5	Configure OSPF Interfaces. <pre>add router/RTR2 If/192.168.1.13 ospfif ifType pointToPoint</pre>
6	If you want ISIS as IGP, complete the following commands and step 7 : <pre>add -s router/RTR2 isis Level/1 add router/RTR2 isis Net/47.0001.1480.0100.1002.00 add -s router/RTR2 If/148.1.1.2 isisIf Level/1 set router/RTR2 If/148.1.1.2 isisIf passive yes</pre>
7	Configure ISIS Interfaces.



- add -s router/RTR2 If/192.168.1.13 isisif Level/1**
- 8** Configure BGP.
- add -s router/RTR2 Bgp localAs 1**
- set router/RTR2 bgp bgpIdentifier 148.1.1.2**
- add -s router/RTR2 bgp peer/148.1.1.1 desc peerAs 1**
- set router/RTR2 bgp peer/148.1.1.1 desc addressFamily
ipv4mplsvpn, lac 148.1.1.2**
- 9** Configure LDP.
- add router/RTR2 ldp**
- add router/RTR2 If/192.168.1.13 ldpif**
- 10** Confirm configuration.
- check prov**
- activate prov**
- confirm prov**

--End--



Access Configuration for PE node Multiservice Switch 2 (Multiservice Switch 15000 node)

Procedure steps

Step	Action
1	Configure RFC 2547 feature set on access. <pre>set sw lpt/atm_access featureList ! rfc2547bis atmMpe ip set sw lpt/frameRelay_access featureList ! rfc2547bis frameRelayUni frUniIpOptimized ip check prov activate prov confirm prov</pre>
2	For ATM PQC cards: <pre>add -s lp/<atm_lp> eng fcrc pqc set lp/<atm_lp> eng fcrc pqc ov ipRoutesPoolCapacity 64000</pre>
3	Configure VRF. <pre>add -s router/RTR2 vrf/RED rd/100:3 add router/RTR2 vrf/RED rt/65001:2 add -s router/RTR2 vrf/BLUE rd/100:4 add router/RTR2 vrf/BLUE rt/65001:1</pre>
4	Configure Interfaces. <pre>add router/RTR2 vrf/RED If/10.1.1.5 netmask 255.255.255.252 add router/RTR2 vrf/RED If/10.1.1.9 netmask 255.255.255.252 add router/RTR2 vrf/BLUE If/10.2.1.13 netmask 255.255.255.252</pre>
5	Configure ATM access media for VPN RED. <pre>add router/RTR2 vrf/RED If/10.1.1.5 atmMpe</pre>
6	Link the Ac/1 subcomponent to an ATM VCC that is configured with the ATM UBR service category. <pre>set router/RTR2 vrf/RED if/10.1.1.5 atmMpe Ac/1 atmConnection AtmIf/<x> Vcc/<vpi.vci> nep</pre>



- set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard enabled**
- 7 Link the Ac/2 subcomponent to an ATM VCC that is configured with the ATM nrtVBR service category.
- ```
add router/RTR2 vrf/RED If/10.1.1.5 atmMpe Ac/2 ipCos 1
set router/RTR2 vrf/RED If/10.1.1.5 atmMpe Ac/2
atmConnection AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory nrtvbr
set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard enabled
```
- 8 Link the Ac/3 subcomponent to an ATM VCC that is configured with the ATM rtVBR service category.
- ```
add router/RTR2 vrf/RED If/10.1.1.5 atmMpe Ac/3 ipCos 2  
set router/RTR2 vrf/RED If/10.1.1.5 atmMpe Ac/3  
atmConnection AtmIf/<x> Vcc/<vpi.vci> nep  
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory rtvbr  
set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard enabled
```
- 9 Link the Ac/4 subcomponent to an ATM VCC that is configured with the ATM CBR service category.
- ```
add router/RTR2 vrf/RED If/10.1.1.5 atmMpe Ac/4 ipCos 3
set router/RTR2 vrf/RED If/10.1.1.5 atmMpe Ac/4
atmConnection AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory cbr
set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard enabled
```
- 10 Configure second ATM access media for VPN RED. The same set of commands shown in [step 5](#) is required to configure ATM media on interface/10.1.1.9 for VPN RED.
- 11 Configure Frame relay access media for VPN BLUE.
- ```
add router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlci  
set FrUni/x numberOfEmissionsQs 4  
set FrUni/<fruni_inst> Dlci/<dlci> IpConn  
dpToDeMapLevel/<level>  
set router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlci Frc/1  
linkToFrDlci Fruni/<x> Dlci/<dlci> IpConnection
```



- 12 Add a frame relay connection for DiffServ connection class 1 and link it to another DlcI subcomponent of the same Fruni component. The DlcI for Frc/2 is configured for better QoS in the FR network than Frc/1.

```
add router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlcI Frc/2
ipCos 1
```

```
set router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlcI Frc/2
linkToFrDlcI Fruni/<x> DlcI/<dlci> IpConnection
```

- 13 Add a frame relay connection for DiffServ connection class 2 and link it to another DlcI subcomponent of the same Fruni component. The DlcI for Frc/3 is configured for better QoS in the FR network than Frc/2.

```
add router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlcI Frc/3
ipCos 2
```

```
add router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlcI Frc/3
linkToFrDlcI Fruni/<x> DlcI/<dlci> IpConnection
```

- 14 Add a frame relay connection for DiffServ connection class 3 and link it to another DlcI subcomponent of the same Fruni component. The DlcI for Frc/4 is configured for better QoS in the FR network than Frc/3.

```
add router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlcI Frc/4
ipCos 3
```

```
set router/RTR2 vrf/BLUE If/10.2.1.13 IpoDlcI Frc/4
linkToFrDlcI Fruni/<x> DlcI/<dlci> IpConnection
```

- 15 Configure access Routing protocols.

- 16 Add static routes for interfaces 10.1.1.5 and 10.1.1.9.

```
add -s router/RTR2 vrf/RED static route/N1 nexthop/
10.1.1.6
```

```
add -s router/RTR2 vrf/RED static route/N2 nexthop/
10.1.1.10
```

- 17 Add RIP for interface 10.2.1.13.

```
add -s router/RTR2 vrf/BLUE rip redistributeIbgp true
```

```
add -s router/RTR2 vrf/BLUE If/10.2.1.13 ripif
```

```
add -s router/RTR2 vrf/BLUE rip export/0 protocol
bgpMplsInternal
```

- 18 Confirm configuration.

```
check prov
```

```
activate prov
```

```
confirm prov
```

--End--



Example of configuring a P node on a Multiservice Switch 3 (Multiservice Switch 15000 node)

Procedure steps

Step	Action
1	<p>Configure RFC 2547 features.</p> <pre>set sw lpt/CP featureList ! OamEnet set sw lpt/atm_trunk featureList ! mplsLdp ip atmmpc atmTrunks check prov activate prov confirm prov add -s lp/<atm_lp> eng arc ov MulticastBranchesCapacity <existing prov number + 4K> add -s lp/<atm_lp> eng fcrc pqc ov ipRoutesPoolCapacity 64000 add -s lp/<atm_lp> eng fcrc ov subConnectionPoolCapacity 4096 set sw lpt/GigE_trunk featureList ! mplsLdp ip</pre>
2	<p>Configure the Router and Primary Loopback Interface.</p> <pre>add router/RTR3 VRP lp/<VpnXc_LP> add router/RTR3 Interface/148.1.1.3 netmask 255.255.255.255 add router/RTR3 If/148.1.1.3 loopback mode primaryLoopback</pre>
3	<p>Configure Interfaces.</p> <pre>add router/RTR3 If/192.168.1.2 netmask 255.255.255.252 add router/RTR3 If/192.168.1.14 netmask 255.255.255.252</pre>
4	<p>Configure OSPF as IGP.</p> <pre>add -s router/RTR3 ospf area/0.0.0.0 set router/RTR3 ospf routerId 148.1.1.3 add router/RTR3 If/148.1.1.3 ospfif ifType passive</pre>
5	<p>Configure OSPF Interfaces.</p> <pre>add router/RTR3 If/192.168.1.2 ospfif ifType pointToPoint</pre>



- ```
add router/RTR3 If/192.168.1.14 ospfif ifType
pointToPoint
```
- 6 If you want ISIS as IGP, complete the following commands and [step 7](#):
- ```
add -s router/RTR3 isis Level/1
add router/RTR3 isis Net/47.0001.1480.0100.1003.00
add -s router/RTR3 If/148.1.1.3 isisif Level/1
set router/RTR3 If/148.1.1.3 isisif passive yes
```
- 7 Configure ISIS Interfaces.
- ```
add -s router/RTR3 If/192.168.1.2 isisif Level/1
add -s router/RTR3 If/192.168.1.14 isisif Level/1
```
- 8 Configure LDP.
- ```
add router/RTR3 ldp
add router/RTR3 If/192.168.1.2 ldpiif
add router/RTR3 If/192.168.1.14 ldpiif
```
- 9 Configure ATM media for four emission priorities.
- ```
add router/RTR3 If/192.168.1.2 atmMpe
set router/RTR3 If/192.168.1.2 atmMpe Ac/1 atmConnection
AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<n.m> vcd tm atmServiceCategory ubr
set AtmIf/<x> Vcc/<n.m> Vcd Tm txPacketWiseDiscard
enabled
```
- 10 Add an ATM connection with DiffServ connection class 1 and link it to an ATM VCC that is configured with the ATM nrtVBR service category.
- ```
add router/RTR3 If/192.168.1.2 atmMpe Ac/2 ipCos 1
set router/RTR3 If/192.168.1.2 atmMpe Ac/2 atmConnection
AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory
nrtvbr
set AtmIf/<x> Vcc/<n.m> Vcd Tm txPacketWiseDiscard
enabled
```
- 11 Add an ATM connection with DiffServ connection class 2 and link it to an ATM VCC that is configured with the ATM rtVBR service category.
- ```
add router/RTR3 If/192.168.1.2 atmMpe Ac/3 ipCos 2
set router/RTR3 If/192.168.1.2 atmMpe Ac/3 atmConnection
AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory
rtvbr
```



- ```
set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard
enabled
```
- 12 Add an ATM connection with DiffServ connection class 3 and link it to an ATM VCC that is configured with the ATM CBR service category.
- ```
add router/RTR3 If/192.168.1.2 atmMpe Ac/4 ipCos 3
set router/RTR3 If/192.168.1.2 atmMpe Ac/4 atmConnection
AtmIf/<x> Vcc/<vpi.vci> nep
set AtmIf/<x> Vcc/<vpi.vci> vcd tm atmServiceCategory
rtvbr
set AtmIf/<x> Vcc/<vpi.vci> Vcd Tm txPacketWiseDiscard
enabled
```
- 13 Configure GigE media.
- ```
add -s router/RTR3 If/192.168.1.14 enet linkToEnetIf La/
n
```
- 14 Confirm configuration.
- ```
check prov
activate prov
confirm prov
```

---

--End--

---



## Example of configuring a BGP MED policy

This is an example procedure for configuring a BGP multi exit discriminator (MED) policy on the PE nodes such that the access link between CE4 and Multiservice Switch 2 is preferred over the access link between CE4 and Multiservice Switch 1. For redundancy purposes, CE4 is connected to VRF RED on both Multiservice Switch 1 and Multiservice Switch 2. The diagram [Example figure for an export policy network configuration \(page 127\)](#) represents the network being used in the following example.

### Procedure steps

| Step | Action                                                                                                                                                                                              |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure the eBGP peers between CE and PE on Multiservice Switch 2.<br><pre>add -s router/RTR2 vrf/RED bgp localAs 1<br/>add -s router/RTR2 vrf/RED bgp peer/10.1.1.10 desc<br/>peerAs 65001</pre> |
| 2    | Add the BGP export policy on Multiservice Switch 2 and set the MED value lower than that of Multiservice Switch 1.                                                                                  |

**Attention:** A lower MED value is preferable to a higher MED value.

- ```
add -s router/RTR2 vrf/RED bgp export/0 protocol  
bgpMplsInternal, med 100  
set router/RTR2 vrf/RED bgp export/0 peerIpAddress  
10.1.1.10
```
- 3 For redundancy purposes, add another Interface with AtmMpe media on Vrf RED on Multiservice Switch 1.
- ```
add -s router/RTR1 vrf/RED if/10.1.1.13 netmask
255.255.255.252
add -s router/RTR1 vrf/RED if/10.1.1.13 atmMpe
atmConnection AtmIf/<x> Vcc/<vpi.vci> nep
```
- 4 Configure the peers between CE to PE links on Multiservice Switch 1.
- ```
add -s router/RTR1 vrf/RED bgp localAs 1  
add -s router/RTR1 vrf/RED bgp peer/10.1.1.14 desc  
peerAs 65001
```
- 5 Add the BGP export policy on Multiservice Switch 1 and set the MED value higher than that of Multiservice Switch 2.
- ```
add -s router/RTR1 vrf/RED bgp export/0 protocol
bgpMplsInternal, med 200
```



```
set router/RTR1 vrf/RED bgp export/0 peerIpAddress
10.1.1.14
```

6 Confirm configuration.

```
check prov
```

```
activate prov
```

```
confirm prov
```

---

**Attention:** For routes learned across the MPLS backbone, CE4 will prefer the ones learned via Multiservice Switch 2 because the MED attached to these routes is lower. If Multiservice Switch 2 stops advertising these routes, or the eBGP peer fails, routes learned from Multiservice Switch 1 will be used.

---

---

--End--

---



## Example of configuring a VRF policy

This is an example procedure for configuring a VRF export policy to advertise a local preference for routes received from CE via eBGP. The diagram [Example figure for an export policy network configuration \(page 127\)](#) represents the network being used in the following example.

### Procedure steps

| Step | Action                                                                                                                                                                   |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Set the protocol and local preference.<br><br><code>add -s router/RTR1 vrf/RED export/1 protocol ebgp, localPreference 140, mode send</code>                             |
| 2    | Add the <i>Network</i> component and set its prefix and length.<br><br><code>add s- router/RTR1 vrf/RED export/1 network/1 prefix &lt;ip_address X&gt;, length 24</code> |
| 3    | Confirm the configuration.<br><br><code>check prov</code><br><code>activate prov</code><br><code>confirm prov</code>                                                     |
| 4    | Set the protocol and local preference.<br><br><code>add -s router/RTR2 vrf/RED export/1 protocol ebgp, localPreference 200, mode send</code>                             |
| 5    | Add the <i>Network</i> component and set its prefix and length.<br><br><code>add -s router/RTR2 vrf/RED export/1 network/1 prefix &lt;ip_address X&gt;, length 24</code> |
| 6    | Confirm the configuration.<br><br><code>check prov</code><br><code>activate prov</code><br><code>confirm prov</code>                                                     |

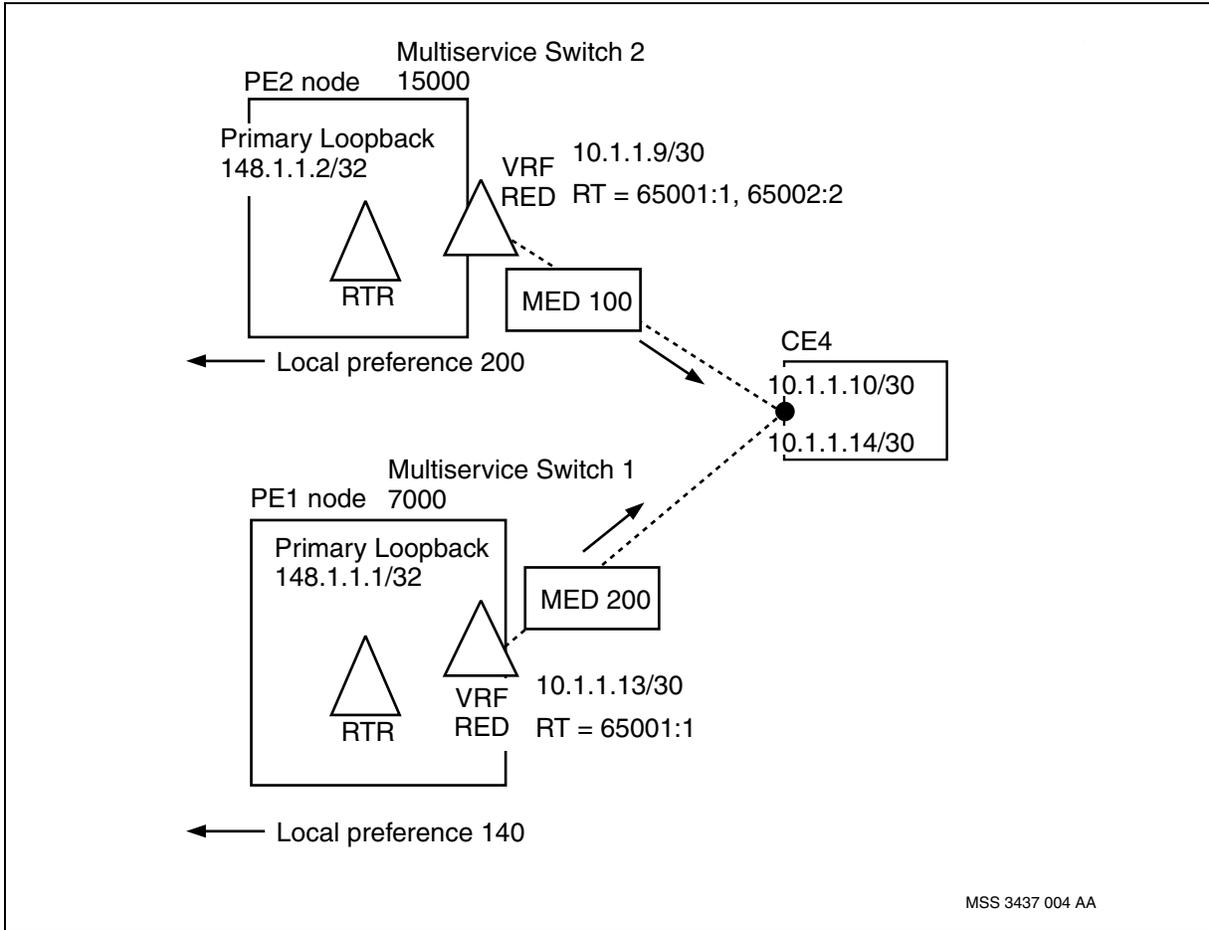
**Attention:** Remote VRFs of VPN RED receive route X from both PE1 and PE2; they will prefer PE2 (higher local preference = 200). If route X stops being advertised from VRF RED on PE2 but it is still advertised from VRF RED on PE1 (local preference = 140), traffic destined to X is redirected to PE1.

--End--



### Procedure job aid

#### Example figure for an export policy network configuration





---

## Example of configuring a route target export policy

This is an example procedure for configuring a route target export policy on the PE node to block VPN IPv4 routes based on route targets to be advertised to a specific peer. The diagram [Example figure for an export policy network configuration \(page 127\)](#) represents the network being used in the following example.

### Procedure steps

---

| Step | Action                                                                                                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add the BGP export policy on the Multiservice Switch 2 and set the <i>addressFamily</i> attribute to match the VPN IPv4 addresses.<br><br><b>add Rtr/RTR2 Bgp Export/0 af ipv4MplsVpn</b> |
| 2    | Set the route targets.<br><br><b>set Rtr/RTR2 Bgp Export/0 rt 65001:1, 65002:2</b>                                                                                                        |
| 3    | Specify the <i>peerIpAddress</i> attribute to which the policy applies to.<br><br><b>set Rtr/RTR2 Bgp Export/0 peerIpAddress x.x.x.x</b>                                                  |
| 4    | Specify the action to take on the policy match by setting the <i>advertiseStatus</i> attribute.<br><br><b>set Rtr/RTR2 Bgp Export/0 advertiseStatus block</b>                             |

---

--End--

---



---

# VCG-based IP VPN configuration

---

Configure a VCG-based IP VPN to:

- aggregate different customer networks over a common backbone connection
- provide a customer site access to a VPN

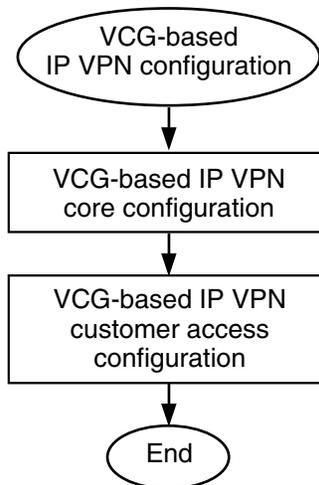
## Prerequisites to VCG-based IP VPN configuration

- Nortel Multiservice Switch IP services must be installed as described in NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.

## VCG-based IP VPN tasks

This work flow shows you the sequence of tasks you perform to configure a VCG-based IP VPN. To link to any task, go to [VCG-based IP VPN configuration task navigation \(page 130\)](#).

### VCG-based IP VPN configuration tasks



MSS 3541 007 AA



**VCG-based IP VPN configuration task navigation**

- [VCG-based IP VPN core configuration \(page 131\)](#)
- [VCG-based IP VPN customer access configuration \(page 146\)](#)



---

## VCG-based IP VPN core configuration

---

Configure a VCG-based IP VPN core configuration to aggregate different customer networks over a common backbone connection.

### Prerequisites to VCG-based IP VPN core configuration

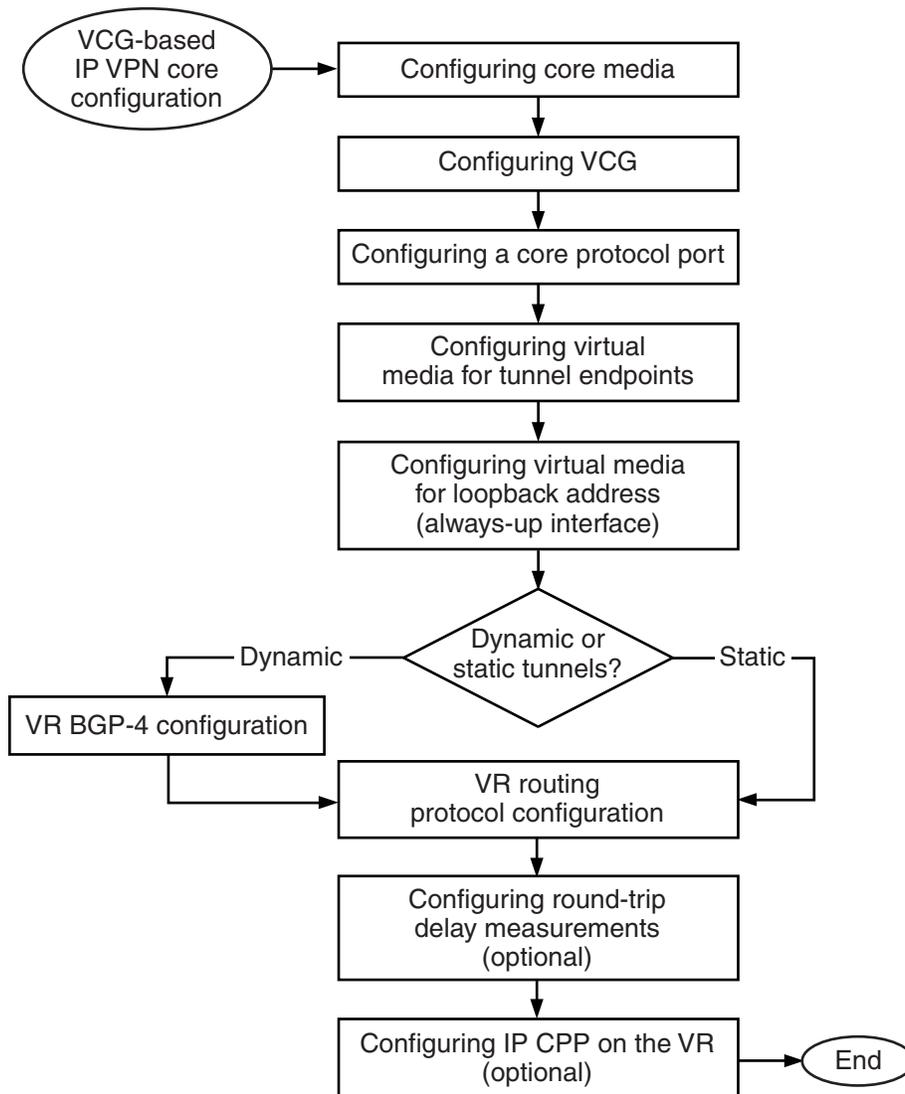
- Nortel Multiservice Switch IP services must be installed as described in NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- The task flow and procedures in this section describe configuring VCG-based IP VPN core configuration services only. Basic configuration (in this case, creating an instance of a logical processor type (LPT), and adding the services to the *featureList* component) must be performed first. Use the tasks and procedures in NN10600-060 *Nortel Multiservice Switch 7400/15000/20000 Component Reference* if you require supporting information or need to provision or reconfigure any node or nodal elements to support VCG-based IP VPN features.
  - For the CP card, include the mvr bgp ip software feature in the featurelist.
  - For the ATM card, include the atmmpc ip software feature in the featurelist.

### VCG-based IP VPN core configuration procedures

This task flow shows you the sequence of procedures you perform to configure a VCG-based IP VPN core configuration. To link to any procedure go to [VCG-based IP VPN core configuration procedure navigation \(page 132\)](#).



**VCG-based IP VPN core configuration procedures**



MSS 3514 006 AA

**VCG-based IP VPN core configuration procedure navigation**

- [Configuring core media \(page 134\)](#)
- [Configuring VCG \(page 136\)](#)
- [Configuring a core protocol port \(page 137\)](#)
- [Configuring virtual media for tunnel endpoints \(page 139\)](#)
- Configuring virtual media for loopback address, always-up interface. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.



- VR BGP-4 configuration. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- VR routing protocol configuration. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- [Configuring round-trip delay measurements \(page 141\)](#)
- Configuring IP CPP on the VR. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.



---

## Configuring core media

Configure core media to build the VPN backbone to interconnect the VCGs.

### Prerequisites

- You must configure an *AtmIf* prior to configuring core media. See the Configuring an *AtmIf* procedure in NN10600-710 *Nortel Multiservice Switch 7400/15000/20000 ATM Configuration Management*.

### Procedure steps

---

| Step | Action                                                                                                                                                                                            |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add the <i>VirtualChannelConnection</i> and <i>NailedUpEndPoint</i> subcomponents to the <i>AtmInterface</i> component.<br><b>add AtmIf/&lt;atmif_value&gt; Vcc/&lt;vpi.vci&gt; Nep</b>           |
| 2    | Add the <i>AtmMultiprotocolEncapsulation</i> component.<br><b>add AtmMpe/&lt;atmmpe_value&gt;</b>                                                                                                 |
| 3    | Link the <i>AtmMpe Ac</i> components to the <i>AtmIf Vcc</i> components.<br><b>set AtmMpe/&lt;atmmpe_value&gt; Ac/&lt;ac_id&gt; AtmCon AtmIf/<br/>&lt;atmif_value&gt; Vcc/&lt;vpi.vci&gt; Nep</b> |

---

--End--

---

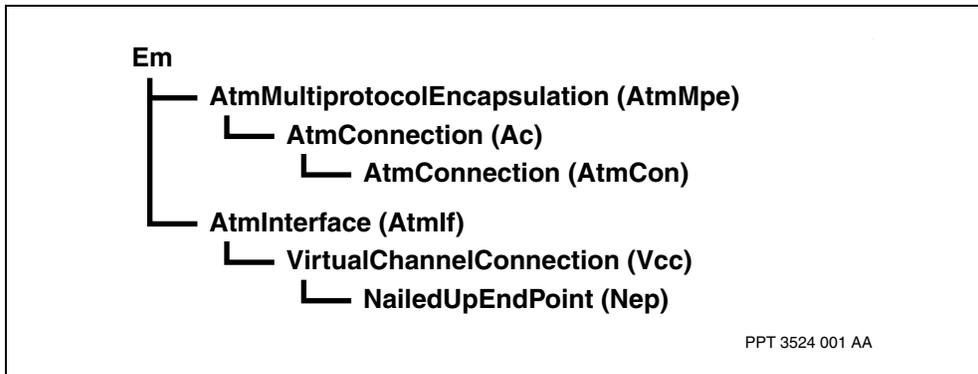


### Variable definitions

| Variable       | Value                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ac_id>        | is the instance value of the atm connection. Any mnemonic (for example, AC/1).                                                                                                                                                                                                                                                                                                               |
| <atmif_value>  | is the instance value of the <i>AtmIf</i> component.                                                                                                                                                                                                                                                                                                                                         |
| <atmmpe_value> | is the logical interface between the virtual router and ATM media ( <i>AtmIf</i> component).                                                                                                                                                                                                                                                                                                 |
| <vpi.vci>      | is the identifier assigned to the VP and VC of the virtual channel. It is a good practice to assign the vci value of the atm connection to the ac_id (example: set Router/<rtr_name> Vrf/<vrf_name> If/<ip_address> AtmMpe Ac/40 atmConnection AtmIf/<n> Vcc/0.40 Nep. It is the ac_id that is displayed in the ARP table for the IP address mapping to the layer 2 attribute (inverse ARP). |

### Procedure job aid

#### Core media component hierarchy





## Configuring VCG

Configure a virtual connection gateway (VCG) to connect customer sites through a VPN.

### Procedure steps

| Step | Action                                                                                                                                       |
|------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add a virtual router (VR).<br><code>add Vr/&lt;vr_name&gt;</code>                                                                            |
| 2    | Set the logical processor (LP) on which the virtual router processor resides.<br><code>set Vr/&lt;vr_name&gt; vrp Lp/&lt;lp_value&gt;</code> |
| 3    | Set the <i>vpnMode</i> attribute to carrier to define this virtual router as a VCG.<br><code>set Vr/&lt;vr_name&gt; vpnm carrier</code>      |
| 4    | Add the IP protocol to the VR.<br><code>add Vr/&lt;vr_name&gt; ip</code>                                                                     |

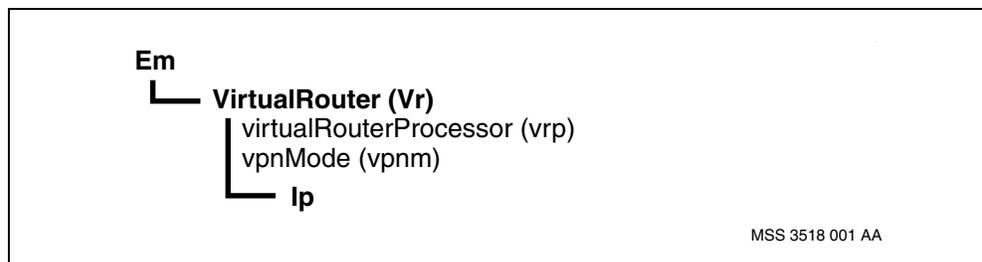
--End--

### Variable definitions

| Variable   | Value                                  |
|------------|----------------------------------------|
| <lp_value> | is the value of the logical processor. |
| <vr_name>  | is the name of the virtual router.     |

### Procedure job aid

#### VCG component hierarchy





---

## Configuring a core protocol port

Configure a core protocol port to link the physical backbone interface to the VCG virtual router.

### Procedure steps

---

| Step | Action                                                                                                                                                                                                    |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add a core protocol port.<br><code>add Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt;</code>                                                                                                                      |
| 2    | Link the protocol port to the media application.<br><code>set Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt; media AtmMpe/<br/>&lt;atmmpe_value&gt;</code>                                                        |
| 3    | Add the <i>IpPort</i> component which contains IP attributes specific to this port.<br><code>add Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt; IpPort</code>                                                     |
| 4    | Add the <i>IpLogicalInterface</i> component.<br><code>add Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt; IpPort LogicalIf/<br/>&lt;ippport_address&gt;</code>                                                     |
| 5    | Set the subnet mask for this logical interface.<br><code>set Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt; IpPort LogicalIf/<br/>&lt;ippport_address&gt; netMask &lt;netmask_address&gt;</code>                  |
| 6    | Set the broadcast address for this logical interface.<br><code>set Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt; IpPort LogicalIf/<br/>&lt;ippport_address&gt; broadcastAddress &lt;broadcast_address&gt;</code> |

---

--End--

---

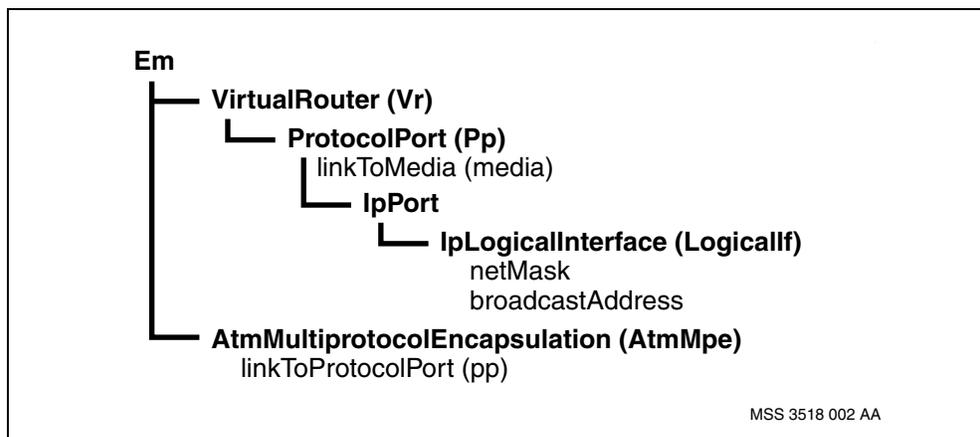


## Variable definitions

| Variable            | Value                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------|
| <atmmpe_value>      | is the logical interface between the virtual router and ATM media ( <i>AtmIf</i> component). |
| <broadcast_address> | is the IP address of the broadcast address for this <i>LogicalIf</i> component.              |
| <ipport_address>    | is the IP address of this IpPort on an IP network.                                           |
| <netmask_address>   | is the IP address of the subnet mask for this <i>LogicalIf</i> component.                    |
| <pp_value>          | is the logical interface to the network.                                                     |
| <vr_name>           | is the name of the virtual router.                                                           |

## Procedure job aid

### Core protocol port component hierarchy





## Configuring virtual media for tunnel endpoints

Configure virtual media for tunnel endpoints to define the customer tunnel address to access the VPN.

### Procedure steps

| Step | Action |
|------|--------|
|------|--------|



#### CAUTION

##### Risk of service interruption

The virtual media interface for tunnel endpoints must be different than the virtual media interface for loopback address. To configure the virtual media for loopback address, refer to NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.

- 1 Add a virtual media (VM).  
`add Vm/<vm_value>`
- 2 Set the mode of operation as `alwaysUpSummaryInterface` for the virtual media interface.  
`set Vm/<vm_value> Interface/0 mode alwaysUpSummaryInterface`
- 3 Add a protocol port.  
`add Vr/<vr_name> Pp/<pp_value>`
- 4 Link the protocol port to the media application.  
`set Vr/<vr_name> Pp/<pp_value> media Vm/<vm_value> Interface/0`
- 5 Add the `IpPort` component which contains IP attributes specific to this port.  
`add Vr/<vr_name> Pp/<pp_value> IpPort`
- 6 Add the `IpLogicalInterface` component. Add the network address logical interface.  
`add Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/<ipport_address>`
- 7 Set the subnet mask for this logical interface.  
`set Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/<ipport_address> netMask/<netmask_address>`
- 8 Set the broadcast address for this logical interface.  
`set Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/<ipport_address> broadcastAddress <broadcast_address>`
- 9 Activate changes. See [Activating configuration changes \(page 161\)](#).



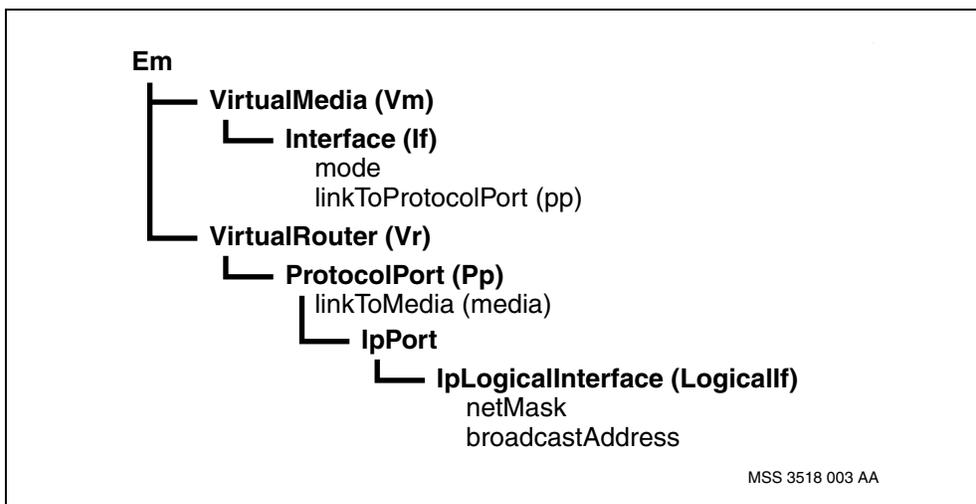
--End--

### Variable definitions

| Variable            | Value                                                                           |
|---------------------|---------------------------------------------------------------------------------|
| <broadcast_address> | is the IP address of the broadcast address for this <i>LogicalIf</i> component. |
| <ipport_address>    | is the IP address of the single IpPort on a logical IP network.                 |
| <netmask_address>   | is the IP address of the subnet mask for this <i>LogicalIf</i> component.       |
| <pp_value>          | is the logical interface to the network.                                        |
| <vm_value>          | is an instance of a logical media.                                              |
| <vr_name>           | is the name of the virtual router.                                              |

### Procedure job aid

#### Virtual media for tunnel endpoints component hierarchy





---

## Configuring round-trip delay measurements

Configure round-trip delay measurements to measure how long it takes for a packet to travel from a host to a remote end and back again.

### Prerequisites

Ensure that the BGP router ID is the same as the BGP loopback address, which is an always-up IP interface (for example, the IP address of a virtual media protocol port where the mode is set to alwaysUpInterface).

### Procedure steps

---

| Step | Action                                                                                                                                                                                                                                                                                                        |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure round-trip delay (RTD) measurements.<br><b>add Vr/&lt;vr_name&gt; Ip Rtd</b>                                                                                                                                                                                                                        |
| 2    | Set the <i>rtdDstAddrList</i> component.<br><b>set Vr/&lt;vr_name&gt; Ip Rtd dst &lt;ip_address&gt;</b>                                                                                                                                                                                                       |
| 3    | Enable spooling for the RTD statistics. If you do not enable statistics spooling, you cannot gather ongoing information for historical reporting purposes.<br><b>set Col/&lt;collector_value&gt; Sp spool on</b><br><b>set Ip/&lt;lp_value&gt; Eng Ds/&lt;datastream_type&gt; agentQ &lt;agentQ_value&gt;</b> |
| 4    | Activate changes. See <a href="#">Activating configuration changes (page 161)</a> .                                                                                                                                                                                                                           |

---

--End--

---

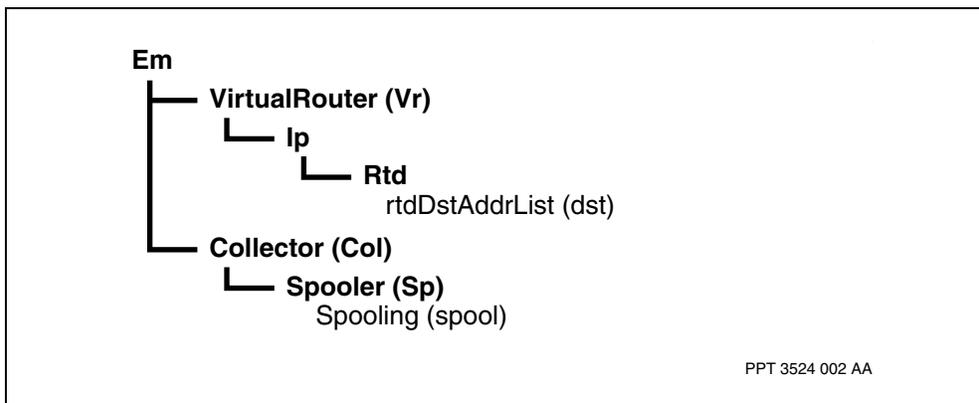


### Variable definitions

| Variable          | Value                                                                                                                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <agentQ_value>    | is the maximum size of the agent queue size for the data stream of the data collection system (DCS) on the LP.                                                                                                                                 |
| <collector_value> | is an instance of a data type, for example stats. The main function of the collector is to coordinate the collection of data from all its Agent subcomponents and distribute that data to the downstream applications which have requested it. |
| <datastream_type> | is engineering parameters used by DCS on this LP for a particular datastream.                                                                                                                                                                  |
| <ip_address>      | is a list of IP destination addresses for which the round trip delays are calculated for the current round trip delay measurement session.                                                                                                     |
| <lp_value>        | is the number of the LP.                                                                                                                                                                                                                       |
| <vr_name>         | is the name of the virtual router.                                                                                                                                                                                                             |

### Procedure job aid

#### Round-trip delay measurements component hierarchy





## Example of configuring BGP on a VCG with dynamic tunnels

This is an example procedure. The values you use in your configuration can differ from the values shown here. Consult your network engineer to ensure the values you are using are accurate for your configuration. The configuration used in this example is shown in [Example of configuring BGP for a VCG for dynamic tunnels \(page 145\)](#).

### Prerequisites

- The atmMpe/<mpe\_value> must be present. See the procedure “Configuring an ATM MPE interface for IP traffic” in NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.

### Procedure steps

| Step | Action                                                                                                                               |
|------|--------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add a virtual media (Vm).<br><code>add Vm/&lt;vm_value&gt;</code>                                                                    |
| 2    | Add the IP BGP attributes.<br><code>add -s Vr/VCG1 Ip Bgp</code>                                                                     |
| 3    | Set the virtualRouterProcessor.<br><code>set Vr/VCG1 Vrp Ip/0</code>                                                                 |
| 4    | Set the local autonomous system for BGP.<br><code>set Vr/VCG1 Ip Bgp localAs 100</code>                                              |
| 5    | Set the bgpIdentifier.<br><code>set Vr/VCG1 Ip Bgp bgpIdentifier &lt;IP_address_VCG1&gt;</code>                                      |
| 6    | Add the BPG peer.<br><code>add Vr/VCG1 Ip Bgp Peer/&lt;IP_address_VCG2&gt;</code>                                                    |
| 7    | Set the peer autonomous system of the BGP peer.<br><code>set Vr/VCG1 Ip Bgp Peer/&lt;IP_address_VCG2&gt; Desc peerAs 100</code>      |
| 8    | Set the IP address of the BGP peer.<br><code>set Vr/VCG1 Ip Bgp Peer/&lt;IP_address_VCG2&gt; Desc lac &lt;IP_address_VCG1&gt;</code> |
| 9    | Set the addressFamily of the BGP peer.<br><code>set Vr/VCG1 Ip Bgp Peer/&lt;IP_address_VCG2&gt; Desc addressFamily ipv4Vpn</code>    |
| 10   | Add the AtmMpe protocol port, IP address and set the network mask.                                                                   |



- add -s Vr/VCG1 Pp/MPE1A IpPort log/<IP\_add\_1A> netMask 255.255.255.252**
- 11 Add the OSPF.
- add -s Vr/VCG1 Ip Ospf area/0.0.0.0**
- 12 Enable the OSPF spareInstance.
- set Vr/VCG1 Ip Ospf spareInstance enable**
- 13 Set the asBdrRtrStatus.
- set Vr/VCG1 Ip Ospf asBdrRtrStatus true**
- 14 Add the OSPF interface.
- add Vr/VCG1 Pp/MPE1A Ip Log/<IP\_add\_1A> OspfIf area 0.0.0.0**
- 15 Link the protocol port to the atmMpe.
- set Vr/VCG1 Pp/MPE1A linkToMedia atmMpe/<mpe\_value>**
- 16 Add a protocol port for the VM interface.
- add -s Vr/VCG1 Pp/<vm> Ip Log/<IP\_address\_VCG1> OspfIf area 0.0.0.0,ifType passive**
- 17 Set the netmask for the protocol port.
- set Vr/VCG1 Pp/<vm> Log/<IP\_address\_VCG1> netMask 255.255.255.255**
- 18 Set the linkModel to pointToPoint.
- set Vr/VCG1 Pp/<vm> IpPort linkModel pointToPoint**
- 19 Repeat [step 1](#) through [step 14](#) for the second node (MSS2) using the corresponding values (for example, VCG2 would be used to specify the name of the Vr component) indicated in the figure [Example of configuring BGP for a VCG for dynamic tunnels \(page 145\)](#).

---

**--End--**

---

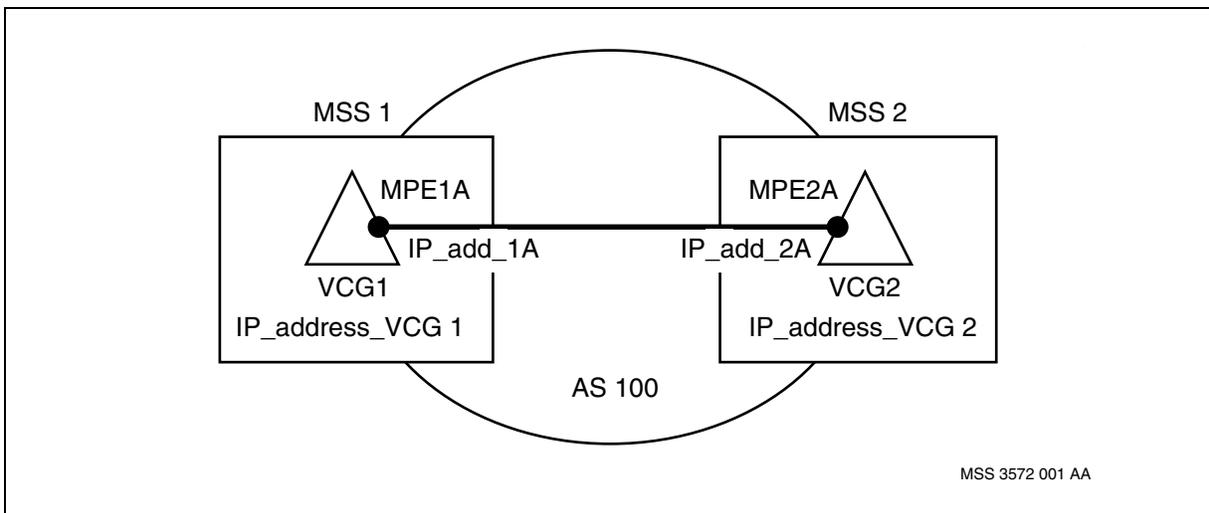


### Variable definitions

| Variable          | Value                                          |
|-------------------|------------------------------------------------|
| <IP_add_1A>       | is the IP address of the AtmMpe protocol port. |
| <IP_address_VCG1> | is the loopback address of VCG1.               |
| <IP_address_VCG2> | is the loopback address of peer VCG2.          |
| <vm_value>        | is the name of the virtual media.              |

### Procedure job aid

#### Example of configuring BGP for a VCG for dynamic tunnels





---

## VCG-based IP VPN customer access configuration

---

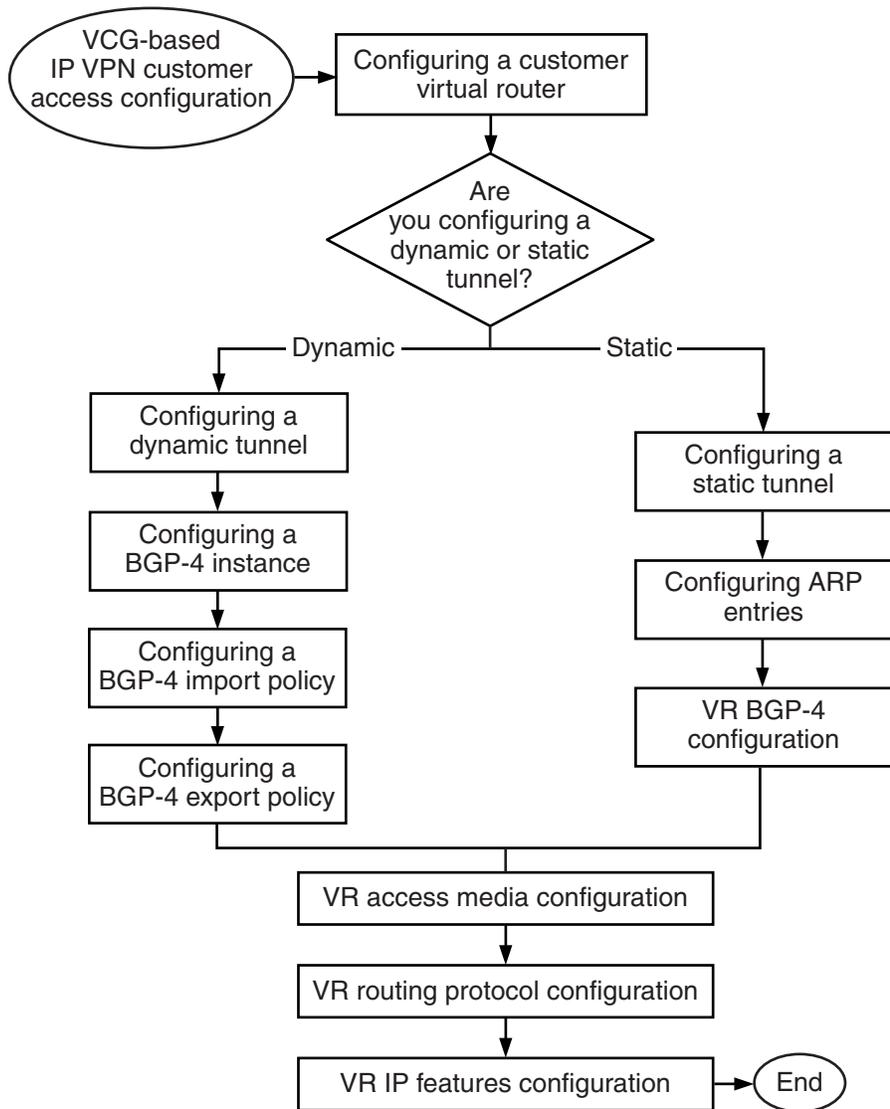
Configure a VCG-based IP VPN customer access configuration to provide a customer site access to a VPN.

### **VCG-based IP VPN customer access configuration procedures**

This task flow shows you the sequence of procedures you perform to configure a VCG-based IP VPN access configuration. To link to any procedure, go to [VCG-based IP VPN customer access configuration procedure navigation \(page 147\)](#).



**VCG-based IP VPN customer access configuration procedures**



MSS 3524 003 AA

**VCG-based IP VPN customer access configuration procedure navigation**

- [Configuring a customer virtual router \(page 149\)](#)
- [Configuring a dynamic tunnel \(page 150\)](#)
- Configuring a BGP-4 instance. See the VR BGP-4 configuration chapter in NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.



- Configuring a BGP-4 import policy. See VR BGP-4 configuration chapter in NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- Configuring a BGP-4 export policy. See VR BGP-4 configuration chapter in NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- [Configuring a static tunnel \(page 153\)](#)
- [Configuring ARP entries \(page 159\)](#)
- VR BGP-4 configuration. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- VR access media configuration. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- VR routing protocol configuration. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.
- VR IP features configuration. See NN10600-801 *Nortel Multiservice Switch 7400/15000/20000 IP Configuration Management*.



## Configuring a customer virtual router

Configure a customer virtual router to provide the customer with an access point to the VPN.

### Procedure steps

| Step | Action                                                                                                                                  |
|------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add the virtual router.<br><code>add Vr/&lt;vr_name&gt;</code>                                                                          |
| 2    | Set the logical processor on which the virtual router processor resides.<br><code>set Vr/&lt;vr_name&gt; vrp lp/&lt;lp_value&gt;</code> |
| 3    | Set the <i>virtualPrivateNetworkIdentifier</i> attribute.<br><code>set Vr/&lt;vr_name&gt; vpnId &lt;vpnId_value&gt;</code>              |
| 4    | Add the IP protocol to the VR.<br><code>add Vr/&lt;vr_name&gt; Ip</code>                                                                |
| 5    | Activate changes. See <a href="#">Activating configuration changes (page 161)</a>                                                       |

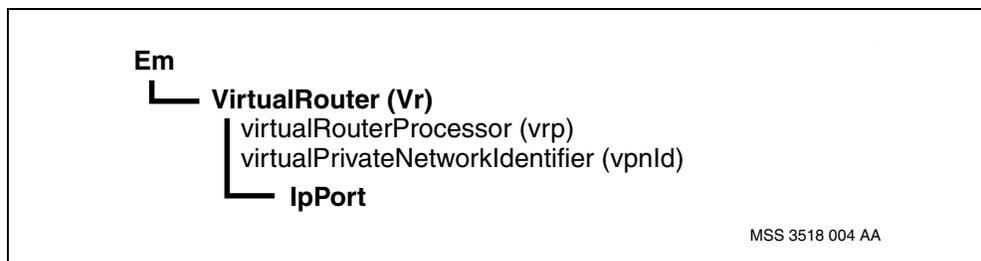
--End--

### Variable definitions

| Variable      | Value                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------|
| <lp_value>    | is the instance value of the logical processor that is linked to the shelf card on which the virtual router resides. |
| <vpnId_value> | is the instance value of the virtual private network (VPN) associated with this virtual router.                      |
| <vr_name>     | is the name of the virtual router.                                                                                   |

### Procedure job aid

#### Customer virtual router component hierarchy



MSS 3518 004 AA



## Configuring a dynamic tunnel

Configure a dynamic tunnel to allow VCGs to automatically exchange customer topology information.

A tunnel port is a protocol port that is VR dependent and is configured as a media subcomponent of the *Vr Ip IpTunnel* component. It is important to note that the CAS Copy command is not supported for the tunnel port and media components. Therefore, do not separate a tunnel port from its associated tunnel or an unexpected result could be produced. To rename a tunnel protocol port, you must first delete both the tunnel port and protocol port making sure to activate changes. See [Activating configuration changes \(page 161\)](#). Finally, you can add both the tunnel and protocol port.

### Procedure steps

| Step | Action                                                                                                                                                                                                                         |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Add the <i>Tunnel</i> component to the <i>VirtualRouter</i> component. The <i>MultipointStaticEndPoint</i> component is added automatically.<br><b>add Vr/&lt;vr_name&gt; Ip Tunnel</b>                                        |
| 2    | Set the <i>autoDiscovery</i> attribute to enabled.<br><b>set Vr/&lt;vr_name&gt; Ip Tunnel Msep/&lt;msep_value&gt; disc enabled</b>                                                                                             |
| 3    | Set the <i>sharedDomainVirtualRouter</i> attribute to be the VCG at the source endpoint of the IP tunnel.<br><b>set Vr/&lt;vr_name&gt; Ip Tunnel Msep/&lt;msep_value&gt; sdvr &lt;sdvr_value&gt;</b>                           |
| 4    | Set the <i>sourceAddress</i> attribute to be one host IP address of local end of the IP tunnel on the shared domain virtual router.<br><b>set Vr/&lt;vr_name&gt; Ip Tunnel Msep/&lt;msep_value&gt; src &lt;src_address&gt;</b> |
| 5    | Add <i>ProtocolPort</i> component.<br><b>add Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt;</b>                                                                                                                                        |
| 6    | Link the <i>ProtocolPort</i> component to the <i>MultipointStaticEndPoint</i> component.<br><b>set Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt; media Vr/&lt;vr_name&gt; Ip Tunnel Msep/&lt;msep_value&gt;</b>                       |
| 7    | Add the <i>IpPort</i> component which contains IP attributes specific to this port.<br><b>add Vr/&lt;vr_name&gt; Pp/&lt;pp_value&gt; IpPort</b>                                                                                |
| 8    | Add the <i>IpLogicalInterface</i> component.                                                                                                                                                                                   |



- ```
add Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/  
<iport_address>
```
- 9 Set subnet mask for this logical interface.
- ```
set Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/
<iport_address> netMask/<netmask_address>,
broadcastAddress <broadcast_address>
```
- 10 Set the broadcast address for this logical interface.
- ```
set Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/  
<iport_address> broadcastAddress <broadcast_address>
```
- 11 Activate changes. See [Activating configuration changes \(page 161\)](#).
-

--End--

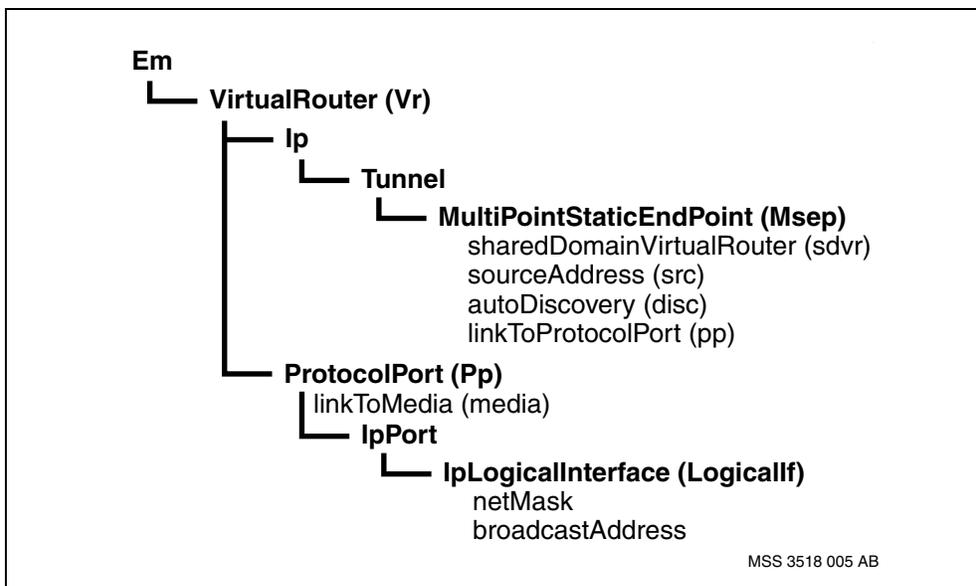


Variable definitions

Variable	Value
<broadcast_address>	is the IP address of the broadcast address for this <i>LogicalIf</i> component.
<ipport_address>	is the IP address of the single IpPort on a logical IP network.
<msep_value>	is an instance that represents a static IP tunnel end point of a point-to-multipoint IP tunneling configuration.
<netmask_address>	is the IP address of the subnet mask for this <i>LogicalIf</i> component.
<pp_value>	is the logical interface to the network.
<sdvr_value>	is the <i>VirtualRouter</i> component. This virtual router is at the source endpoint of the IP tunnel. The <i>vpnMode</i> attribute of that VR must be set to carrier.
<src_address>	is one host IP address of the local end of the IP tunnel on the shared domain virtual router.
<vr_name>	is the name of the virtual router.

Procedure job aid

Dynamic tunnel component hierarchy





Configuring a static tunnel

Configure a static tunnel to manually configure the exchange of topology information between customer virtual routers.

Procedure steps

Step	Action
1	Add the <i>Tunnel</i> component to the <i>VirtualRouter</i> component. The <i>MultipointStaticEndPoint</i> component is added automatically. add Vr/<vr_name> Ip Tunnel
2	Set the <i>sharedDomainVirtualRouter</i> (<i>sdvr</i>) attribute to be the virtual router at the source endpoint of the IP tunnel. set Vr/<vr_name> Ip Tunnel Msep/<msep_value> sdvr vr/ <vcg_value>
3	Set the <i>sourceAddress</i> (<i>src</i>) attribute to be the IP address of local end of the IP tunnel in the shared domain. set Vr/<vr_name> Ip Tunnel Msep/<msep_value> src <src_value>
4	Set the <i>destinationAddresses</i> attribute. set Vr/<vr_name> Ip Tunnel Msep/<msep_value> dst <dst_address>
5	Optionally, enable tunnel optimization. set Vr/<vr_name> Ip Tunnel optimization enabled



WARNING

Tunnel optimization is not supported on GQM-based FPs. If a tunnel utilizes both PQC-based and GQM-based FPs, tunnel optimization must not be used on either the PQC or GQM-based FP.

- 6 Create a static address resolution protocol (ARP) entry for the private address of each PTMP IP tunnel end point and specify the public address of the tunnel endpoint on the associated VCGs.

add -s Vr/<vr_name> Ip Arp Host/<host>,na tda <tda>
- 7 Add *ProtocolPort* component.

add Vr/<vr_name> Pp/<pp_value>
- 8 Link the *ProtocolPort* component to the *MultipointStaticEndPoint* component.

**set Vr/<vr_name> Pp/<pp_value> media Vr/<vr_name> Ip
Tunnel Msep/<msep_value>**



- 9 Add the *IpPort* component which contains IP attributes specific to this port.
add Vr/<vr_name> Pp/<pp_value> IpPort
- 10 Add the *IpLogicalInterface* component.
**add Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/
<iport_address>**
- 11 Set subnet mask for this logical interface.
**set Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/
<iport_address> netMask/<netmask_address>,
broadcastAddress <broadcast_address>**
- 12 Set the broadcast address for this logical interface.
**set Vr/<vr_name> Pp/<pp_value> IpPort LogicalIf/
<iport_address> broadcastAddress <broadcast_address>**
- 13 Activate changes. See [Activating configuration changes \(page 161\)](#).

--End--

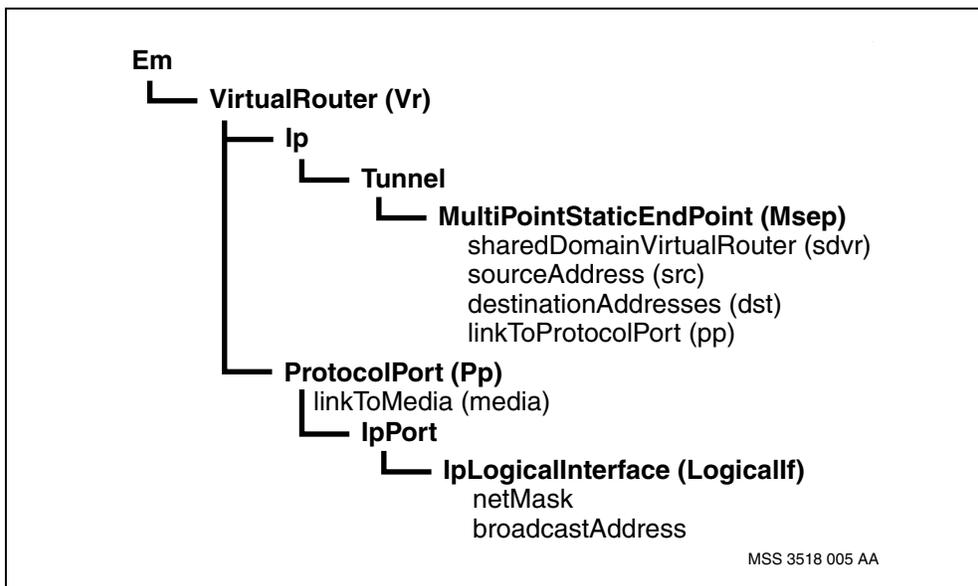


Variable definitions

Variable	Value
<broadcast_address>	is the IP address of the broadcast address for this <i>LogicalIf</i> component.
<dst_address>	is a list of IP addresses mapping to each of the far end IP tunnel endpoints in the private domain.
<ipport_address>	is the IP address of the single IpPort on a logical IP network.
<msep_value>	is an instance that represents a static IP tunnel end point of a point-to-multipoint IP tunneling configuration.
<netmask_address>	is the IP address of the subnet mask for this <i>LogicalIf</i> component.
<pp_value>	is the logical interface to the network.
<sdvr_value>	is the <i>VirtualRouter</i> component. This virtual router is at the source endpoint of the IP tunnel. The <i>vpnMode</i> attribute of that VR must be set to carrier.
<src_address>	is the IP address of the local end of the IP tunnel in the shared domain.
<vr_name>	is the name of the virtual router.

Procedure job aid

Static tunnel component hierarchy





Example of configuring a static tunnel

This is an example procedure. The values you use in your configuration can differ from the values shown here. Consult your network engineer to ensure the values you are using are accurate for your configuration. The configuration used in this example is shown in [Example of configuring a static tunnel \(page 158\)](#).

A tunnel port is a protocol port that is VR dependent and is configured as a media subcomponent of the *Vr Ip IpTunnel* component. It is important to note that the CAS Copy command is not supported for the tunnel port and media components. Therefore, do not separate a tunnel port from its associated tunnel or an unexpected result could be produced. To rename a tunnel protocol port, you must first delete both the tunnel port and protocol port making sure to activate changes. See [Activating configuration changes \(page 161\)](#). Finally, you can add both the tunnel and protocol port.

Procedure steps

Step	Action
1	Create a PTMP IP tunnel end point on the customer VR. <code>add -s Vr/<CVR1> Ip Tunnel Msep/<msep></code>
2	Specify the VCG as the shared domain VR at the source end of the PTMP IP tunnel. <code>set Vr/<CVR1> Ip Tunnel Msep/<msep_value> sdvr Vr/VCG1</code>
3	Specify the source and destination address of the tunnel. <code>set Vr/<CVR1> Ip Tunnel Msep/<msep_value> src <IP_public_1B></code> <code>set Vr/<CVR1> Ip Tunnel Msep/<msep_value> dst <IP_public_2B></code> The source address represents the public address of the tunnel end point on the local VCG. The destination addresses represent the public addresses of the tunnel end points on neighboring VCGs.
4	Create a protocol port and logical interface for the tunnel source address on the customer VR. <code>add -s Vr/<CVR1> Pp/TNLIA IpPort LogicalIf/ <IP_private_1A> netmask 255.255.255.0</code>
5	Link the protocol port defined for the PTMP IP tunnel on the customer VR to the IP tunnel end point. <code>set Vr/<CVR1> Pp/TNLIA linkToMedia Vr/<IP_private_1A> Ip Tunnel Msep/<msep></code>
6	Optionally, enable tunnel optimization.



set Vr/<CVR1> Ip Tunnel optimization enabled



WARNING

Tunnel optimization is not supported on GQM-based FPs. If a tunnel utilizes both PQC-based and GQM-based FPs, tunnel optimization must not be used on either the PQC or GQM-based FP.

- 7 Create a static Address Resolution Protocol (ARP) entry for the private address of each PTMP IP tunnel end point and specify the public address of the tunnel end point on the associated VCGs.

add -s Vr/<CVR1> Ip Arp Host/<IP_private_2A>,na tda <IP_public_1B>
- 8 Optionally, set the maximum transmission unit (MTU) size for the IP packets in the IP tunnel. Set the MTU size for the PTMP IP tunnel to the lowest MTU value supported in the Carrier routing domain. The sample command shows the default MTU value for Ethernet.

set Vr/<CVR1> Ip Tunnel Msep/<msep_value> mtu 1500
- 9 Repeat [step 1](#) through [step 8](#) for every PTMP IP tunnel on the Multiservice Switch node.
- 10 Repeat [step 1](#) through [step 9](#) on Multiservice Switch node 2 (MSS2) replacing the corresponding values (for example, VCG1 becomes VCG2, and so on) as indicated in figure [Example of configuring a static tunnel \(page 158\)](#).
- 11 Activate changes. See [Activating configuration changes \(page 161\)](#).

--End--

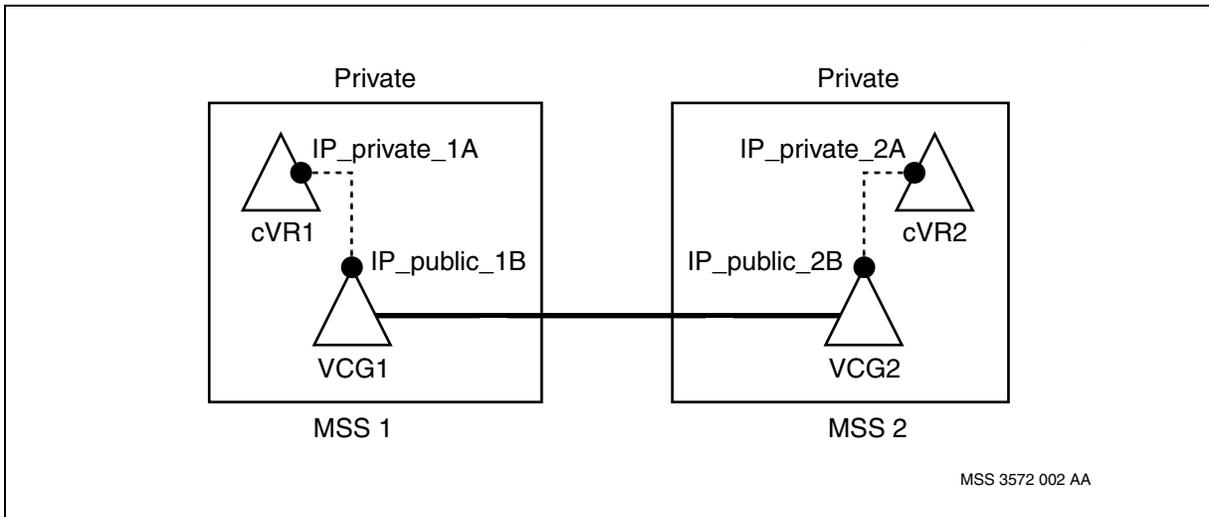


Variable definitions

Variable	Value
<msep_value>	is an instance that represents a static IP tunnel end point of a point-to-multipoint IP tunneling configuration.

Procedure job aid

Example of configuring a static tunnel





Configuring ARP entries

Configure address resolution protocol (ARP) entries to associate a tunnel destination address to the IP address of the remote customer virtual router.

Procedure steps

Step	Action
1	Add the <i>HostEntry</i> component. <code>add Vr/<vr_name> Ip Arp Host/<host_ip_address>, <Cos></code>
2	Set the <i>tunnelDestinationAddress</i> attribute. <code>set Vr/<vr_name> Ip Arp Host/<host_ip_address>, <Cos> tda <tunnel_ip_address></code>
3	Repeat step 1 and step 2 for every tunnel destination in this VPN.
4	Activate changes. See Activating configuration changes (page 161) .

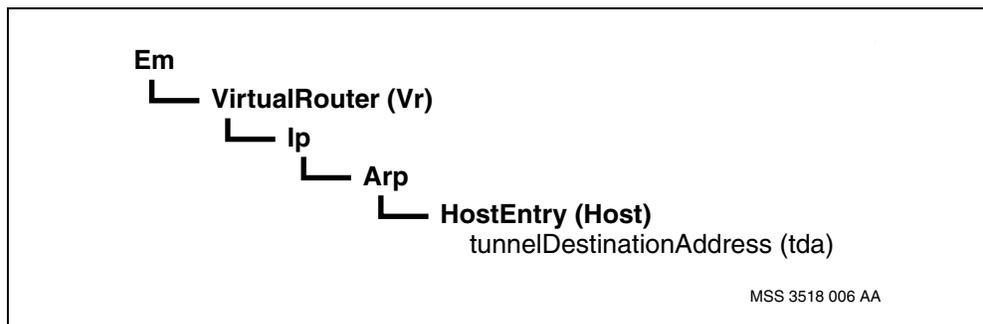
--End--

Variable definitions

Variable	Value
<Cos>	is the one value of the class of service (Cos).
<host_ip_address>	is defining a static host entry in the ARP table. This instance contains an IP address.
<tunnel_ip_address>	is the IP address of a remote IP tunnel endpoint in the shared domain.
<vr_name>	is the name of the virtual router.

Procedure job aid

ARP entries component hierarchy





Procedure conventions

This document uses the following procedure conventions:

- You can enter commands using full component and attribute names, or you can abbreviate them. The commands used in the procedures contain the full component and attribute names in the first instance. In the second instance, the component and attribute names are abbreviated. For more information on abbreviating component and attribute names, see NN10600-060 *Nortel Multiservice Switch 7400/15000/20000 Component Reference*. All component and attribute names are formatted in italics.
- The introduction of every procedure states whether you must perform the procedure in operational mode or provisioning mode. For more information on these modes, see [Operational mode \(page 160\)](#) or [Provisioning mode \(page 161\)](#).
- When you complete a procedure, you can verify your changes and then activate them as the new node configuration. For more information on completing configuration changes and exiting provisioning mode, see [Activating configuration changes \(page 161\)](#).

Operational mode

Procedures contained within this document can either be performed in operational mode or provisioning mode. When you initially log into a node, you are in operational mode. Nortel Multiservice Switch systems use the following command prompt when you are in operational mode:

```
#>
```

where:

is the current command number

In operational mode, you work with operational components and attributes. In operational mode, you can

- list operational components and display operational attributes to determine the current operating parameters for the node
- control the state of parts of the node by locking and unlocking components



- set certain operational attributes and enter commands to perform diagnostic tests

Provisioning mode

To change from operational mode to provisioning mode, type the following command at the operator prompt:

```
start Prov
```

Only one user can be in provisioning mode at a time. Nortel Multiservice Switch systems use the following command prompt whenever you are in provisioning mode:

```
PROV #>
```

where:

is the current command number

In provisioning mode, you work with the provisionable components and attributes that contain the current and future configurations of the node. You can add and delete components, and display and set provisionable attributes. For information on completing the configuration changes, exiting provisioning mode, and returning to operational mode see [Activating configuration changes \(page 161\)](#).

For information on operational and provisionable attributes, see NN10600-060 *Nortel Multiservice Switch 7400/15000/20000 Component Reference*.

Activating configuration changes

Several procedures in this document ask that you complete the configuration changes. When you complete the configuration changes, you are activating the configuration changes, confirming that you want to activate them, and saving the changes. You are instructed to complete the configuration changes only at the end of procedures that you perform in provisioning mode.



CAUTION

Activating a provisioning view can affect service

Activating a provisioning view can result in a CP reload or restart, causing all services on the node to fail. See NN10600-050 *Nortel Multiservice Switch 7400/15000/20000 Command Reference*, for more information.



CAUTION

Risk of service failure

When you activate the provisioning changes (see [step 3](#)), you have 20 minutes to confirm these changes. If you do not confirm these changes within 20 minutes, the shelf resets and all services on the node fail.

- 1 Verify that the provisioning changes you have made are acceptable.

check Prov

Correct any errors and then verify the provisioning changes again.

- 2 If you want to store the provisioning changes in a file, save the provisioning view.

save -f(<filename>) Prov

- 3 If you want these changes as well as other changes made in the edit view to take effect immediately, activate, confirm, and commit the provisioning changes.

activate Prov

confirm Prov

commit Prov

- 4 End the provisioning session.

end Prov

Nortel Multiservice Switch 7400/15000/20000
IP VPN Configuration Management

Copyright © 2005 Nortel.
All Rights Reserved.

Publication: NN10600-803
Document status: Standard
Document issue: 7.1S1
Document date: October 2005
Product release: PCR7.1 and up
Job function: Operations
Type: NTP
Language type: U.S. English

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel.

