

IP Networking

Version 7.2

Table of Contents

1	Introduction	11
2	IPv4.....	13
2.1	Example of Primary and Secondary IP Address Configuration	13
2.1.1	Configuration	13
2.1.2	Output	13
2.2	Interface VLAN – Link State Monitor.....	14
2.2.1	Configuration	14
3	ICMP	15
3.1	ping	15
3.2	Traceroute.....	16
4	VRRP	17
4.1	Feature Key.....	17
4.2	CLI Configuration and Status Commands.....	17
4.2.1	Configuration Commands.....	17
4.2.2	Status Commands	17
4.3	VRRP Example	19
5	DHCP	25
5.1	DHCP Client.....	25
5.2	DHCP Server.....	26
5.2.1	DHCP Zones.....	27
5.2.1.1	Selectors.....	27
5.2.1.2	Default Zone	28
5.3	DHCP Relay	29
5.4	Example of DHCP Server and DHCP Client	30
5.4.1	DHCP Client Configuration Example (WAN Side).....	30
5.4.2	DHCP Server Configuration Example (LAN Side).....	30
5.5	Example of DHCP Relay	31
5.6	Example of DHCP Server with Zones	31
5.7	Output of show Commands	32
5.7.1	show dhcp server leased ip addresses	32
5.7.2	show dhcp relay configuration display.....	32
6	DNS.....	33
6.1	DNS Configuration.....	33
6.1.1	Global Configuration	33
6.1.2	Interface-specific Configuration	33
6.2	Example #1 of Basic Dynamic DNS Configuration.....	34
6.2.1	Configuration	34
6.2.2	Output and show Commands	35
6.3	Example #2 of Basic Static DNS Configuration.....	35
6.3.1	Configuration	35
6.4	DNS Query Randomization	36
7	Track.....	37
7.1	Configuring Track	37
7.2	Output	37

8	BFD	39
8.1	Configuring BFD	39
8.2	Output	40
9	Static Routing	41
9.1	Configuring Static Routing	41
9.2	Example of Basic Static Route Configuration	41
9.2.1	Configuration	41
9.2.2	Output	42
9.3	Example of "Floating" Static Route and Track	43
9.3.1	Configuration	43
9.4	Example of "Floating" Static Route and BFD	45
9.4.1	Configuration	45
10	Manipulating the Routing Table	47
11	Administrative Distance	49
11.1	Examples of Configuring AD for Various Protocols	49
11.2	Example of Changing Default AD for a Dynamic Routing Protocol	50
11.2.1	Configuration	50
11.2.2	Output	51
11.3	Example of Configuring Static Route with Custom Metric	51
11.3.1	Configuration	51
11.3.2	Output	52
12	Dynamic IP Routing	53
12.1	RIP Routing Protocol	53
12.1.1	Configuring RIP	53
12.1.2	Example of RIP Routing	55
12.1.2.1	Configuration	55
12.1.2.2	Output and show Commands	56
12.2	OSPF Routing Protocol	57
12.2.1	Configuring OSPF	57
12.2.1.1	Router-Configuration Level	57
12.2.1.2	Interface-Configuration Level	59
12.2.2	Example of OSPF Routing	59
12.2.3	Useful Output and show Commands	61
12.3	Border Gateway Protocol (BGP)	62
12.3.1	Configuring BGP	62
12.3.1.1	Address-Family Level Configuration (configuration can also be set without entering the AF mode)	62
12.3.1.2	General Configuration	64
12.3.2	Example of Basic BGP WAN Connectivity	66
12.3.2.1	Configuration	66
12.3.2.2	Output	66
12.3.3	Example 2	67
12.3.3.1	Configuration	67
12.3.3.2	Output	68
12.4	Advanced Routing Examples	69
12.4.1	Multi-WAN with BGP and Static Route	69
12.4.1.1	Configuration	69
12.4.1.2	Output and Show Commands	70
12.4.2	Filtering Dynamic Routing Protocol Routes	71

12.4.3	Multi-WAN with BGP and IPSec.....	72
12.4.3.1	MSBR1 Configuration.....	72
12.4.3.2	Output.....	74
13	Policy Based Routing (PBR)	75
13.1	PBR Configuration.....	75
13.1.1	Example of PBR using Route-Map-Static.....	75
13.1.1.1	Configuration	76
13.1.1.2	Output.....	76
14	Loopback Interfaces	79
14.1.1	Loopback Interface Configuration.....	79
14.1.2	Example of Loopback Interface Configuration	79
14.1.2.1	Configuration	79
14.1.2.2	Output.....	79
14.1.3	Example of Protocol Binding to Loopback Interfaces.....	80
14.1.3.1	OAMP Binding to Loopback	80
14.1.3.2	BGP Termination on Loopback	80
14.1.4	Configuring Loopback Interfaces to Work with Voice	81
15	Virtual Routing and Forwarding (VRF)	83
15.1.1	VRF Configuration	83
15.1.1.1	Global Configuration.....	83
15.1.1.2	Interface Configuration	83
15.1.1.3	Other.....	83
15.1.2	VRF App Awareness	84
15.1.3	Example of Segment Isolation using VRF	85
15.1.3.1	Configuration	85
15.1.3.2	Output.....	86
15.1.4	Routing Services on Different VRF'S	87
15.1.4.1	Configuration	87
15.1.4.2	Output.....	88
16	GRE Tunnels.....	89
16.1.1	Configuring GRE Tunnels.....	89
16.1.2	Example of Connecting Multiple Subnets using GRE	89
16.1.2.1	Configuration	90
16.1.2.2	Output.....	91
17	Quality of Service (QoS)	93
17.1.1	QoS Configuration	94
17.1.2	Example of Weighted Bandwidth Sharing	95
17.1.2.1	Configuration	95
17.1.2.2	Output.....	96
17.1.3	Example using QoS to Ensure Bandwidth for Critical Traffic	97
17.1.3.1	Configuration	97
17.1.3.2	Output.....	97
17.1.4	Remarking DSCP/P-bit for Exceeded Traffic (Over the Reserved Bandwidth).....	98
17.1.5	Weighted Random Early Detect	99
17.1.6	QoS on Mediant 500Li MSBR	101
17.1.6.1	Weighted Fair Queuing	101
18	IPv6.....	103
18.1	Example of multiple IPv6 Address Configuration	104
18.1.1	Configuration	104
18.1.2	Output	104
18.1.3	Example of a Dual-Stack Configuration.....	105
18.1.3.1	Configuration	105

18.1.3.2	Output.....	105
19	ICMPv6	107
19.1	ping ipv6.....	107
19.2	Traceroute v6	108
20	Track v6.....	109
20.1	Configuring Track	109
20.2	Output	109
21	IPv6 Routing	111
21.1	Static Routing	111
21.1.1	Configuring Static Routing	111
21.1.2	Example of a Basic Static Route Configuration.....	111
21.1.2.1	Configuration	111
21.1.2.2	Output.....	112
21.2	RIPng Routing Protocol	113
21.2.1	Configuring RIPng	113
21.2.2	Example of RIPng Routing	114
21.2.2.1	Configuration	114
21.2.2.2	Output and show Commands.....	115
21.3	OSPFv3 Routing Protocol.....	116
21.3.1	Configuring OSPF.....	116
21.3.1.1	Router-Configuration Level	116
21.3.1.2	OSPF6 Router Level	116
21.3.1.3	Main options for Interface-Configuration Level	116
21.3.2	Example of OSPFv3 Routing.....	117
21.3.3	Useful Output and show Commands.....	118
21.4	Border Gateway Protocol (BGP) for IPv6.....	119
21.4.1	Configuring BGP.....	119
21.4.1.1	Main options for Address-Family Level Configuration	119
21.4.2	Example of Basic BGP WAN Connectivity	120
21.4.2.1	Configuration	120
21.4.2.2	Output.....	120
21.4.3	Example 2.....	121
21.4.3.1	Configuration	121
21.4.3.2	Output.....	123
21.5	DCHPv6	125
21.5.1	Configuring Stateless DHCP	126
21.5.2	Configuring Stateful DHCP	126
21.5.3	Configuring Router Advertisement	126
21.5.4	Configuring Prefix Delegation.....	127
21.5.5	Example of DHCPv6 Prefix Delegation with Autoconfig.....	128
21.5.5.1	Configuration of Prefix Delegation	128
21.5.5.2	Output.....	130
21.5.6	Example of RA Configuration	132
21.5.6.1	Configuration	132
21.5.6.2	Output.....	132
21.5.7	DHCPv6 advertised information	132
21.5.8	DHCPv6 Client.....	133
21.6	DNSv6.....	134
21.6.1	DNSv6 Configuration.....	134
21.6.1.1	Global Configuration.....	134
21.6.1.2	Interface-Specific Configuration	134
21.6.2	Example of Basic Static DNS Configuration.....	135

22 IP Multicast – PIM Sparse Mode.....	137
22.1 Feature Key.....	137
22.2 CLI Configuration and Status Commands.....	137
22.2.1 Configuration Commands.....	137
22.2.2 Status Commands	138
22.2.3 Multicast Example - Static RP	140
22.2.4 Multicast Example - Dynamic RP – Bootstrap Router Elects RP	151
22.2.4.1 On the Client \ Media Receiving Side	152
23 IP Multicast – IGMP Proxy	153
23.1 Feature Key.....	153
23.2 CLI Configuration and Status Commands.....	153
23.2.1 Configuration Commands.....	153
23.2.2 Status Commands	154
23.2.3 Multicast Example.....	155
A Mediant 500 Transmitter Examples	163

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: October-06-2020

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

Stay in the Loop with AudioCodes



Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Throughout this manual, unless otherwise specified, the term *device* refers to AudioCodes Mediant MSBR products.

Related Documentation

Document Name
Mediant 500Li Hardware Installation Manual
Mediant 500Li User's Manual
Mediant 500L MSBR Hardware Installation Manual
Mediant 500L MSBR User's Manual
Mediant 500 MSBR Hardware Installation Manual
Mediant 500 MSBR User's Manual
Mediant 800 MSBR Hardware Installation Manual
Mediant 800 MSBR User's Manual

Document Revision Record

LTRT	Description
31652	Initial document release.
31653	Updated section 4.1 DHCP client.
31654	Sections 4, 7, 18, 19, 21 and 22 were added.
31655	Added configuration for loopback of interfaces to work with voice.
31656	Updates to the Ping command, Traceroute command, Static routing, RIP interface configuration, Dynamic Routing protocol routes, OAMP Binding to loopback, VRF configuration, OSPF Routing protocol and BGP configuration.
31657	Updates to the Policy Based Routing (PBR) configuration.
31659	Added BFD Neighbor commands and floating static routes and BFD.
31720	Updated Configuration of Prefix Delegation.
31721	Updated BFD - Output, Example of "Floating" Static Route and BFD.
31722	Updates to IPv4, VRRP Example, DNC Configuration, DNS, Loopback Interfaces, DHCPv6, IP Multicast-PIM Sparse Mode.
31745	Updated DHCPv6 & QoS sections.
31746	Section Example of Basic BGP WAN Connectivity was updated.
31748	QoS section for Mediant 500Li.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at <https://online.audiocodes.com/documentation-feedback>.

1 Introduction

As an all-in-one product family, the Mediant MSBR Series (hereafter referred to as *device*) provide a variety of data services. As a rule, data services of any-size organization are based on IP networking as a standard, as IPv4 (and in the future, IPv6) are the official and standard suits of data network protocols.

This document deals with the device's IP data functionality and addresses the purpose of listing and explaining the kinds and nature of the supported IP protocols, explaining their most common uses and functionality, how to configure and implement them in an existing network, and demonstrating the most common and real-life-like scenarios and best practices in which those protocols can and should be used. In addition, a list of available commands and options for each protocol is described.

The examples in this document include topology, configuration methods and sample output and verifying commands to better understand the way they operate.

All mentioned protocols and technologies can be used in a more complex and advanced configuration than some of those demonstrated in this document; however, the main goal is to demonstrate common and well-tested implementations.

This page is intentionally left blank.

2 IPv4

IPv4 is the common and most widespread version of the Internet Protocol which is responsible for routing traffic on the internet and private networks. IPv4 also defines the structure and rules of IP addressing for network devices and nodes.

The device maintains a routing table which lists the IP addresses familiar to the device and how to reach them in terms of next-hop. Information stored in the routing table is received from different sources, such as local physical and logical interfaces, static routes configured by the network administrator, and dynamic routing protocols. All of the listed items are seen as different routing domains.

IP addresses on the device are configured on interfaces, and usually are accompanied by the subnet mask, which is used for the subnet calculation.

Each Layer-3 interface can be assigned one primary IP address, and several secondary IP addresses. Secondary IP addresses are typically used to provide connectivity to several subnets through a single interface, facilitating network transitions and multi-homing.

2.1 Example of Primary and Secondary IP Address Configuration

The following is an example of primary and secondary IP address configuration.

2.1.1 Configuration

```
# configure data
(conf-data)# interface VLAN 1
(conf-if-VLAN 1)# ip address 192.169.12.1 255.255.255.0
(conf-if-VLAN 1)# ip address 192.169.0.1 255.255.255.0 secondary
(conf-if-VLAN 1)# no shutdown
```

2.1.2 Output

```
# show data int vlan 1

VLAN 1 is Connected.
  Description: LAN switch VLAN 1
  Hardware address is 00:90:8f:4a:23:43
  IP address is 192.169.12.1
  netmask is 255.255.255.0
  State Time: 242:26:48
  Time since creation: 242:27:11
  Time since last counters clear :    0:00:05
  mtu auto
  Secondary IP address is 192.169.0.1
  Secondary netmask is 255.255.255.0
  DNS is configured static
  DNS primary IP address is 0.0.0.0
  DNS secondary IP address is 0.0.0.0
```

2.2 Interface VLAN – Link State Monitor

The device handles physical and logical interfaces. While the state of a physical interface is determined by whether its connected to the power (plugged in or not), logical interfaces, such as interface VLAN, can remain in UP state even if ports associated with them are disconnected. To prevent such a scenario, it is possible to enable a link-state monitor, which probes the state of VLAN-associated interfaces, and brings down VLAN interfaces if ports associated with them are disconnected.

2.2.1 Configuration

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface vlan vlan</code>	Enters the interface vlan configuration mode.
<code>(conf-if-Vlan num)# link-state monitor</code>	Enables the link-state monitor.

3 ICMP

Internet Control Message Protocol (ICMP) is one of the main protocols in the IP suite and in general, is used by network equipment to obtain information or notify about data delivery problems, for example, in case a specific service is unavailable or a specific network or host is unreachable.

The most common and known usages of ICMP are the `ping` and `tracert` commands, using ICMP messages to test IP reachability to an IP address on the internet, and to verify the IP “hops” a packet travels on its way to the destination, respectively.

The ICMP protocol “runs” over UDP and is defined in RFC 792.

3.1 ping

The ping tests IP reachability to a desired destination. If the destination is reachable, there will be the same amount of echo requests and replies.

Command structure:

```
ping <IP address / host> options
```

where the options are:

- repeat - amount of ICMP requests to send.
- size - size of the of the ICMP packet in bytes.
- source – source from where to send the packets
- summarized - display summarized results (! - successful reply, .U - No reply, timeout and Unreachable)
- source [data voip]- interface to use as source address for the ICMP requests. Voip or data interfaces can be used. “Source voip” – allows you to select the source interface as name or as VLAN number. “Source data – allows you to select any interface as source for ping. The pings are sent from this interface. “Source data source-address” allows you to ping from IP of any address while the next hop calculated using the routing table. “Source data vrf” allows you to ping from any configured VRF.

Typical output:

```
# ping 192.168.0.3
Reply from 192.168.0.3: time=1 ms
Reply from 192.168.0.3: time=1 ms
Reply from 192.168.0.3: time=1 ms
Reply from 192.168.0.3: time=1 ms
4 packets transmitted, 4 packets received
Round-trip min/avg/max = 1/1/1 ms
```

3.2 Traceroute

The ping command informs you if the destination is reachable or not. Traceroute can be used to discover the path that packets travel to the remote destination.

Command structure:

```
traceroute <IP Address / host> [vrf | source-address]
```

Typical output:

```
# traceroute 8.8.8.8
1  192.168.0.1 (192.168.0.3)  1.169 ms  *  7.346 ms
2  100.100.100.2 (100.100.100.2)  1.169 ms  *  7.346 ms
.
.
8  8.8.8.8 (8.8.8.8)  1.169 ms  *  7.346 ms
Traceroute: Destination reached
#
```


4 VRRP

VRRP provides for automatic assignment of available routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on a LAN.

The protocol achieves this by creating virtual routers, comprised of master and backup routers. VRRP routers use multicast to notify its presence in the LAN (never forwarding outside of the LAN).

VRRP is based on RFC 2338 and RFC 3768.

4.1 Feature Key

Advanced routing feature key must be enabled.

4.2 CLI Configuration and Status Commands

The following describes the CLI Configuration and Status commands.

4.2.1 Configuration Commands

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface <Interface></code>	Configures an interface.
<code>vrrp <VRID> ip <ip address></code>	Sets primary IP address for the VRID
<code>vrrp <VRID> ip <ip address> secondary</code>	Sets secondary IP address for the VRID
<code>vrrp <VRID> priority <priority></code>	Sets priority for VRID, range 1-254
<code>vrrp <VRID> preempt</code>	Sets preemption for lower priority Master
<code>vrrp <VRID> advertisement-timer <time in seconds></code>	Sets interval timer for advertising the Master VRID

4.2.2 Status Commands

Command	Description
<code>show data vrrp</code>	Displays vrrp status
<code>show data vrrp interface <interface name></code>	Displays vrrp interface status.
<code>show data vrrp brief</code>	Displays vrrp brief status

```
# show data vrrp

VLAN 1 - Group 1
  State is Master
  Virtual IP address is 10.4.6.14
```

```

Advertisement interval is 1 sec
Preemption is enabled
Priority is 100
Master Router is 10.4.6.12 (local), priority is 100
Master Advertisement interval is 1 sec
Master Down interval is 3.609 sec

```

```

VLAN 2 - Group 1
State is Master
Virtual IP address is 10.7.5.4
Advertisement interval is 10 sec
Preemption is enabled
Priority is 120
Master Router is 10.7.7.7 (local), priority is 120
Master Advertisement interval is 10 sec
Master Down interval is 30.531 sec

```

show data vrrp interface vlan 2

```

VLAN 2 - Group 1
State is Master
Virtual IP address is 10.7.5.4
Advertisement interval is 10 sec
Preemption is enabled
Priority is 120
Master Router is 10.7.7.7 (local), priority is 120
Master Advertisement interval is 10 sec
Master Down interval is 30.531 sec

```

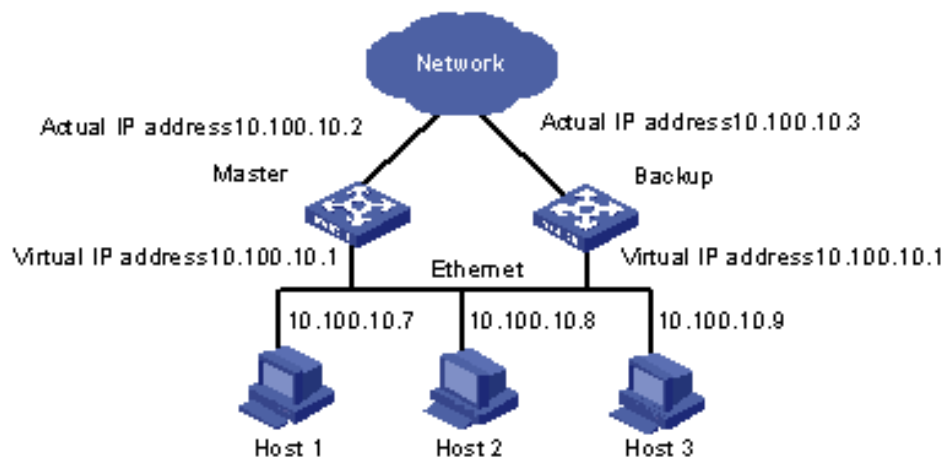
show data vrrp brief

Interface addr	Group addr	Grp	Pri	Time,msec	Own	Pre	State	Master
VLAN 1000		2	100	765609	Y	Y	Master	
101.101.101.101	2.2.2.2							
VLAN 1000		100	255	3003	Y	Y	Master	
101.101.101.101	101.101.101.101							
VLAN 2		3	100	3609	Y	Y	Master	
10.50.50.50	200.200.200.200							
VLAN 2		4	100	3609	Y	Y	Master	
10.50.50.50	10.4.3.2							
VLAN 2		2	120	300531	Y	Y	Master	
10.50.50.50	10.9.9.9							

4.3 VRRP Example

In the example below, there are two VRRP routers – one with IP 10.100.10.2 and one with 10.100.10.3. They use a common virtual IP address 10.100.10.1, where one is the Master and the other is the Backup. In the example, we will use VRID 1 over VLAN 1.

Figure 4-1: VRRP Example



The Master will be the device with the higher priority. For example:

■ **Master configuration:**

```
# configure data
(config-data) # interface vlan 1
(conf-if-VLAN 1) # vrrp 1 ip 10.100.10.1
(conf-if-VLAN 1) # vrrp 1 priority 200
(conf-if-VLAN 1) # exit
(config-data)
```

■ **Backup configuration:**

```
# configure data
(config-data) # interface vlan 1
(conf-if-VLAN 1) # vrrp 1 ip 10.100.10.1
(conf-if-VLAN 1) # vrrp 1 priority 100
(conf-if-VLAN 1) # exit
(config-data)
```

The following is an example of the *show run* command for two devices:

■ **Master:**

```
*# show run data

## Data Configuration
configure data
interface GigabitEthernet 0/0
  ip address dhcp
  ip dhcp-client default-route
  mtu auto
  desc "WAN Copper"
  no ipv6 enable
  speed auto
  duplex auto
  no service dhcp
  ip dns server auto
  napt
  firewall enable
  no shutdown
exit
interface Fiber 0/1
  ip address 200.0.0.2 255.255.255.252
  mtu auto
  desc "WAN Fiber"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no napt
  no firewall enable
  no shutdown
exit
interface dsl 0/2
  #DSL configuration is automatic
  #Termination cpe
  mode adsl
  shutdown
exit
interface EFM 0/2
  #This interface is DISABLED due to physical layer
configuration
  no ip address
  mtu auto
  desc "WAN DSL"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no shutdown
exit
interface GigabitEthernet 1/1
  speed auto
  duplex auto
```

```
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/2
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/3
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/4
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface VLAN 1
ip address 10.100.10.2 255.255.255.0
vrrp 1 advertisement-timer 10
vrrp 1 priority 200
vrrp 1 ip 10.100.10.1
mtu auto
desc "LAN switch VLAN 1"
no ipv6 enable
no napt
no firewall enable
no link-state monitor
no shutdown
exit
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 86400
ip nat translation icmp-timeout 6
# Note: The following WAN ports are in use by system
services,
#       conflicting rules should not be created:
#       Ports 80 - 80 --> HTTP
#       Ports 23 - 23 --> Telnet CLI
#       Ports 22 - 22 --> SSH CLI
#       Ports 82 - 82 --> TR069
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
```

```
exit
```

■ Slave:

```
# show run data

## Data Configuration

configure data
interface GigabitEthernet 0/0
  ip address dhcp
  ip dhcp-client default-route
  mtu auto
  desc "WAN Copper"
  no ipv6 enable
  speed auto
  duplex auto
  no service dhcp
  ip dns server auto
  napt
  firewall enable
  no shutdown
exit
interface Fiber 0/1
  ip address 200.0.0.3 255.255.255.252
  mtu auto
  desc "WAN Fiber"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no napt
  no firewall enable
  no shutdown
exit
interface dsl 0/2
  #DSL configuration is automatic
  #Termination cpe
  mode adsl
  shutdown
exit
interface EFM 0/2
  #This interface is DISABLED due to physical layer
configuration
  no ip address
  mtu auto
  desc "WAN DSL"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no shutdown
```

```
exit
interface GigabitEthernet 1/1
    speed auto
    duplex auto
    switchport mode trunk
    switchport trunk native vlan 1
    no shutdown
exit
interface GigabitEthernet 1/2
    speed auto
    duplex auto
    switchport mode trunk
    switchport trunk native vlan 1
    no shutdown
exit
interface GigabitEthernet 1/3
    speed auto
    duplex auto
    switchport mode trunk
    switchport trunk native vlan 1
    no shutdown
exit
interface GigabitEthernet 1/4
    speed auto
    duplex auto
    switchport mode trunk
    switchport trunk native vlan 1
    no shutdown
exit
interface VLAN 1
    ip address 10.100.10.3 255.255.255.0
    vrrp 1 advertisement-timer 10
    vrrp 1 priority 100
    vrrp 1 ip 10.100.10.1
    mtu auto
    desc "LAN switch VLAN 1"
    no ipv6 enable
    ip dns server static
    no napt
    no firewall enable
    no link-state monitor
    no shutdown
exit
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 86400
ip nat translation icmp-timeout 6
# Note: The following WAN ports are in use by system
services,
#         conflicting rules should not be created:
#         Ports 80 - 80 --> HTTP
#         Ports 23 - 23 --> Telnet CLI
#         Ports 22 - 22 --> SSH CLI
```

```
#          Ports 82 - 82 --> TR069
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
exit
```


5 DHCP

DHCP is a network protocol that allows network devices to acquire IPv4 address and additional network configuration parameters automatically from a DHCP server. DHCP is defined in RFC 2131 and the DHCP server options are defined in RFC 2132.

The device supports the following DHCP operation modes:

- DHCP Client
- DHCP Server
- DHCP Relay

5.1 DHCP Client

The DHCP client operation mode allows the device to acquire IPv4 addresses and network configuration parameters automatically on its network interfaces.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface gigabitethernet 0/0</code>	Selects an interface to configure.
<code>(config-if-VLAN-1)# ip address dhcp</code>	Configures the interface to acquire the IPv4 address and configuration via DHCP.
<code>(config-if-VLAN-1)# ip dhcp-client default-route</code>	Configures the interface to use the gateway address received via DHCP as the default route.
<code>(config-if-VLAN-1)# ip dhcp-client default-route track 1</code>	Configures the interface to use the gateway address received via DHCP as default route when track 1 is up. Note: If the track destination is remote, a static route will automatically be added to reach it through the gateway address.
<code>(config-if-VLAN-1)# no service dhcp</code>	Disables the DHCP server service on the interface.



Note: Track number cannot be configured using zero-conf.

5.2 DHCP Server

The DHCP server operation mode allows the device to act as a DHCP server on the network and to lease IPv4 addresses to network devices. The DHCP server functionality is configured per interface.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface VLAN 1</code>	Selects an interface to configure.
<code>(config-if-VLAN-1)# ip dhcp-server network 192.169.12.10 192.169.12.20 255.255.255.0</code>	Configures the start and end IP address for the leased range and the network mask.
<code>(config-if-VLAN-1)# ip dhcp-server dns-server 0.0.0.0</code>	Configures the DNS server address that will be advertised.
<code>(config-if-VLAN-1)# ip dhcp-server netbios-name-server 0.0.0.0</code>	Configures the NetBIOS server address that will be advertised.
<code>(config-if-VLAN-1)# ip dhcp-server netbios-node-type</code>	Configures the NetBIOS node type.
<code>(config-if-VLAN-1)# ip dhcp-server lease 0 1 0</code>	Configures the lease timer for the IP addresses (days , hours , and minutes).
<code>(config-if-VLAN-1)# ip dhcp-server provide-host-name</code>	Configures whether the server provides hostnames for network devices.
<code>(config-if-VLAN-1)# ip dhcp-server ntp-server 0.0.0.0</code>	Configures the NTP server IP address that will be advertised.
<code>(config-if-VLAN-1)# ip dhcp-server tftp-server 0.0.0.0</code>	Configures the TFTP server IP address that will be advertised.
<code>(config-if-VLAN-1)# ip dhcp-server override-router-address 0.0.0.0</code>	Configures the Default Gateway to advertise to clients when not acting as a default gateway.
<code>(config-if-VLAN-1)# ip dhcp-server next-server 0.0.0.0</code>	Configures the next TFTP server that can be used to advertise.
<code>(config-if-VLAN-1)# ip dhcp-server boot-file-name</code>	Configures a boot file path/name that will be advertised to clients (DHCP option 67).
<code>(config-if-VLAN-1)# ip dhcp-server classless-static-route</code>	Configures a static route that will be advertised to clients (DHCP option 121).
<code>(config-if-VLAN-1)# ip dhcp-server static-host <i>HostName</i></code> <code>(static-dhcp)# ip 1.1.1.1</code> <code>(static-dhcp)# mac AA:BB:CC:DD:EE:FF</code>	<ul style="list-style-type: none"> Enters the static address binding menu Configures the MAC address for the binding. Configures the IP address for the binding.
<code>(config-if-VLAN-1)# ip dhcp-server tftp-server-name</code>	Configures the TFTP server name that will be advertised to clients.

Command	Description
<code>(config-if-VLAN-1)# ip dhcp-server time-offset</code>	Configures the time-offset (GMT time zone) to be advertised to clients (in seconds).
<code>(config-if-VLAN-1)# ip dhcp-server tr069-acis-server-name</code>	Configures ACS server IP to be advertised to clients.
<code>(config-if-VLAN-1)# service dhcp</code>	Enable the DHCP service on the interface.

5.2.1 DHCP Zones

DHCP zones enable a router to act as a DHCP server to several different subnets. Each DHCP zone has its own IP address pool and an array of selectors indicating which requests each zone accepts.

If zones are configured in addition to the DHCP configuration as above, this configuration is referred to as the *default zone*.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface VLAN 1</code>	Selects an interface to configure.
<code>(config-if-VLAN-1)# ip dhcp-server zone meep</code>	Enters the configuration menu for zone meep
<code>(conf-zone meep)# network 5.5.1.1 5.5.200.200 255.255.0.0</code>	Configures the start and end IP addresses for the zone's leased range and the network mask. A zone's pool can't conflict with any other zone's IP pool.
<code>(conf-zone meep)# lease 0 1 0</code>	Configures the lease timer for the IP addresses (days, hours, and minutes) in the zone.
<code>(conf-zone meep)# next-server 0.0.0.0</code>	Configures the next TFTP server that can be used to advertise. If not defined, the interface's IP address will be used as a default value.
<code>(conf-zone meep)# dns 55.44.33.22</code>	Configures the DNS server address that will be advertised.
<code>(conf-zone meep)#exit (config-if-VLAN-1)# service dhcp</code>	Exits the zone definition and starts the DHCP service.

5.2.1.1 Selectors

Packet selectors can be defined on the following properties:

- DHCP Option 60
- DHCP Option 61 (client identifier)
- DHCP Option 77 (user class option)

- MAC Address
- Relay agent which forwarded this packet to server

A packet will be accepted by a zone if it meets one or more of the selectors defined in it. If a packet matches several zones, it will receive its IP from an arbitrary zone among them. If a zone has no selectors defined, it can accept no requests.

The same selector can't be defined in multiple zones.

Command	Description
<code>(conf-zone meep)# selector option 60 MSBR</code>	Accepts packets where the value of Option 60 is exactly 'MSBR'
<code>(conf-zone meep)# selector option 60 substr MSBR</code>	Accepts packets where the value of Option 60 contains 'MSBR', ex MSBR500
<code>(conf-zone meep)# selector option 61 01008F58C0EE</code>	Accepts packets where the value of Option 61 is the hex value 0x01008F58C0EE
<code>(conf-zone meep)# selector option 61 prefix 01008F58</code>	Accepts packets where the value of Option 61 starts with the hex value 0x01008F58
<code>(conf-zone meep)# selector option 77 phone</code>	Accepts packets where the value of Option 77 is exactly 'phone'
<code>(conf-zone meep)# selector option 77 substr phone</code>	Accepts packets where the value of Option 77 contains 'phone', ex ip-phone
<code>(conf-zone meep)# selector mac 00:8F:58:C0:22:EE</code>	Accepts packets where the client's mac address is 00:8F:58:C0:22:EE
<code>(conf-zone meep)# selector mac prefix 00:8F:58</code>	Accepts packets where the client's mac address starts with 00:8F:58
<code>(conf-zone meep)# selector relay 3.3.3.3</code>	Accepts packets received from the relay agent whose IP is 3.3.3.3
<code>(conf-zone meep)# selector relay 3.3.3.3 3.3.3.16</code>	Accepts packets received from the relay agent whose IP is in the range between 3.3.3.3 and 3.3.3.16

5.2.1.2 Default Zone

The DHCP server also has a default zone, which if configured will accept and respond to any DHCP request that no other zone accepts. See configuration details above.

5.3 DHCP Relay

The DHCP relay operation mode allows the device to relay and forward DHCP packets between different Layer-3 network segments, and between different interfaces.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface VLAN 1</code>	Selects an interface to configure.
<code>(config-if-VLAN-1)# ip dhcp-server 1.1.1.1</code>	Configures the IP address of the DHCP server from which to relay messages.

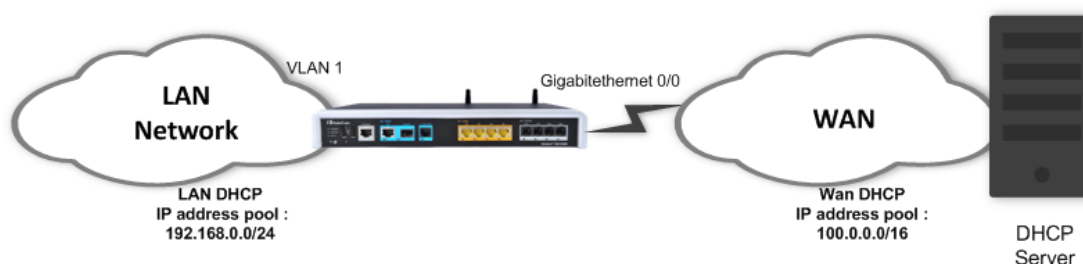
5.4 Example of DHCP Server and DHCP Client

This example configuration demonstrates a scenario in which the device acts as a DHCP server on the LAN network to which it is connected, and acquires its' WAN address using DHCP (as a client).



Note: Acquiring a WAN address using DHCP and acting as a DHCP server on the LAN is a common case, and describes a best-practice hierarchical DHCP functionality.

Figure 5-1: DHCP



On the WAN interface, the address is dynamically acquired once connectivity is established with a DHCP server. On the LAN interface, you need to configure the device to activate the DHCP service, specify the DHCP address pool, and which Default Gateway address to advertise. In addition, we specify the lease timers and TFTP and DNS server addresses to be advertised to DHCP clients.

5.4.1 DHCP Client Configuration Example (WAN Side)

```
# configure data
(conf-data)# interface GigabitEthernet 0/0
(conf-if-GE 0/0)# firewall enable
(conf-if-GE 0/0)# napt
(conf-if-GE 0/0)# ip address dhcp
(conf-if-GE 0/0)# ip dhcp-client default-route
(conf-if-GE 0/0)# no service dhcp
(conf-if-GE 0/0)# no shutdown
(conf-if-GE 0/0)# exit
```

5.4.2 DHCP Server Configuration Example (LAN Side)

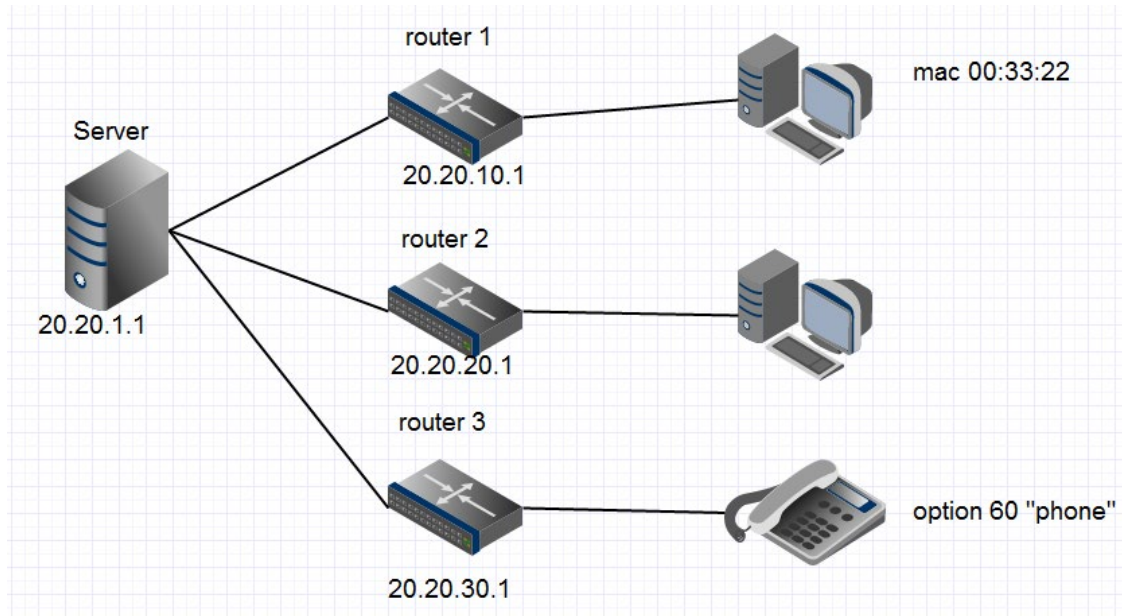
```
# configure data
(conf-data)# interface VLAN 1
(conf-if-VLAN 1)# ip address 192.168.0.1 255.255.255.0
(conf-if-VLAN 1)# desc "VLAN 1 LAN VOIP"
(conf-if-VLAN 1)# ip dhcp-server network 192.168.0.10 192.168.0.20 255.255.255.0
(conf-if-VLAN 1)# ip dhcp-server lease 0 1 0
(conf-if-VLAN 1)# service dhcp
(conf-if-VLAN 1)# no shutdown
(conf-if-VLAN 1)# exit
```

5.5 Example of DHCP Relay

This example configures the device to accept DHCP packets from the configured IP address, which will act as a DHCP relay.

```
# configure data
(conf-data)# ip dhcp-server 100.100.100.100 gigabitEthernet 0/0
```

5.6 Example of DHCP Server with Zones



In this example, the server is connected to three subnets via relay agents. For every subnet, a zone is configured, in addition to a default zone.

Configure the first zone, which accepts packets with source mac addresses beginning with 00:33:22:

```
# configure data
(config-data)# interface VLAN 1
(config-if-VLAN-1)# ip dhcp-server zone z1
(conf-zone z1)# selector mac prefix 00:33:22
(conf-zone z1)#network 20.20.10.5 20.20.10.200 255.255.255.0
(conf-zone z1)#lease 0 1 0
(conf-zone z1)#exit
```

Configure the second zone, which accepts packets arriving via relay agents whose addresses are in the 20.20.20.1-20.20.20.4 range:

```
(config-if-VLAN-1)# ip dhcp-server zone z2
(conf-zone z2)# selector relay 20.20.20.1 20.20.20.4
(conf-zone z2)#network 20.20.20.5 20.20.20.200 255.255.255.0
(conf-zone z2)#lease 0 1 0
(conf-zone z2)#exit
```

Configure the third zone, which accepts packets whose DHCP option 60's value contains the text "phone":

```
(config-if-VLAN-1)# ip dhcp-server zone z3
(conf-zone z3)# selector option 60 substr phone
(conf-zone z3)#network 20.20.30.5 20.20.30.200 255.255.255.0
(conf-zone z3)#lease 0 1 0
(conf-zone z3)#exit
```

Configure the default zone to have an address pool in the same subnet as its IP and activate the dhcp server:

```
(config-if-VLAN-1)# ip address 20.20.1.1 255.255.0.0
(config-if-VLAN-1)# ip dhcp-server 20.20.1.5 20.20.1.200
255.255.0.0
(config-if-VLAN-1)# ip dhcp-server lease 0 1 0
(config-if-VLAN-1)# service dhcp
```

5.7 Output of show Commands

The following displays the output of the *show* commands.

5.7.1 show dhcp server leased ip addresses

```
# show data ip dhcp binding
Hostname      Ip address      Mac address      IF name
Lease expiration
Test-Laptop   192.169.1.10    e8:11:32:05:05:26  VLAN 1
37
```

5.7.2 show dhcp relay configuration display

```
# show data ip dhcp-server all
DHCP relay server of interface GigabitEthernet 0/0:
Relay Server is enabled.
Configured servers:
100.100.100.100
```


6 DNS

Domain Name System (DNS) is a hierarchical naming system for computers, devices, or any resources connected to a network. DNS is used to resolve hostnames into IP addresses, and to enforce naming conventions for devices in the network and/or domain.

DNS configuration for devices can be either static – administrator configured – or acquired dynamically through DHCP.

6.1 DNS Configuration

The following describes DNS configuration commands.

6.1.1 Global Configuration

The following is the global configuration of the DNS:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# ip dns server all <auto static></code>	Configures the DNS configuration method (static or dynamic).
<code>(config-data)# ip dns server concurrent</code>	Configures the DNS server to issue queries to all configured name-servers concurrently. Use the “no” form to do it sequentially.
<code>(config-data)# ip name-server server1ip [server2ip] all</code>	Configures DNS server(s) IP address in case of static configuration.

6.1.2 Interface-specific Configuration

The following is the configuration of the DNS per interface:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface int_name</code>	Selects an interface to configure
<code>(config-if-name)# ip dns server <dynamic static></code>	Configures interface-specific DNS configuration method: static or dynamic
<code>(config-if-name)# ip name-server server1ip [server2ip] all</code>	Configures DNS server/s ip address in case of static configuration on the interface

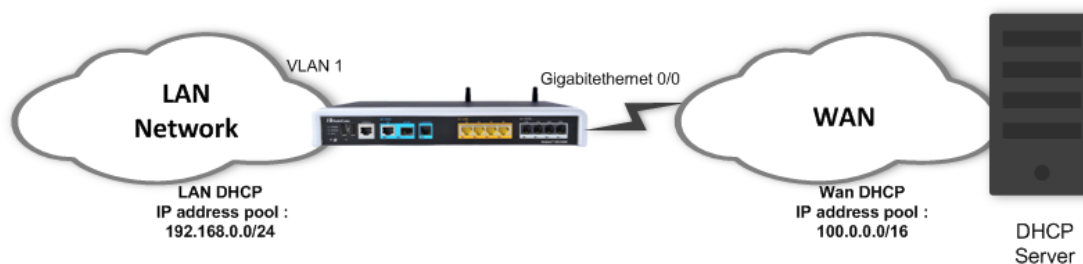
The device can act as a DNS server. To configure the device as a DNS server, use the following commands:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# ip host <name> <ip ipv6> <ttd></code>	<ul style="list-style-type: none"> <name>: any name for the host. <ip ipv6>: can configure IPv4 or IPv6 for the name. <TTL>: time to live of the DNS record.

6.2 Example #1 of Basic Dynamic DNS Configuration

In this typical example scenario, the device, acting as an access router for the organizational network, receives the DNS server's IP address dynamically through DHCP on the WAN interface. The device also acts as a DHCP server on the LAN, and by the configuration `ip name-server 0.0.0.0`, the device acts as a DNS server, relaying DNS messages to the DNS server's IP address that it acquires dynamically on the WAN interface.

Figure 6-1: Dynamic DNS



6.2.1 Configuration

```
# configure data
(conf-data)# interface GigabitEthernet 0/0
# WAN Interface is set as DHCP client
(conf-if-GE 0/0)# firewall enable
(conf-if-GE 0/0)# napt
(conf-if-GE 0/0)# ip address dhcp
(conf-if-GE 0/0)# ip dhcp-client default-route
(conf-if-GE 0/0)# ip dns-server auto
(conf-if-GE 0/0)# no shutdown
(conf-if-GE 0/0)# exit
(conf-data)# interface VLAN 1
# LAN Interface is set as DHCP server
(conf-if-VLAN 1)# ip address 192.168.0.1 255.255.255.0
(conf-if-VLAN 1)# desc "VLAN 1 LAN VOIP"
(conf-if-VLAN 1)# ip dhcp-server network 192.168.0.10 192.168.0.20
255.255.255.0
(conf-if-VLAN 1)# ip dhcp-server lease 0 1 0
(conf-if-VLAN 1)# ip dns server static
(conf-if-VLAN 1)# ip name-server 0.0.0.0
(conf-if-VLAN 1)# service dhcp
(conf-if-VLAN 1)# no shutdown
```

```
(conf-if-VLAN 1)# exit
```

6.2.2 Output and show Commands

```
# show data hosts
```

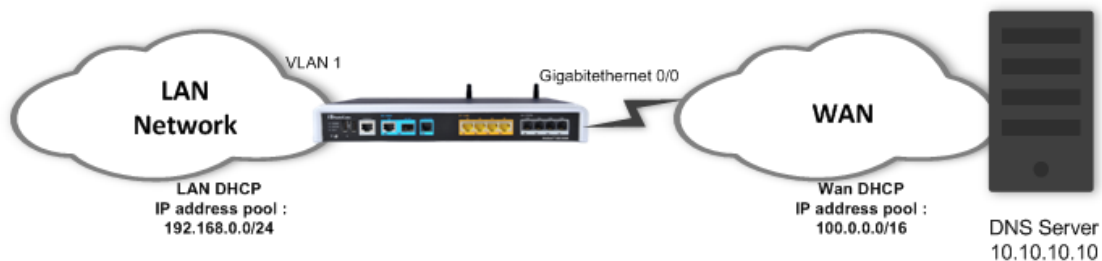
Interface name	DNS configuration	Primary IP address	Secondary IP address
GigabitEthernet 0/0	Dynamic	80.179.52.100	80.179.55.100
Fiber 0/1	Static	0.0.0.0	0.0.0.0
VLAN 1	Static	0.0.0.0	0.0.0.0

Host	Type	Parameters
------	------	------------

6.3 Example #2 of Basic Static DNS Configuration

In this typical example scenario, the device, acting as an access router for the organizational network, is configured with a static DNS server address. The device also acts as a DHCP server on the LAN, and by the configuration **ip name-server 0.0.0.0**, the device acts as a DNS server, relaying DNS messages to the DNS server's IP address that was provided statically or dynamically from the WAN interface.

Figure 6-2: Static DNS



6.3.1 Configuration

```
# configure data
(conf-data)# interface GigabitEthernet 0/0
(conf-if-GE 0/0)# firewall enable
(conf-if-GE 0/0)# napt
(conf-if-GE 0/0)# ip address dhcp
(conf-if-GE 0/0)# ip dhcp-client default-route
(conf-if-GE 0/0)# ip dns-server static
(conf-if-GE 0/0)# ip name-server 10.10.10.10
(conf-if-GE 0/0)# no service dhcp
(conf-if-GE 0/0)# no shutdown
(conf-if-GE 0/0)# exit
(conf-data)# interface VLAN 1
(conf-if-VLAN 1)# ip address 192.168.0.1 255.255.255.0
(conf-if-VLAN 1)# desc "VLAN 1 LAN VOIP"
```

```
(conf-if-VLAN 1)# ip dhcp-server network 192.168.0.10 192.168.0.20
255.255.255.0
(conf-if-VLAN 1)# ip dhcp-server lease 0 1 0
(conf-if-VLAN 1)# ip dns server static
(conf-if-VLAN 1)# ip name-server 0.0.0.0
(conf-if-VLAN 1)# service dhcp
(conf-if-VLAN 1)# no shutdown
```

6.4 DNS Query Randomization

The device supports randomization of DNS query ID and source port, on outgoing queries on the WAN side.

To configure it, refer to the *Mediant MSBR Security Setup CLI Configuration Guide* document.

7 Track

This command tracks a destination IP address from a given source interface. The tracking is done by sending ICMP probes and monitors the replies. If the destination is reachable, the Track Status is set to 'up'. When a configurable number of replies are not received, the Track Status is set to 'down'.

7.1 Configuring Track

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# track id icmpecho destIP interface [source-ip-interface interface] [interval val] [retries val]</code>	Configures a Track to monitor reachability to destIP from the interface .

7.2 Output

```
# show data track brief
Track      Type                State      Max round trip time (m.s)
1          ICMP reachability   Up         37
```

Get the time of up to the last 10 Track states:

```
# show data track 1 history

Track history:  New state      Date and Time [MM-DD-YYYY@hh:mm:ss]
                Up             08-28-2015@18:17:40
                Down           08-28-2015@18:25:30
                Up             08-28-2015@18:26:20
```

This page is intentionally left blank.

8 BFD

This command configures a BFD neighbor to track the bidirectional connectivity to the neighbor and manipulate routes in case of a failure. Unlike ICMP track, BFD uses UDP datagrams to communicate with the remote side. BFD requires that both sides must support the protocol and send BFD packets to each other.

If used in multiple VRFs, a different BFD process will run for each VRF.

8.1 Configuring BFD

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<pre>(config-data)# bfd neighbor <neighbor id> <ip address> <interface ID> interval <value> min_rx <value> multiplier <value> [multihop]</pre>	<p>Configures a BFD neighbor.</p> <ul style="list-style-type: none"> • neighbor id - (1-20) Neighbor identifier. • ip address - Address of the remote BFD device. • interface id - Name and number of the outgoing interface. • interval - (200-30000) Desired interval for outgoing bfd messages in milliseconds. The interval will be increased if the remote system requires it. • min_rx - (200-30000) Minimal interval between bfd messages in milliseconds. The remote system will use this interval for sending messages in case its interval is lower. • multiplier - (1-20) Maximum number of packets that can be missed before the session status is considered down. • multihop - Sets the neighbor to multihop mode in case the remote device is not on the local LAN.

8.2 Output

```
MSBR1# show data bfd neighbors [vrf vrf-name]
VRF main-vrf
Protocol Codes: S - Static, O - OSPF
  Proto NeighAddr          Holdown(mult) RH/RS State      Int
  1 S   192.168.110.10      600(3)       Up Up        VLAN 2
MSBR1# show data neighbors details [vrf vrf-name]
VRF main-vrf
Protocol Codes: S - Static, O - OSPF
  Proto NeighAddr          Holdown(mult) RH/RS State      Int
  1 S   192.168.110.10      600(3)       Up Up        VLAN 2
OutAddr: 192.168.100.254
Local Diag: 1, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 3
Holdown (hits): 600(1), Hello (hits): 200(4575)
Rx Count: 4575
Tx Count: 4578
Last packet: Version: 1          - Diagnostic: 3
              State bit: Up      - Demand bit: 0
              Poll bit: 0        - Final bit: 0
              Multiplier: 3      - Length: 24
              My Discr: 1        - Your Discr: 51
              Min tx interval: 200000 - Min rx interval: 200000
              Min Echo interval: 0
```


9 Static Routing

Static routing is used when the router uses pre-defined, user-configured routing entries to forward traffic. Static routes are usually manually configured by the network administrator and are added to the routing table.

A Common use of static routes is for providing the gateway of a "last resort", i.e., providing an instruction on how to forward traffic when no other route exists.

Static routes have a much lower administrative distance in the system than the dynamic routing protocols, and in most scenarios are prioritized over the dynamic routes.

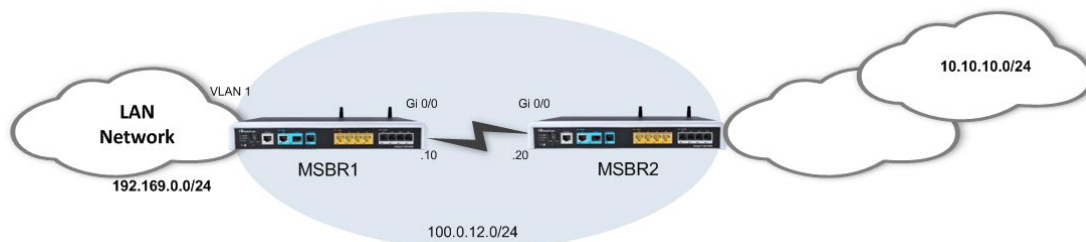
9.1 Configuring Static Routing

Command	Description
<code># configure data</code>	Enter the data configuration menu.
<code>(config-data)# ip route [vrf vrf] destIP destMask [next-hop] interface [A-distance] [track number] [output-vrf vrf]</code>	Configure a static route by specifying the destination prefix, an output interface and optionally a next-hop address, the metric for the route and a tracking object and output vrf.

9.2 Example of Basic Static Route Configuration

In this example, MSBR1 needs to reach the 10.10.10.0/24 network segment from its LAN. The destination segment is located somewhere in the network, behind MSBR2. This example does not include the configuration of dynamic routing. For this to configuration to work, MSBR1 needs to be configured to forward traffic to 10.10.10.0/24 through MSBR2's network interface, interfacing with MSBR1, whose address is 10.0.12.20.

Figure 9-1: Static Routing



9.2.1 Configuration

```
# configure data
(config-data)# ip route 10.10.10.0 255.255.255.0 100.0.12.20
gigabitethernet 0/0
(config-data)#
```

9.2.2 Output

```
# show running-config data
```

```
Configure data
```

```
*****
```

```
**
```

```
General configuration omitted, assume that configured as in  
diagram
```

```
*****
```

```
**
```

```
ip route 10.10.10.0 255.255.255.0 100.0.12.20 GigabitEthernet 0/0  
1  
exit
```

```
# show data ip route
```

```
Codes: K - kernel route, C - connected, S - static,
```

```
       R - RIP, O - OSPF, B - BGP
```

```
C   1.1.1.12/32 [1/4] is directly connected, Loopback 1
```

```
C   100.0.12.0/24 [1/3] is directly connected, GigabitEthernet
```

```
0/0
```

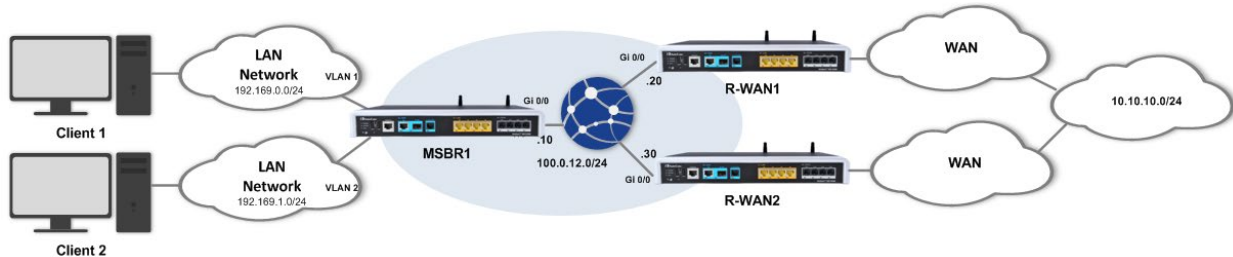
```
C   192.169.12.0/24 [1/4] is directly connected, VLAN 1
```

```
S   10.10.10.0/24 [1/1] via 100.0.12.20, GigabitEthernet 0/0
```

9.3 Example of "Floating" Static Route and Track

In this example, MSBR1 needs to reach the 10.10.10.0/24 network segment from its LAN. The destination network segment is reachable from both MSBR-R-WAN1 and MSBR-R-WAN2; however, this example assumes that due to routing considerations, the route through MSBR-R-WAN1 is preferable. Static routes will be configured through both of the MSBRs, while the one pointing to MSBR-R-WAN1 will have lower metric value and will be linked with a tracking object.

Figure 9-2: Multi WAN with Floating Static Route



If connectivity through MSBR-R-WAN1 fails, the tracking mechanism deletes the static route pointing to MSBR-R-WAN1 from the local MSBR's routing table and the second, higher metric value static route is used.

9.3.1 Configuration

```
MSBR1# show run data
```

```
Configure data
*****
**
General configuration omitted, assume that configured as in
diagram
*****
**
track 1 IcmpEcho 100.0.12.20 GigabitEthernet 0/0 interval 2
retries 2
ip route 10.10.10.0 255.255.255.0 100.0.12.20 GigabitEthernet
0/0 30 track 1
ip route 10.10.10.0 255.255.255.0 100.0.12.30 GigabitEthernet
0/0 50
Exit
```

```
MSBR1# show data track brief
```

Track	Type	State	Max round trip time (m.s)
1	ICMP reachability	Up	21

```
MSBR1# show data ip route
```

```
Codes: K - kernel route, C - connected, S - static,
R - RIP, O - OSPF, B - BGP

C 1.1.1.12/32 [1/4] is directly connected, Loopback 1
C 100.0.12.0/24 [1/3] is directly connected, GigabitEthernet
0/0
C 192.169.12.0/24 [1/4] is directly connected, VLAN 1
S 10.10.10.0/24 [1/30] via 100.0.12.20, GigabitEthernet 0/0
```

■ After reachability failure to MSBR-R-WAN1:

```
MSBR1# show data track brief
Track          Type          State          Max round trip
time (m.s)
1              ICMP reachability  Down          -218137

MSBR1# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

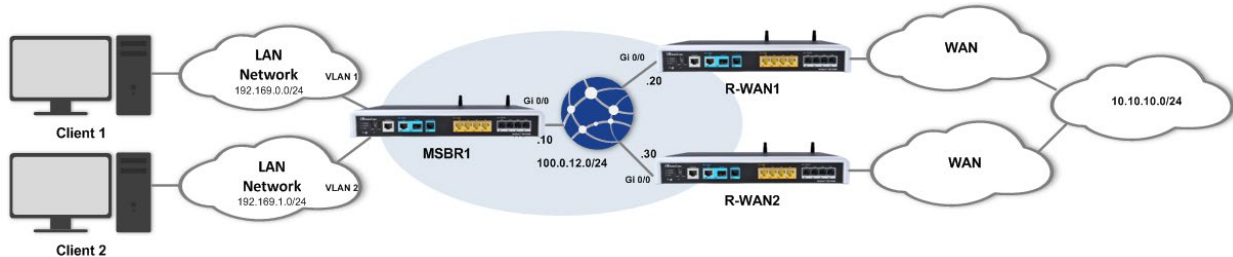
C    1.1.1.12/32 [1/4] is directly connected, Loopback 1
C    100.0.12.0/24 [1/3] is directly connected,
GigabitEthernet 0/0
C    192.169.12.0/24 [1/4] is directly connected, VLAN 1
S    10.10.10.0/24 [1/50] via 100.0.12.30, GigabitEthernet 0/0

MSBR-R-WAN1#
```

9.4 Example of "Floating" Static Route and BFD

In this example, MSBR1 needs to reach the 10.10.10.0/24 network segment from its LAN. The destination network segment is reachable from both MSBR-R-WAN1 and MSBR-R-WAN2; however, this example assumes that due to routing considerations, the route through MSBR-R-WAN1 is preferable. Static routes will be configured through both of the MSBRs, while the one pointing to MSBR-R-WAN1 will have a lower metric value and will be linked to the state of a BFD session between MSBR1 and MSBR-R-WAN1.

Figure 9-3: Multi WAN with Floating Static Route



If connectivity to MSBR-R-WAN1 fails, the BFD mechanism will detect it and delete the static route pointing to MSBR-R-WAN1 from the local MSBR's routing table and the second, higher metric value static route is used.

9.4.1 Configuration

```
MSBR-R-WAN1# show run data
  Configure data
*****
**
General configuration omitted, assume that configured as in
diagram
*****
**
bfd neighbor 1 100.0.12.10 GigabitEthernet 0/0 interval 500 min_rx
500 multiplier 3
Exit
MSBR1# show run data
  Configure data
*****
**
General configuration omitted, assume that configured as in
diagram
*****
**
bfd neighbor 1 100.0.12.20 GigabitEthernet 0/0 interval 500 min_rx
500 multiplier 3
  ip route 10.10.10.0 255.255.255.0 100.0.12.20 GigabitEthernet
0/0 30 bfd-neighbor 1
  ip route 10.10.10.0 255.255.255.0 100.0.12.30 GigabitEthernet
0/0 50
  Exit
MSBR1# show data bfd neighbors
VRF main-vrf
Protocol Codes: S - Static, O - OSPF
  Proto NeighAddr      Holdown(mult)  RH/RS State      Int
  1 S      100.0.12.20      1500(3)        Up      Up GigabitEthernet 0/0
```

```
SBR1# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C 1.1.1.12/32 [1/4] is directly connected, Loopback 1
C 100.0.12.0/24 [1/3] is directly connected, GigabitEthernet
0/0
C 192.169.12.0/24 [1/4] is directly connected, VLAN 1
S 10.10.10.0/24 [1/30] via 100.0.12.20, GigabitEthernet 0/0
```

■ After reachability failure to MSBR-R-WAN1:

```
MSBR1# show data bfd neighbors

VRF main-vrf
Protocol Codes: S - Static, O - OSPF
  Proto NeighAddr      Holdown(mult) RH/RS State      Int
  1 S      100.0.12.20      1500(3)      Up      Down GigabitEthernet 0/0

MSBR1# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C 1.1.1.12/32 [1/4] is directly connected, Loopback 1
C 100.0.12.0/24 [1/3] is directly connected,
GigabitEthernet 0/0
C 192.169.12.0/24 [1/4] is directly connected, VLAN 1
S 10.10.10.0/24 [1/50] via 100.0.12.30, GigabitEthernet 0/0
```

10 Manipulating the Routing Table

The device's routing table contains the “best” routes the device is familiar with to known destinations; however, how does it decide which route is the better route to a destination?

The device starts by examining the prefixes and prefix lengths. The same prefixes, however with different prefix lengths are considered as different destinations, and as a rule, the most specific prefix always “wins” in a tie. Next, for destinations with the same prefixes and prefix lengths, the decision is made according to the lower Administrative Distance (AD) of the protocol it was learned from. Next, if there are two routes with similar AD, the one with the lower metric wins. The product of this decision process is the “best” route to a specific network destination.

The parameters which determine the best route are configurable, i.e. a network administrator can influence of the determination of this route by configuring the AD of the protocols running on the device (OSPF, RIP, BGP, and Static) and the metrics of the specific protocols, for example, changing BGP attributes, changing BW for OSPF and, changing metrics for static routes, etc.).

This page is intentionally left blank.

11 Administrative Distance

The parameter that is used by the device to rate the priority of routing information from the different routing domains is called the Administrative Distance and the system default ADs are as follows:

- Connected – 1 (can't be changed)
- Static – 1 (can't be changed)
- RIP - 120
- OSPF - 110
- BGP – 200/20 (iBGP / eBGP)

If the router learns how to reach the same subnet from two different sources, the subnet with the lower AD is added in the routing table.

It is important to understand that the device's routing table does not necessarily represent all the routes known to the device, merely the best ones, while every route protocol has a routing database of its own for storing known routes.

When a routing decision is made and there are two routes in the routing table with the same prefix, with two similar AD values, the decision is reached according to the metric parameter.

11.1 Examples of Configuring AD for Various Protocols

The following examples configure AD for various protocols.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# router</code> <code><OSPF BGP RIP></code>	Enters routing protocol configuration mode.
<code>(config-router)# distance</code> <code>distance</code>	Configures the AD for the selected dynamic routing protocol.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# ip route</code> <code>prefix/length next-hop</code> <code>interface [metric]</code>	Configures a static route with a non-default metric.

11.2 Example of Changing Default AD for a Dynamic Routing Protocol

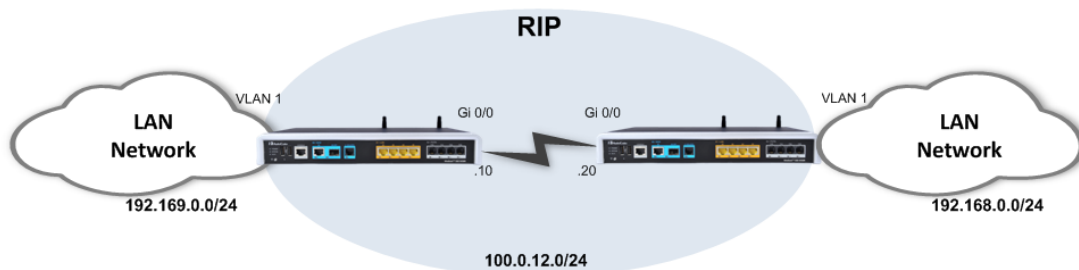
The following examples configure AD for various protocols.

11.2.1 Configuration

This example changes the default AD for the RIP dynamic routing protocol.

Assume a pre-configured network with the correct RIP routing according to the following diagram:

Figure 11-1: Changing RIP Protocol AD



➤ **To demonstrate the effect of the AD change:**

```
MSBR1# configure data
(config-data)# router rip
(conf-router)# distance 60
```

11.2.2 Output

■ Before the change:

```
MSBR(conf-router)#
MSBR1# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C    1.1.1.12/32 [1/4] is directly connected, Loopback 1
C    100.0.12.0/24 [1/3] is directly connected,
GigabitEthernet 0/0
C    192.169.0.0/24 [1/4] is directly connected, VLAN 1
R    192.168.0.0/24 [120/2] via 100.0.12.30, Gigabit Ethernet
0/0, 00:00:58
```

■ After the change:

```
MSBR1# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C    1.1.1.12/32 [1/4] is directly connected, Loopback 1
C    100.0.12.0/24 [1/3] is directly connected,
GigabitEthernet 0/0
C    192.169.0.0/24 [1/4] is directly connected, VLAN 1
R    192.168.0.0/24 [60/2] via 100.0.12.30, GigabitEthernet
0/0, 00:00:21
```

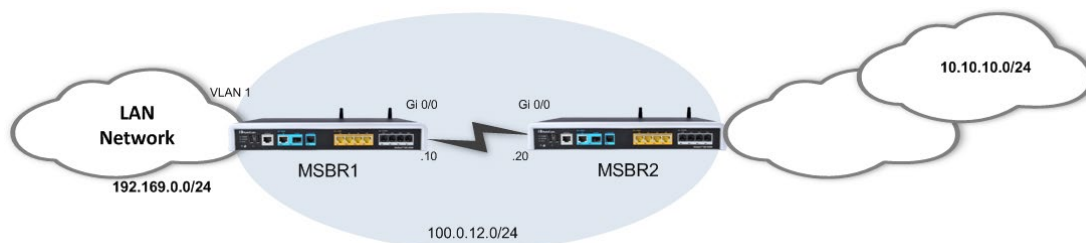
11.3 Example of Configuring Static Route with Custom Metric

The following is an example of configuring static route with custom metric.

11.3.1 Configuration

In the event where there is a prefix that needs to be reached and is located behind MSBR2, you need to configure a static route on MSBR1 that points to this prefix through MSBR2's interface towards MSBR1.

Figure 11-2: Changing Static Route Metric



Configure this static route with a non-default metric:

```
MSBR1# configure data
(config-data)# ip route 10.10.10.0 255.255.255.0 100.0.12.20
gigabitethernet 0/0 50
(config-data)#
```

11.3.2 Output

```
MSBR1# show running-config data
```

```
Configure data
```

```
*****
**
General configuration omitted, assume that configured as in
diagram
*****
**

ip route 10.10.10.0 255.255.255.0 100.0.12.20 GigabitEthernet 0/0
50
exit
```

```
MSBR1# show data ip route
```

```
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP
```

```
C  1.1.1.12/32 [1/4] is directly connected, Loopback 1
C  100.0.12.0/24 [1/3] is directly connected, GigabitEthernet
0/0
C  192.169.12.0/24 [1/4] is directly connected, VLAN 1
S  10.10.10.0/24 [1/50] via 100.0.12.20, GigabitEthernet 0/0
```

12 Dynamic IP Routing

While the concept of data IP routing deals with getting data from point A to point B over the network, it is important to note that there are two distinct methods for doing this:

- **Static routing:** specifically and manually pointing the router as to through which next-hop to route to which destination.
- **Dynamic routing:** configuring a dynamic routing protocol on all the routers in the network, enabling them to become aware of each other and the different subnets in the network and dynamically learn the best route to each destination.

The advantages of dynamic routing are clear – it is automated, adaptive, makes routers network-aware and provides even redundant routing paths.

This chapter elaborates on the different dynamic routing protocols that are supported by the device.

12.1 RIP Routing Protocol

Routing Information Protocol (RIP) is a dynamic routing protocol from the Distance Vector family which uses hop-count as a routing metric. The protocol is limited to 15 hops per route, which prevents loops; however also limits the network size and scalability.

Low metric routes are considered “better” and a route with hop count (metric) of 16 is considered “unreachable”.

RIP is considered a “chatty” and bandwidth consuming protocol due to the fact it “floods” its routing database once in a period (default is 30 seconds).

RIP can work both in broadcast and unicast modes (without or with peers, respectively).

The device supports both RIP versions, RIPv1 (RFC 1058) and RIPv2 (RFC 2453).

12.1.1 Configuring RIP

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# router rip</code>	Enters the RIP configuration mode.
<code>(conf-router)# default-information originate</code>	Configures whether to advertise the default route.
<code>(conf-router)# default-metric metric</code>	Configures the metric for redistributed routes.
<code>(conf-router)# distance distance</code>	Configures the AD for the protocol.
<code>(conf-router)# distribute-list prefix list-name <in/out> interface</code>	Configures filtering of incoming/outgoing routing updates.
<code>(conf-router)# neighbor IPaddress password Password</code>	Configures a neighbor with secured session password.
<code>(conf-router)# neighbor IPaddress</code>	Configures a neighbor router.
<code>(conf-router)# network interface</code> <code>(conf-router)# network prefix/prefLen</code>	Configures a network or interface upon which to enable RIP routing.

Command	Description
(conf-router)# passive-interface <i>interface</i>	Configures suppression of routing updates on an interface.
(conf-router)# redistribute <i>protocol metric metric [route-map name]</i>	Configures redistribution of routes from other protocols into RIP.
(conf-router)# route <i>prefix/length</i>	Adds a RIP static route.
(conf-router)# route-map <i>RMname <in/out> interface interface</i>	Configures a route-map for the RIP routing.
(conf-router)# timers basic <i>value</i>	Configures the routing table update timer.
(conf-router)# version <i><1/2></i>	Configures which RIP version to run.

Rip interface configuration:

Command	Description
# configure data	Enters the data configuration menu.
(config-data)# interface <i>GigabitEthernet 0/0</i>	Enters the interface configuration mode.
(conf-if-GE 0/0)# ip rip <i>receive</i>	Rip version for received packets.
(conf-if-GE 0/0)# ip rip <i>send</i>	Rip version for sent packets.
(conf-if-GE 0/0)# ip rip <i>split-horizon</i>	Perform split horizon.

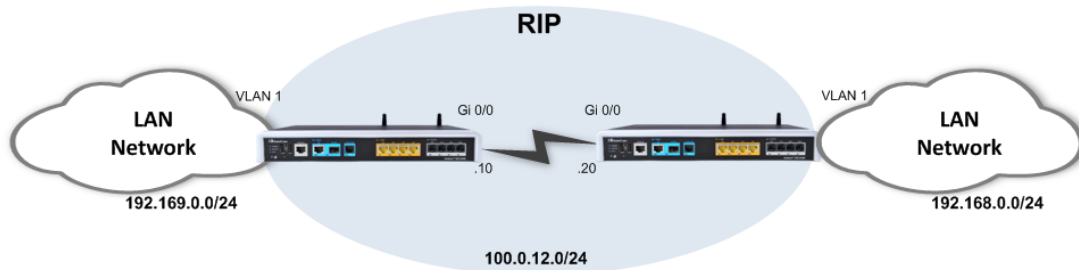
Rip general configuration:

Command	Description
# configure data	Enters the data configuration menu.
(config-data)# key chain	Rip Authentication key management.

12.1.2 Example of RIP Routing

This example demonstrates a LAN network scenario with the device, where the connection to the WAN is through RIP.

Figure 12-1: RIP Routing



12.1.2.1 Configuration

■ MSBR1:

```
MSBR1# configure data
(config-data)# router rip
(conf-router)# network vlan 1
(conf-router)# network gigabitethernet 0/0
(conf-router)# neighbor 100.0.12.20
(conf-router)# version 2
(conf-router)# timers basic 60
```

■ MSBR2:

```
MSBR2# configure data
(config-data)# router rip
(conf-router)# network vlan 1
(conf-router)# network gigabitethernet 0/0
(conf-router)# neighbor 100.0.12.10
(conf-router)# version 2
(conf-router)# timers basic 60
```

12.1.2.2 Output and show Commands

```
# show data ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
  (n) - normal, (s) - static, (d) - default, (r) -
redistribute,
  (i) - interface

      Network          Next Hop      Metric From      Tag Time
C(i) 100.0.0.0/16      0.0.0.0        1 self          0
R(n) 192.168.0.0/24    100.0.12.20    2 100.0.12.20   0
02:34
C(i) 192.169.12.0/24   0.0.0.0        1 self          0
```

A network learned
via RIP protocol

```
# show data ip rip status
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50, next due in -
1041379202 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface      Send  Recv  Key-chain
    VLAN 1         2     2
    GigabitEthernet 0/0      2     2
  Routing for Networks:
    GigabitEthernet 0/0
    VLAN 1
    100.0.12.20
  Routing Information Sources:
    Gateway      BadPackets BadRoutes  Distance Last Update
    100.0.12.20      163         0        120    00:00:08
  Distance: (default is 120)
```

List of RIP peers and parameters

12.2 OSPF Routing Protocol

Open Shortest Path First (OSPF) is a dynamic routing protocol from the Link-State family, basing its routing decisions on the bandwidth parameter using the Dijkstra Algorithm. The protocol establishes adjacencies with other OSPF routers to which it's connected, and maintains detailed topology and routing tables. OSPF provides fast network convergence and great scalability. The version of the protocol that is being used is OSPFv2 (RFC 2328).

12.2.1 Configuring OSPF

The following describes how to configure OSPF.

12.2.1.1 Router-Configuration Level

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# router ospf</code>	Enters the OSPF configuration mode.
<code>(conf-router)# area <i>area</i> authentication [message-digest]</code>	Configures authentication in the specified area.
<code>(conf-router)#area <i>area</i> default-cost <i>cost</i></code>	Configures default summary cost for stub and NSSA areas.
<code>(conf-router)#area <i>area</i> filter-list prefix <i>list</i> <in/out></code>	Configures filtering of networks between OSPF areas.
<code>(conf-router)#area <i>area</i> nssa [no-summary translate-always translate-candidate translate-never]</code>	Configures the specified area as nssa.
<code>(conf-router)# area <i>area</i> range <i>prefix/length</i> [advertise cost not-advertise substitute]</code>	Configures summarization of routes that match the specified prefix.
<code>(conf-router)#area <i>area</i> stub [no-summary]</code>	Configures the specified area as stub or totally stubby.
<code>(conf-router)# auto-cost reference-bandwidth <i>bandwidth</i></code>	Configures auto-calculation of interface cost using the provided reference cost.
<code>(conf-router)# compatible rfc1583</code>	Configures the protocol to be compatible with RFC 1583 (summary route cost calculation).
<code>(conf-router)# default-information originate [always metric metric-type route-map]</code>	Configures the advertisement of default route.
<code>(conf-router)# default-metric <i>metric</i></code>	Configures the default metric for redistributed routes.
<code>(conf-router)# distance <i>distance</i></code>	Configures the AD for OSPF routes in the system.

Command	Description
(conf-router)# distance ospf <external/inter-area/intra-area> <i>distance</i>	Configures the AD for the different types of OSPF routes in the system.
(conf-router)# log-adjacency-changes [detail]	Configures the system to log changes in OSPF peers adjacency state changes.
(conf-router)# max-metric router-lsa <administrative/on-shutdown/on-startup> <i>seconds</i>	Configures the system to advertise maximum-metric (infinite-distance) for OSPF routes.
(conf-router)# neighbor <i>address</i> [poll-interval <i>seconds</i>] [priority <i>priority</i>]	Configures neighbor IP address when connected to a non-broadcast network.
(conf-router)# network <i>prefix/length area area</i>	Configures OSPF routing and advertisement on an IP network.
(conf-router)# ospf abr-type <cisco/ibm/shortcut/standard>	Configures the OSPF ABR implementation type.
(conf-router)# ospf rfc1583compatibility	Enables the RF1583 compatibility flag (OSPF cost calculation in summarized routes).
(conf-router)# ospf router-id <i>router-id</i>	Configures the router-id for the OSPF process.
(conf-router)# passive-interface <i>interface</i>	Configures an interface to not participate in the OSPF routing.
(conf-router)# redistribute <bgp/connected/kernel/rip/static> [metric <i>metric</i>] [metric-type <i>1/2</i>] [route-map <i>map</i>]	Configures redistribution of routes from another protocol into OSPF.
(conf-router)# refresh timer <i>seconds</i>	Configures the refresh timer for LSAs in the OSPF LSDB.
(conf-router)# router-id <i>router-id</i>	Configures the router-id for the OSPF process.
(conf-router)# timers spf <i>chane delay holdtime</i>	Configures OSPF SPF timers: delay between change and calculation, and the hold-time between calculations.
(conf-router)# timers throttle spf delay initialhold maxhold	Configures the OSPF hold timers: delay from change to calculation, initial hold timer, and the maximum hold timer.

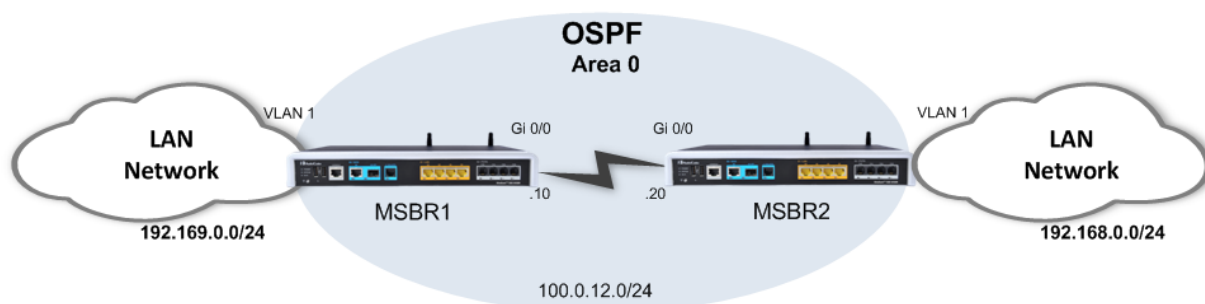
12.2.1.2 Interface-Configuration Level

Command	Description
# configure data	Enters the data configuration menu.
(config-data)# interface <i>interface</i>	Enters the interface configuration mode.
(conf-if-int)# ip ospf authentication [<i>address</i> / <i>message-digest</i> /null]	Configures the type of OSPF authentication to use on the specified interface.
(conf-if-int)# ip ospf authentication-key <i>auth-key</i>	Configures the authentication key to be used on the specified interface in case authentication is configured.
(conf-if-int)# ip ospf cost <i>cost</i>	Configures the OSPF cost for the specified interface.
(conf-if-int)# ip ospf <hello-interval/dead-interval> <i>seconds</i>	Configures the Hello and Dead timer for OSPF to use on the specified interface.
(conf-if-int)# ip ospf message-digest-key <i>key</i> md5 <i>password</i> [<i>address</i>]	Configures the MD5 key to use for message-digest authentication.
(conf-if-int)# ip ospf mtu-ignore	Configures to ignore the MTU mismatch detection on the specified interface.
(conf-if-int)# ip ospf network <broadcast/non-broadcast/point-to-multipoint/point-to-point>	Configures the network type the interface connects to (has effects on adjacency formation and message forwarding).
(conf-if-int)# ip ospf priority <i>priority</i>	Configures the OSPF priority of the specified interface (used for DR election).
(conf-if-int)# ip ospf retransmit-interval <i>seconds</i>	Configures the time between retransmitting lost LSAs.
(conf-if-int)# ip ospf transmit-delay <i>seconds</i>	Configures the link state transmit delay.

12.2.2 Example of OSPF Routing

The example shown below demonstrates a typical scenario where the device acts as a default gateway for a LAN network, and connects to the WAN network using the OSPF protocol. The example includes a single-area (area 0) OSPF network; however, in more complex and large-scale networks, multi-area topology may be more adequate in terms of scalability.

Figure 12-2: OSPF Routing



The following configuration demonstrates a basic OSPF configuration in which OSPF is activated on the LAN interfaces (for advertisement) and on the WAN interfaces (for adjacency forming). The router-ids are explicitly configured to the addresses of loopback interfaces configured on the device. Adjacency change logging is activated for debugging. The OSPF timers are configured on the WAN interfaces of the devices and should always be matched on both ends to avoid adjacency flapping.

```
*****
IP address configuration is omitted, assume it is as described in
the topology above.
*****
```

MSBR1 :

```
MSBR1# configure data
(config-data)# router ospf
(conf-router)# network 100.0.12.0/24 area 0
(conf-router)# network 192.168.12.0/24 area 0
(conf-router)# router-id 1.1.1.12
(conf-router)# log-adjacency-changes
(conf-router)# exit
(config-data)# interface gigabitEthernet 0/0
(conf-if-GE 0/0)# ip ospf hello-interval 1
(conf-if-GE 0/0)# ip ospf dead-interval 3
```

MSBR2 :

```
MSBR2# configure data
(config-data)# router ospf
(conf-router)# network 100.0.12.0/24 area 0
(conf-router)# network 192.168.12.0/24 area 0
(conf-router)# router-id 1.1.1.22
(conf-router)# log-adjacency-changes
(conf-router)# exit
(config-data)# interface gigabitEthernet 0/0
(conf-if-GE 0/0)# ip ospf hello-interval 1
(conf-if-GE 0/0)# ip ospf dead-interval 3
```

12.2.3 Useful Output and show Commands

```
MSBR2# show data ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.12	1	Full/Backup	38.143s	100.0.12.10	GigabitEthernet0/0:10.31.2.8

OSPF Neighbor Details

```
MSBR2# # sh d ip route
```

Codes: K - kernel route, C - connected, S - static,
R - RIP, O - OSPF, B - BGP

```
C 1.1.1.22/32 [1/4] is directly connected, Loopback 1
C 100.0.12.0/24 [1/3] is directly connected, GigabitEthernet
0/0
C 192.168.0.0/24 [1/4] is directly connected, VLAN 1
O 192.169.12.0/24 [110/20] via 100.0.12.10,
GigabitEthernet0/0,01:30:46
```

A network learned via
OSPF protocol

```
MSBR2# show data ip
```

OSPF Routing Process, Router ID: 1.1.1.22

Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
Initial SPF scheduling delay 200 millisec(s)
Minimum hold time between consecutive SPF's 1000 millisec(s)
Maximum hold time between consecutive SPF's 10000 millisec(s)
Hold time multiplier is currently 2
SPF algorithm last executed 1m01s ago
SPF timer is inactive
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
All adjacency changes are logged

Area ID: 0.0.0.0 (Backbone)

Number of interfaces in this area: Total: 2, Active: 2
Number of fully adjacent neighbors in this area: 1
Area has no authentication
SPF algorithm executed 8 times
Number of LSA 3
Number of router LSA 2. Checksum Sum 0x00009eee
Number of network LSA 1. Checksum Sum 0x00005e16
Number of summary LSA 0. Checksum Sum 0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000

12.3 Border Gateway Protocol (BGP)

BGP is a standardized exterior gateway protocol (EGP) for exchanging routing and reachability information between routers on different Autonomous Systems (AS's) in large scale, internet provider and public internet networks.

It does not use the metrics used by IGP protocols (such as RIP, OSPF, EIGRP, ISIS), however, makes its routing decisions based on paths, network policies and custom rules configured by network administrators.

BGP is more stable and much less “chatty” protocols than the common IGP protocols, and does not form adjacencies unless specifically configured. The formed adjacencies are connection oriented and based on TCP connections.

BGP is the main routing protocol of internet service providers and the Internet.

12.3.1 Configuring BGP

The following describes the commands for configuring BGP.

12.3.1.1 Address-Family Level Configuration (configuration can also be set without entering the AF mode)

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# router bgp as-number</code>	Enters the BGP configuration mode and the number of the local autonomous system.
<code>(conf-router)# address-family ipv4 [unicast]</code>	Enters the address-family configuration mode.
<code>(conf-router-af)# aggregate-address prefix/[length] [as-set] [summery-only]</code>	Configures BGP aggregate entries.
<code>(conf-router-af)# bgp dampening [1-45]</code>	Configures route-flap dampening.
<code>(conf-router-af)# neighbor address activate</code>	Enables the address family for the specified neighbor.
<code>(conf-router-af)# neighbor address alooas-in [occ.]</code>	Accepts as-path with local AS present in it.
<code>(conf-router-af)# neighbor address attribute-unchanged [as-path/med/next-hop]</code>	Configures unchanged propagation of the specified attribute to the neighbor.
<code>(conf-router-af)# neighbor address capability orf prefix-list <both/receive/send></code>	Advertises ORF capability to the specified neighbor.
<code>(conf-router-af)# neighbor address default-originate [route-map]</code>	Advertises default route to the specified neighbor.

Command	Description
(conf-router-af)# neighbor address filter-list name <in/out>	Configures BGP AS-Path filter list.
(conf-router-af)# neighbor address maximum-prefix num [threshold] [restart] [warning-only]	Configures a maximum number of prefixes that can be learned from the specified neighbor.
(conf-router-af)# neighbor address next-hop-self	Configures advertisement of self as next-hop for routing.
(conf-router-af)# neighbor address peer-group name	Configures as member of a peer-group.
(conf-router-af)# neighbor address prefix-list name <in/out>	Configures filtering of updates to/from the specified neighbor.
(conf-router-af)# neighbor address remove-private-as	Removes the private AS number from outbound updates.
(conf-router-af)# neighbor address route-map name <export/import/in/out>	Configures to apply a route-map to a neighbor.
(conf-router-af)# neighbor address route-reflector-client	Configures neighbor as a route reflector client.
(conf-router-af)# neighbor address route-server-client	Configures neighbor as route server client.
(conf-router-af)# neighbor address send-community [both/extended/standard]	Configures to send community attributes to the specified neighbor.
(conf-router-af)# neighbor address soft-reconfiguration inbound	Configures per-neighbor soft reconfiguration.
(conf-router-af)# neighbor address unsuppresse-map	Configures a route-map to selectively un-suppress suppressed routes.
(conf-router-af)# network prefix/[length] [route-map name]	Configures a network to be announced via BGP protocol.

12.3.1.2 General Configuration

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# router bgp as-number</code>	Enters the BGP configuration mode and the number of the local autonomous system.
<code>(conf-router)# bgp always-compare-med</code>	Configures to always compare MED attribute from different neighbors.
<code>(conf-router)# bgp bestpath <as-path/compare-routerid/med></code>	Changes the default parameter for best path selection.
<code>(conf-router)# bgp client-to-client reflection</code>	Configures Client-to-Client route reflection.
<code>(conf-router)# bgp cluster-id cluster-id</code>	Configures route-reflector cluster-id.
<code>(conf-router)# bgp confederation <peers/identifier></code>	Configures BGP confederation parameters.
<code>(conf-router)# bgp dampening [time]</code>	Configures route-flap dampening.
<code>(conf-router)# bgp default <local-preference/ipv4-unicast></code>	Configures BGP default parameters.
<code>(conf-router)# bgp deterministic-med</code>	Configures to pick best-MED path advertised from neighbors.
<code>(conf-router)# bgp enforce-first-as</code>	Configures to enforce the first AS for EBGp routes.
<code>(conf-router)# bgp fast-external-failover</code>	Configures to reset the session when a link to a directly connected neighbor goes down.
<code>(conf-router)# bgp graceful-restart [stalepath-time]</code>	Configures BGP graceful restart parameters.
<code>(conf-router)# bgp log-neighbor-changes</code>	Configures to log changes in neighbors state and reason.
<code>(conf-router)# bgp network import-check</code>	Configures BGP to check whether network route exists in IGP.
<code>(conf-router)# bgp router-id router-id</code>	Configures a router-id manually.
<code>(conf-router)# bgp scan-time sec</code>	Configures the background scanner interval.
<code>(conf-router)# distance dist [bgp internal external local]</code>	Configures the administrative distance and BGP distances.

Command	Description
<code>(conf-router)# neighbor address</code>	Configure BGP neighbor address and parameters.
<code>(conf-router)# network prefix/[length] [route-map name]</code>	Configures a network to be announced via BGP protocol.
<code>(conf-router)# redistribute protocol [metric] [route-map]</code>	Configures redistribution of routes from other routing protocols into BGP.
<code>(conf-router)#timers bgp keepalive holdtime</code>	Configures routing timers.



Note: When applying the configuration, some changes may require a process/peer clear to take effect. To perform a process clear, the following command can be used.

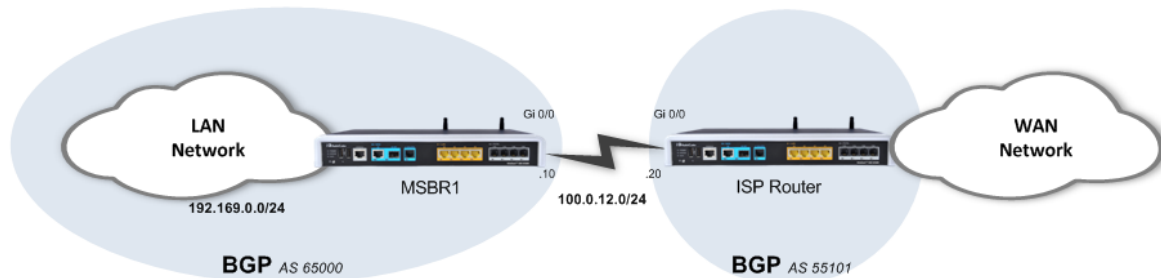
```
# clear ip bgp [AS] [address] [dampening] [external] [peer-group]
[view] [*]
```

- **AS:** Clears peers with the AS number
- **Address:** BGP neighbor IP address to clear
- **Dampening:** Clears route flap dampening information
- **External:** Clears all external peers
- **Peer-group:** Clears all members of peer-group
- **View:** BGP view
- *****: Clears all peers

It is typically recommended to use the `clear ip bgp *` command. This clears all the peers and their TCP sessions, allowing for configuration changes to take effect.

12.3.2 Example of Basic BGP WAN Connectivity

Figure 12-3: Basic BGP Routing



This example shows a basic and a very common BGP WAN connectivity. The local device establishes a BGP adjacency with the ISP router and receives a default route it, enabling it full connectivity to the “outer world”.

Usually in scenarios like this, the internal (LAN) network segment is allocated by the ISP and allows it to be routed across the ISP network.

12.3.2.1 Configuration

```
# configure data
(conf-router)# router bgp 65000
(conf-router)# bgp router-id 1.1.1.1
(conf-router)# bgp log-neighbor-changes
(conf-router)# network 100.0.12.0/24
(conf-router)# network 192.168.0.0/24
(conf-router)# neighbor 100.0.12.10 remote-as 55101
(conf-router)# exit
```

12.3.2.2 Output

The output shows local parameters of the BGP process and also the established BGP adjacencies:

```
# show data ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65000
RIB entries 3, using 264 bytes of memory
Peers 1, using 4488 bytes of memory

Neighbor      V    AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
100.0.12.10    4 55101    100     100         0    0    0
01:36:56      2

Total number of neighbors 1

#
```

The following output shows that the router learns a default route through ISP BGP peer:

```
# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

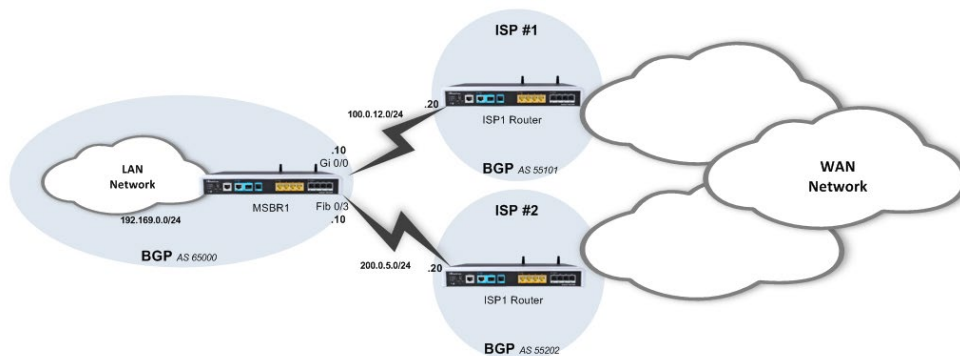
C 100.0.12.0/24 is directly connected, GigabitEthernet 0/0
C 192.168.0.0/24 is directly connected, VLAN 1
B 0.0.0.0/0 [20/0] via 100.0.12.10, GigabitEthernet 0/0,
01:30:46

#
```

12.3.3 Example 2

The example shows a scenario in which an organization is connected to the public internet through two ISPs. This is often called a Multi-WAN configuration and it provides high availability and redundancy of the internet connection. It is demonstrated that both ISPs advertise a default route through the BGP protocol, and are prioritized by manually changing the BGP Weight attribute.

Figure 12-4: BGP Multi-WAN



12.3.3.1 Configuration

```
*****
Basic Configuration omitted
*****

(conf-router)# router bgp 65000
(conf-router)# bgp router-id 1.1.1.1
(conf-router)# bgp log-neighbor-changes
(conf-router)# network 100.0.12.0/24
(conf-router)# network 200.0.5.0/24
(conf-router)# network 192.168.0.0/24
(conf-router)# neighbor 100.0.12.20 remote-as 55101
(conf-router)# neighbor 100.0.12.20 Activate
(conf-router)# neighbor 200.0.5.20 remote-as 55202
(conf-router)# neighbor 200.0.5.20 Activate

(conf-router)# neighbor 200.0.5.20 weight 200
(conf-router)# neighbor 100.0.12.20 weight 100
```

The configuration includes two important parts:

- The basic configuration defines the networks to be advertised and routed, and the neighbors to which to establish adjacency.
- The second part of the configuration deals with prioritizing the routes received from neighbors. Given the fact that a default route is received via the BGP protocols from both neighbors, you need to give one of them a higher priority (better metric). This is performed using a route-map that tweaks the “Weight” BGP attribute of incoming route-updates, and the one with the higher Weight value gets inserted into the routing table.

12.3.3.2 Output

■ BGP adjacency status:

```
# show data ip bgp sum
BGP router identifier 1.1.1.1, local AS number 65000
RIB entries 3, using 264 bytes of memory
Peers 2, using 8976 bytes of memory

Neighbor      V    AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
100.0.12.20    4 55101    120    139       0    0    0
01:04:09      1
200.0.5.20     4 55202    158    166       0    0    0
00:00:35      1

Total number of neighbors 2

#
```

■ MSBR routing table:

```
# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C 100.0.12.0/24 is directly connected, GigabitEthernet 0/0
C 192.168.0.0/24 is directly connected, VLAN 1
C 200.0.5.0/24 is directly connected, Fiber 0/3
B 0.0.0.0/0 [20/0] via 200.0.5.20, Fiber 0/3, 00:51:25

#
```

■ If the main ISP fails:

```
# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C 100.0.12.0/24 is directly connected, GigabitEthernet 0/0
C 192.168.0.0/24 is directly connected, VLAN 1
B 0.0.0.0/0 [20/0] via 100.0.12.20, GigabitEthernet 0/0, 00:00:06

#
```

12.4 Advanced Routing Examples

The following are examples of Advanced Routing.

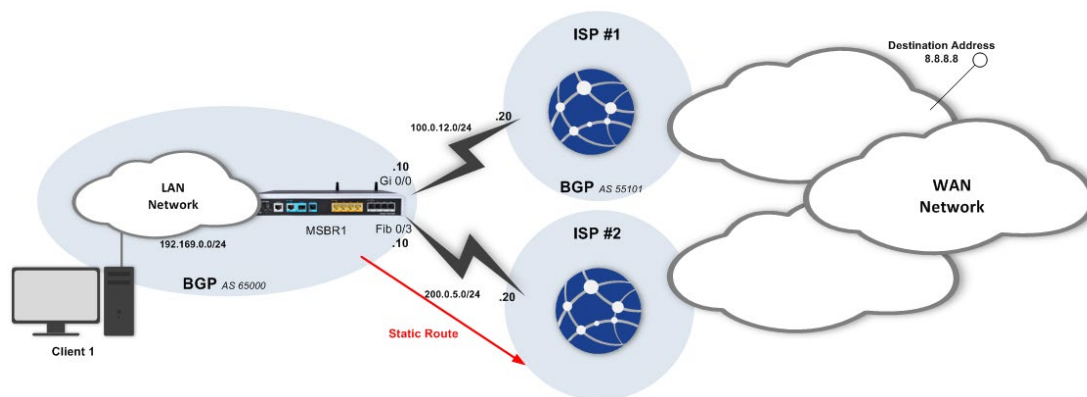
12.4.1 Multi-WAN with BGP and Static Route

This example shows a scenario with multi-WAN topology, involving two types of technologies for redundant connectivity -- BGP dynamic routing protocol static routing, where each protocol runs on a different physical interface.

This type of connectivity provides redundancy and a failover option for cases where the primary service provider fails.

Note that even though the static route should be preferred over the BGP, it is fine-tuned to be a "floating" route only for an ISP failure scenario, through fine-tuning BGP's administrative distance, and the static route's metric.

Figure 12-5: Multi-Wan with Floating Static Route



12.4.1.1 Configuration

```
*****
Basic Configuration omitted
*****
(config-data)# router bgp 65000
(conf-router)# bgp router-id 1.1.1.1
(conf-router)# bgp log-neighbor-changes
(conf-router)# network 100.0.12.0/24
(conf-router)# network 192.169.0.0/24
(conf-router)# neighbor 100.0.12.20 remote-as 55101
(conf-router)# neighbor 100.0.12.20 Activate
(conf-router)# distance bgp 1 1 1
(conf-router)# exit
(config-data)# ip route 0.0.0.0 0.0.0.0 gig 0/0 40
```

12.4.1.2 Output and Show Commands

■ Before failover:

```
# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

   B   0.0.0.0/0 [1/0] via 100.0.12.20, GigabitEthernet 0/0,
00:23:06
   C   100.0.12.0/24 [1/3] is directly connected,
GigabitEthernet 0/0
   C   200.0.5.0/24 [1/3] is directly connected, Fiber 0/1

#

Client1> traceroute 8.8.8.8

Tracing route to 10.10.10.3 over a maximum of 30 hops
 1  192.169.0.1 (192.169.0.1)  0.980 ms  0.808 ms  0.809 ms
 2  100.0.12.20 (100.0.12.20)  51.238 ms  7.115 ms  10.770 ms
.
10  8.8.8.8 (8.8.8.8)  44.878 ms  *  56.230 ms
Trace complete.
Client1>
```

■ After failover:

```
# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

   S   0.0.0.0/0 [1/40] via 200.0.5.20, Fiber 0/1
   C   100.0.12.0/24 [1/3] is directly connected,
GigabitEthernet 0/0
   C   200.0.5.0/24 [1/3] is directly connected, Fiber 0/1

#

Client1> traceroute 8.8.8.8

Tracing route to 10.10.10.3 over a maximum of 30 hops
 1  192.169.1.1 (192.169.0.1)  0.870 ms  0.807 ms  0.800 ms
 2  200.0.5.20 (200.0.5.20)  51.238 ms  7.123 ms  10.770 ms
.
10  10.10.10.3 (8.8.8.8)  44.878 ms  *  56.230 ms
Trace complete.
Client1>
```

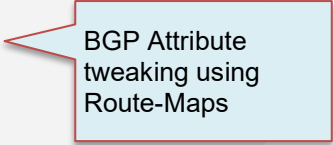
12.4.2 Filtering Dynamic Routing Protocol Routes

You can manipulate the BGP/OSPF/RIP routing advertisements using the route-map menu. Route-map contains tools to prioritize routes from specific BGP/OSPF/RIP sources, as well as denying some BGP/OSPF/RIP sources to be advertised in the device routing table. The example below demonstrates both methods:

```
*****
Basic Configuration omitted
*****

(conf-router)# ip prefix-list Example seq 5 deny host 10.10.10.10
(conf-router)# route-map Example1 permit 10
(conf-route-map)# match ip address prefix-list Example
(conf-route-map)# set weight 10
(conf-route-map)# exit
(conf-router)# route-map Example1 permit 20
(conf-route-map)# exit
(conf-router)# route-map Example2 permit 10
(conf-route-map)# match ip address prefix-list Example
(conf-route-map)# set weight 20
(conf-route-map)# exit
(conf-router)# route-map Example2 permit 20
(conf-route-map)# exit

(conf-router)# router bgp 65000
(conf-router)# bgp router-id 1.1.1.1
(conf-router)# bgp log-neighbor-changes
(conf-router)# network 100.0.12.0/24
(conf-router)# network 200.0.5.0/24
(conf-router)# network 192.168.0.0/24
(conf-router)# neighbor 100.0.12.20 remote-as 55101
(conf-router)# neighbor 100.0.12.20 Activate
(conf-router)# neighbor 100.0.12.20 route-map Example1 in
(conf-router)# neighbor 200.0.5.20 remote-as 55202
(conf-router)# neighbor 200.0.5.10 Activate
(conf-router)# neighbor 200.0.5.10 route-map Example1 in
```



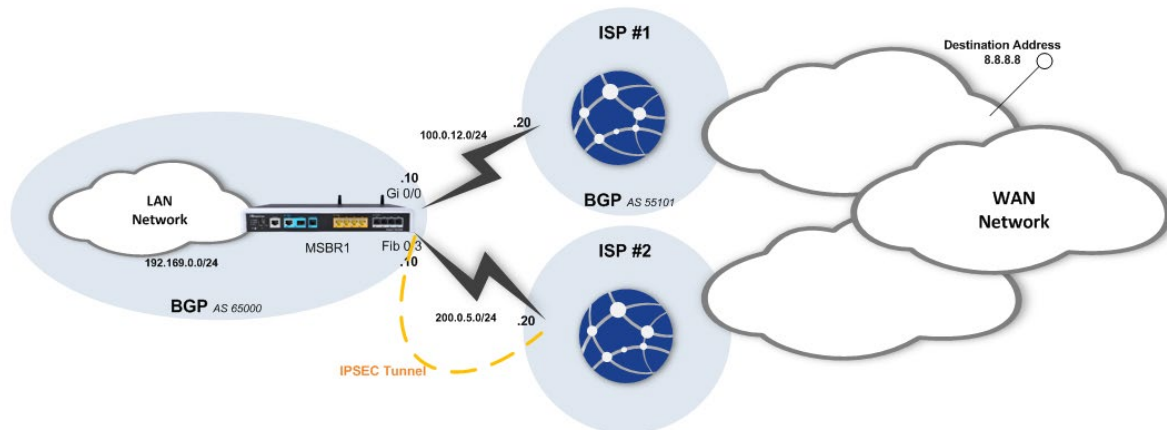
BGP Attribute
tweaking using
Route-Maps

12.4.3 Multi-WAN with BGP and IPsec

This example shows a scenario with multi-WAN topology, involving two types of technologies for redundant connectivity -- BGP dynamic routing protocol and IPsec VPN, with each protocol running on a different physical interface.

This type of connectivity provides redundancy, security on untrusted circuits and an option to fine-tune routing parameters in your network.

Figure 12-6: Multi WAN with BGP and IPsec



12.4.3.1 MSBR1 Configuration

```
configure data
access-list ipsec permit ip 192.168.0.0 0.0.0.255 any
crypto isakmp key P@ssw0rd address 10.10.10.20
crypto isakmp policy 1
  encr aes 128
  authentication pre-share
  hash sha
  group 2
  lifetime 3600
exit
crypto ipsec transform-set crypto_set1 esp-aes 128 esp-sha-hmac
mode tunnel
exit
crypto map MAP1 1 ipsec-isakmp
  set peer 10.10.10.20
  set transform-set crypto_set1
  set security-association lifetime seconds 28000
  match address ipsec
  set metric 42
exit
interface GigabitEthernet 0/0
  ip address 20.20.20.10 255.255.255.0
  mtu auto
  desc "WAN Copper"
  speed auto
  duplex auto
  no service dhcp
```



```
ip dns server static
napt
no firewall enable
no shutdown
exit
interface Fiber 0/1
ip address 10.10.10.10 255.255.255.0
mtu auto
desc "WAN Fiber"
no service dhcp
ip dns server static
crypto map MAP1
no firewall enable
no shutdown
exit
interface VLAN 1
ip address 192.168.0.1 255.255.255.0
exit
router bgp 60001
bgp router-id 20.20.20.10
network 20.20.20.0/24
neighbor 20.20.20.20 remote-as 60002
neighbor 20.20.20.20 default-originate
distance bgp 1 1 1
exit
```

12.4.3.1.1ISP1

ISP1 is used for BGP connectivity and therefore, it is configured accordingly for BGP peering with the device over the GigabitEthernet interface, and propagates a default route to the device.

12.4.3.1.2ISP2

ISP2 is used to set up an IPSec tunnel over the Fiber interface, for security and redundancy reasons. The IPSec configuration on the ISP2, in terms of key, authentication and encryption matches with the IPSec configuration on the device.

12.4.3.2 Output

```
# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C 10.10.10.20/32 is directly connected, Fiber 0/1
C 192.168.0.0/24 is directly connected, VLAN 1
C 20.20.20.0/24 is directly connected, GigabitEthernet 0/0
C 10.10.10.0/24 is directly connected, Fiber 0/1
default [42] via 10.10.10.20, Fiber 0/1 [IPSec]
B 0.0.0.0/0 [1/0] via 20.20.20.20, GigabitEthernet 0/0,
00:00:30
#
```



Note: If and when the main link fails, the default route learned through BGP is erased from the routing table and IPSec is then used as a gateway of last resort. This can be observed, for example, using Traceroute, which shows that the next-hop is through IPSec.

The following shows the Routing table after the change:

```
# show data ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C 10.10.10.20/32 is directly connected, Fiber 0/1
C 192.168.0.0/24 is directly connected, VLAN 1
C 20.20.20.0/24 is directly connected, GigabitEthernet 0/0
C 10.10.10.0/24 is directly connected, Fiber 0/1
default [42] via 10.10.10.20, Fiber 0/1 [IPSec]
#
```

13 Policy Based Routing (PBR)

Policy Based Routing (PBR) is a solution in the routing world that allows you to perform user-defined routing manipulation on specific network traffic up to various parameters, like layer-4 ports. PBR is implemented using a tool called Route-maps.

Route-maps are powerful tools for routing manipulation. Route-maps allow you to select specific traffic, by **match** at extended access-list and route it to specific interface and IP next hop (if needed).

13.1 PBR Configuration

The following describes PBR configuration.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface VLAN 1</code>	Enters VLAN 2 configuration menu.
<code>(conf-if-VLAN 2)# ip policy route-map-static name</code>	Configures the static route map for traffic that received by this interface.
<code>(conf-if-VLAN 2)# exit</code>	Exits the VLAN 2 configuration menu.
<code>(config-data)# route-map-static name</code>	Configures the static route map and enter route-map-static configuration mode.
<code>(conf-route-map-static)# match ip address ACL_name</code>	Configures the access list that select the traffic which route by the route-map.
<code>(conf-route-map-static)# set attribute value</code>	Configures the set command for traffic that passed the match condition.

Only single **match** rule can be applied in a single route-map-static, and only single **set interface** and **set next-hop** rules can be set.

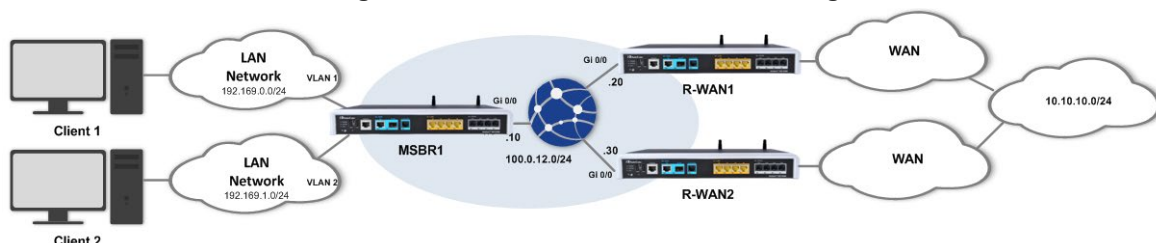
13.1.1 Example of PBR using Route-Map-Static

In this example, the device acts as a router for two LAN segments: VLAN1 and VLAN2.

The example assumes that the device needs to reach a specific destination network segment in the WAN, and a default route on the device has been configured to route regular traffic through R-WAN1, but the traffic from host 192.169.0.115 and assigned to TCP port 80, route through R-WAN2.

This is easily done using PBR and route-map-static.

Figure 13-1: PBR Source-Based Routing



13.1.1.1 Configuration

```
MSBR1# configure data
(config-data)# access-list 130 permit tcp host 192.169.0.115
0.0.0.0 255.255.255.255 eq 80
(config-data)# access-list 130 deny ip any any
(config-data)# ip route 0.0.0.0 0.0.0.0 100.0.12.20 GigabitEthernt
0/0
(config-data)# route-map-static example1
(conf-route-map-static)# match ip address 130
(conf-route-map-static)# set interface GigabitEthernt 0/0
(conf-route-map-static)# set next-hop 100.0.12.20
(conf-route-map-static)# exit
```

13.1.1.2 Output

■ Client 1:

```
Client1> traceroute 10.10.10.3

Tracing route to 10.10.10.3 over a maximum of 30 hops
 1  192.169.1.1 (192.169.1.1)  0.980 ms  0.808 ms  0.809 ms
 2  100.0.12.20 (100.0.12.20)  51.238 ms  7.115 ms  10.770 ms
 .
 .
 .
10  10.10.10.3 (10.10.10.3)  44.878 ms  *  56.230 ms
Trace complete.
Client1>
```

■ Client 2

```
Client2> traceroute 10.10.10.3

Tracing route to 10.10.10.3 over a maximum of 30 hops
 1  192.169.1.1 (192.169.1.1)  0.870 ms  0.807 ms  0.800 ms
 2  100.0.12.30 (100.0.12.30)  51.238 ms  7.123 ms  10.770 ms
 .
 .
 .
10  10.10.10.3 (10.10.10.3)  44.878 ms  *  56.230 ms
Trace complete.
Client2>
```

■ **MSBR:**

```
MSBR1# show data ip route
```

```
From input dev [VLAN 1] match up to ACL [130] route to  
[GigabitEthernet 0/0] via GW [100.0.12.20]
```

```
Codes: K - kernel route, C - connected, S - static,  
       R - RIP, O - OSPF, B - BGP
```

```
S   0.0.0.0/0 [1/1] is directly connected, PPPOE  
C   1.1.1.12/32 [1/4] is directly connected, Loopback 1  
C   100.0.12.0/24 [1/3] is directly connected,  
GigabitEthernet 0/0  
C   192.169.12.0/24 [1/4] is directly connected, VLAN 1  
C   192.169.1.0/24 [1/4] is directly connected, VLAN 2
```

```
MSBR1#
```

This page is intentionally left blank.

14 Loopback Interfaces

Loopback interfaces are logical interfaces configured by the network administrator, which in contrary to physical interfaces on the device, will always be in “Connected” and “IP” state, as they do not correspond to a physical port. Usage of loopback interfaces for management IPs, router IDs for various protocols and persistent peer IDs for neighbor relationships is considered good practice.

IP addresses on these interfaces are configured without a subnet mask, as they are by definition /32 e.g. single host subnet.

14.1.1 Loopback Interface Configuration

The following describes the commands for Loopback Interface configuration.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface loopback <i>number</i></code>	Creates a loopback interface (up to 5) and enter the interface configuration mode.
<code>(conf-if-Loopback <i>num</i>) #</code>	Interfaces configuration mode.

The configuration options available for loopback interfaces in the interface configuration mode are generally similar to those of physical interfaces, except for L1/L2 options.

14.1.2 Example of Loopback Interface Configuration

The following is an example of Loopback Interface configuration.

14.1.2.1 Configuration

```
# configure data

(config-data)# interface loopback 1
(conf-if-Loopback 1)# ip address 1.1.1.1
(conf-if-Loopback 1)# description LOOPBACK
```

14.1.2.2 Output

```
MSBR1# show data ip interfaces brief

Interface                               IP Address      Status
Protocol
GigabitEthernet 0/0                     100.0.0 .10     Connected
Up
Fiber 0/1                               unassigned      Enabled
Up
VLAN 1                                  192.168.1.1     Connected
Up
VLAN 2                                  192.169.2.1     Connected
Up
Loopback 1                             1.1.1.1        Connected
Up
```

```
MSBR1# show running-config data

configure data

*****
**
General configuration omitted
*****
**
interface Loopback 1
    ip address 1.1.1.12
    mtu auto
    desc "LOOPBACK"
    no napt
    no firewall enable
    no shutdown
exit
```

14.1.3 Example of Protocol Binding to Loopback Interfaces

The following is an example of Protocol Binding to Loopback Interfaces.

14.1.3.1 OAMP Binding to Loopback

In some cases, you may wish to bind the management protocols and interface to a loopback interface on the device, instead of a physical interface, so that management protocols and messages will have to originate from and be addressed to this loopback interface.

This can be configured as follows:

```
# configure data

(config-data)# interface loopback 1
(conf-if-Loopback 1)# ip address 1.1.1.1
(conf-if-Loopback 1)# description LOOPBACK
(conf-if-Loopback 1)#exit
(config-data)#exit
# config system
(config-system)# bind interface loopback 1 management-servers
```

14.1.3.2 BGP Termination on Loopback

It is common practice to terminate the BGP adjacency on loopback interfaces instead of the physical interfaces, which provides more stability for the connection in case of connectivity failure.

14.1.4 Configuring Loopback Interfaces to Work with Voice

In some cases it is a good practice to use telephony traffic with the loopback interface. In this case, if more than one WAN connection is being used, and one WAN connection fails, the traffic is be able to flow via the secondary connection.

For Voice traffic, NAT rules need to be created for the device to forward traffic to the Voice processor. If a global VRF is used to forward Voice traffic, the device can be configured to create these NAT rules automatically.

In order for the device to route Voice traffic via the loopback interface, the loopback needs to be bound to the saved "WAN" keyword in the voice configuration context. For this to work, the sip-interface in the voice context needs to be assigned to the WAN keyword, and loopback interface needs to be assigned to voice. In this way the device will know to route the voice traffic from LAN to WAN and vice versa using the Loopback interface.

The following is the required configuration to bind the loopback configuration to WAN keyword.

➤ **To bind the loopback configuration to WAN keyword:**

1. Bind the SIP interface to the WAN keyword.

```
# conf voip
MSBR(config-voip)# sip-interface 2
(sip-interface-2)# network-interface "WAN"
Note: Changes to this parameter will take effect when applying
the 'activate' or 'exit' command
(sip-interface-2)# exit
(config-voip)# exit
#
```

2. Configure the Loopback as WAN.

```
# configure data
MSBR(config-data)# interface loopback 1
(conf-if-Loopback 1)# network wan
(conf-if-Loopback 1)# exit
(config-data)# exit
#
```

3. Bind the loopback interface to the WAN.

```
# configure network
MSBR(config-network)# bind interface loopback 1 voip
Note: Changes will take effect after reset.
(config-network)*# exit
MSBR*#
```

4. Reset the router for the configuration to take effect.

To check that the configuration took effect, use the “show run” command. At the bottom of the data configuration, the ports used by system services are shown.

```
# Note: The following WAN ports are in use by system
services,
#      conflicting rules should not be created:
#      Ports 80 - 80 --> HTTP
#      Ports 23 - 23 --> Telnet CLI
#      Ports 22 - 22 --> SSH CLI
#      Ports 82 - 82 --> TR069
#      Ports 6000 - 6090 --> RealmPortPool::MR_WAN
#      Ports 5060 - 5060 --> SIPUDP#2
#      Ports 5060 - 5060 --> SIPLISTENING#2
#      Ports 5061 - 5061 --> SIPLISTENING#2
```

5. To see the WAN binding, use the “show voip wan-bindings” command:

```
# show network wan-bindings
WAN interface was defined by configuration (Loopback 1, ip
address 0.0.0.0)
The following WAN ports are in use by VOIP services:
  Ports 6000 - 6090 --> RealmPortPool::MR_WAN
  Ports 5060 - 5060 --> SIPUDP#2
  Ports 5060 - 5060 --> SIPLISTENING#2
  Ports 5061 - 5061 --> SIPLISTENING#2
```



Note: This feature cannot be used with VRFs other than global. If other than global VRFs are used, the port forwarding rules need to be added manually for all VoIP inbound and outbound traffic.

15 Virtual Routing and Forwarding (VRF)

VRF is an IP feature that is included in IP network routers, which allows the simultaneous existence and work of multiple routing tables on a single physical router. This can be visualized, in general and simple terms, as several logical routers inside a physical one.

Because of this separation to different routing and forwarding tables, this feature allows the creation of different networks and segments without using multiple devices, creation of VPNs, and isolation of different network segments for better security due to the fact that no data is transferred from one VRF to another, and much more.

In addition, to utilize this separation of routing and forwarding tables, many components and configuration objects can be associated with different VRFs on the same device, such as physical and logical interfaces, static routes, prefix-lists and routing protocol instances.

On the device's MAIN-VRF by default, BGP, OSPF, RIP services exist. The device supports up to five additional VRFs. For all additional VRFs, the user can enable up to five dynamic routing services. For example, if VRF "BLUE" has BGP enabled towards the WAN and RIP towards the LAN, the other VRFs will have cumulatively only three services remaining for use.

15.1.1 VRF Configuration

The following describes the VRF configuration commands.

15.1.1.1 Global Configuration

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# ip vrf vrf-name</code>	Creates a VRF instance.
<code>(config-data)# ip vrf vrf-name enable <ospf/rip/bgp></code>	Enables a routing protocol on the VRF instance.

15.1.1.2 Interface Configuration

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface int-name</code>	Enters the interface configuration mode.
<code>(conf-if-name)# ip vrf forwarding vrf-name</code>	Associates the interface with a specific VRF.

15.1.1.3 Other

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# ip route vrf - vrf-name destination mask next-hop interface</code>	Associates a static route with a VRF instance.

Command	Description
<code>(config-data)# ip prefix-list list-name vrf vrf-name action prefix/length</code>	Associates a prefix-list with a VRF instance.
<code>(config-data)# route-map <name> vrf vrf-name</code>	Associates a route-map with a VRF.
<code>(config-data)# router ospf bgp rip vrf vrf-name</code>	Associates a BGP/OSPF/RIP routing-instance with a VRF.

Also the show commands of the above configurations and the following utilities: **Ping**, **Traceroute**, **Copy** files, **debug capture data physical**, **show data mac** table.

15.1.2 VRF App Awareness

The device VRF App awareness is essentially the ability to perform ICMP commands (such as ping, and traceroute) with a **vrf** attribute, enabling VRF-specific reachability and connectivity testing. Note that ICMP packets are not routed from one VRF to another.

The operation is performed according to the ICMP ping and traceroute command syntax, for example:

```
# ping 192.168.0.1 source data vrf blue
4 packets transmitted, 0 packets received

#
```

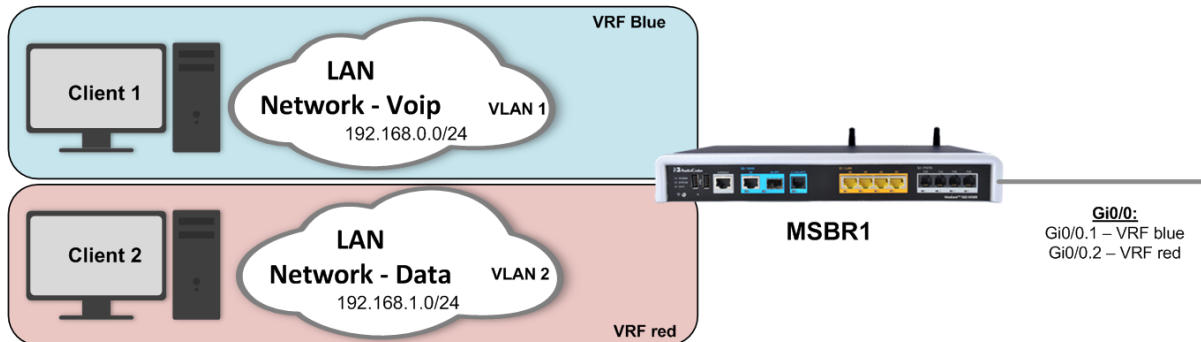
15.1.3 Example of Segment Isolation using VRF

This example includes two hosts, each connected to a separate VLAN. On the device, Layer-3 interface VLANs for the two VLANs are configured where each interface VLAN is associated to a different VRF.

Without a VRF configuration, there would be routing between the two Layer-3 interfaces where if Workstation 1 tries to reach Workstation 2 (with ICMP Ping, for example) it would get an answer.

In the example, Layer-3 VLAN interfaces are associated with different VRFs and belong to different routing tables. The device isolates them from one another, and if ICMP reachability is checked, an Unreachable message is received.

Figure 15-1: Segment Isolation using VRF



15.1.3.1 Configuration

```
# configure data
(conf-data)# ip vrf blue
(conf-data)# ip vrf red
(conf-data)# interface VLAN 1
(conf-if-VLAN 1)# ip address 192.169.0.1 255.255.255.0
(conf-if-VLAN 1)# desc "VLAN 1 - Lan segment 1"
(conf-if-VLAN 1)# ip vrf forwarding blue
(conf-if-VLAN 1)# exit
(conf-data)# interface VLAN 2
(conf-if-VLAN 2)# ip address 192.169.1.1 255.255.255.0
(conf-if-VLAN 2)# desc "VLAN 2 - Lan segment 2"
(conf-if-VLAN 2)# ip vrf forwarding red
(conf-data)# interface gi 0/0.1
(conf-if-VLAN 2)# desc "vlan 1 - WAN"
(conf-if-VLAN 2)# ip vrf forwarding blue
(conf-data)# interface gi 0/0.2
(conf-if-VLAN 2)# desc "vlan 2 - WAN"
(conf-if-VLAN 2)# ip vrf forwarding red
```

15.1.3.2 Output

```
Client 1>ping 192.169.0.100
```

```
Pinging 192.169.0.100 with 32 bytes of data:
Request timed out.
```

```
Ping statistics for 192.169.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Client 1>
```

```
Client 2>ping 192.169.1.100
```

```
Pinging 192.169.1.100 with 32 bytes of data:
Request timed out.
```

```
Ping statistics for 192.169.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
Client 2>
```

```
# show data ip vrf
```

```
VRF - blue
```

```
Interfaces: VLAN 1  GigabitEthernet 0/0.1
Enabled protocols:
```

```
VRF - red
```

```
Interfaces: VLAN 2  GigabitEthernet 0/0.2
Enabled protocols:
```

```
#
```

```
# show data ip route vrf blue
```

```
Codes: K - kernel route, C - connected, S - static,
        R - RIP, O - OSPF, B - BGP
```

```
C   192.169.0.0/24 is directly connected, VLAN 1
```

```
#
```

```
# show data ip route vrf red
```

```
Codes: K - kernel route, C - connected, S - static,
        R - RIP, O - OSPF, B - BGP
```

```
C   192.169.1.0/24 is directly connected, VLAN 2
```

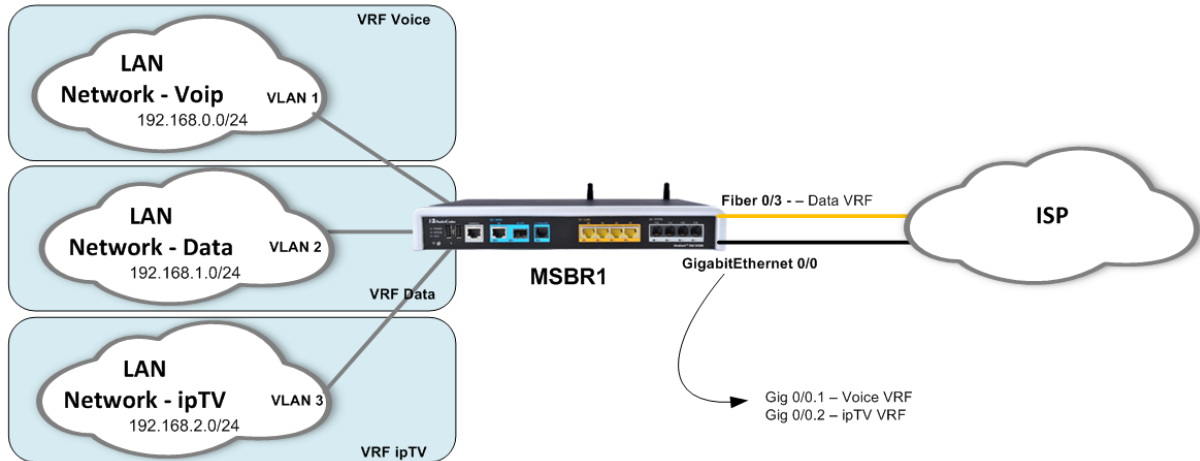
```
#
```

15.1.4 Routing Services on Different VRF'S

This example shows a scenario in which there are several LAN segments connected to the device via different VLANs, which are associated with different VRFs. The Data VRF has BGP connectivity to the ISP and RIP protocol for routing on the LAN. The ipTV VRF has a static route towards the ISP and OSPF routing protocol for the LAN network.

This is a conceptual scenario to show how to provide different services using different protocols on different VRFs.

Figure 15-2: Routing Services on Different VRFs



15.1.4.1 Configuration

The configuration regarding the VRFs and their associated protocols is shown below. Standard protocol and addressing configuration is omitted and can be observed in their respective chapters in this guide.

```
(config-data)# ip vrf DATA enable bgp
(config-data)# ip vrf DATA enable rip
(config-data)# ip vrf VOICE
(config-data)# ip vrf IPTV enable ospf
(config-data)# interface vlan 1
(config-if-VLAN-1)# ip address 192.168.0.1 255.255.255.0
(config-if-VLAN-1)# ip vrf forwarding DATA
(config-if-VLAN-1)# exit
(config-data)# interface vlan 2
(config-if-VLAN-2)# ip address 192.168.1.1 255.255.255.0
(config-if-VLAN-2)# ip vrf forwarding VOICE
(config-if-VLAN-2)# exit
(config-data)# interface vlan 3
(config-if-VLAN-3)# ip address 192.168.3.1 255.255.255.0
(config-if-VLAN-3)# ip vrf forwarding IPTV
(config-if-VLAN-3)# exit
(config-data)# interface gigabitethernet 0/0.1
(config-if-GE 0/0.1)# ip address 100.0.0.1 255.255.255.0
(config-if-GE 0/0.1)# ip vrf forwarding VOICE
(config-if-GE 0/0.1)# exit
(config-data)# interface gigabitethernet 0/0.2
(config-if-GE 0/0.2)# ip address 100.0.1.1 255.255.255.0
(config-if-GE 0/0.2)# ip vrf forwarding IPTV
(config-if-GE 0/0.2)# exit
```

```
(config-data)#interface fiber 0/3
(config-if-Fi 0/3)#ip address 200.0.0.1 255.255.255.0
(config-if-Fi 0/3)#ip vrf forwarding DATA
(config-if-Fi 0/3)# napt
(config-if-Fi 0/3)# firewall enable
(config-if-Fi 0/3)#exit
(config-data)# router ospf vrf IPTV

*****
Standard protocol configuration - omitted
*****

(config-data)# router rip vrf DATA
```

```
*****
Standard protocol configuration - omitted
*****

(config-data)# router bgp 65000 vrf DATA

*****
Standard protocol configuration - omitted
*****

(config-data)#
```

15.1.4.2 Output

```
# show data ip vrf

VRF - DATA
Interfaces: VLAN 1 Fiber 0/3
Enabled protocols: bgp rip

VRF - VOICE
Interfaces: VLAN 2 GigabitEthernet 0/0.1
Enabled protocols:

VRF - IPTV
Interfaces: VLAN 3 GigabitEthernet 0/0.2
Enabled protocols: ospf

#
```


16 GRE Tunnels

The device supports GRE tunnels. Tunnels are a type of interface where when there is a proper and working IP connectivity between its two ends, appears as directly connected to the “other side”, even if there are multiple different IP networks between them. GRE tunnels are tunnels that use a special encapsulation on the IP packets.

16.1.1 Configuring GRE Tunnels

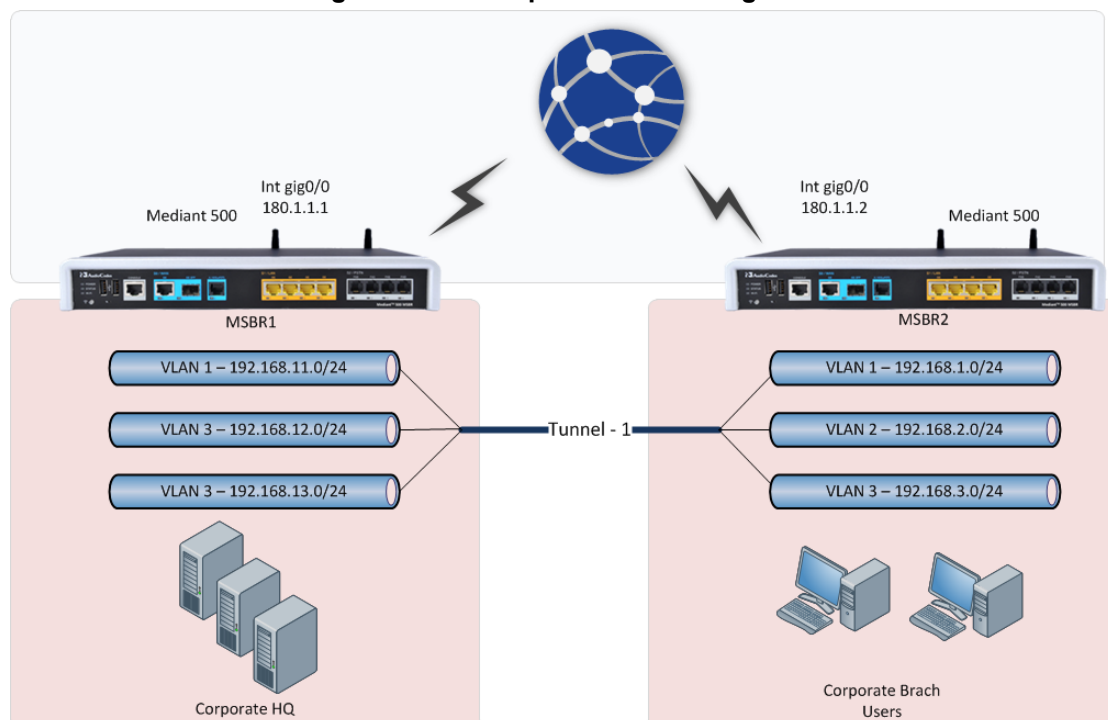
The following describes the commands for configuring GRE Tunnels.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface gre <number></code>	The device supports up to 255 GRE interfaces. The GRE interfaces can be a number from 1 to 255.
<code>(conf-if-GRE 1)# ip address <IP> <MASK></code>	Configures the IP address of the GRE interface. The mask is not mandatory and if not stated the default value of 255.255.255.255 is applied.
<code>(conf-if-GRE 1)# tunnel destination <IP></code>	Configures the destination IP for the tunnel interface. The tunnel is created for this address.

16.1.2 Example of Connecting Multiple Subnets using GRE

This example describes the configuration of the next topology, where three different subnets are connected using GRE tunnels. Note that for a GRE tunnel to work properly, you must have a route to the tunnel destination.

Figure 16-1: Multiple Subnets using GRE



16.1.2.1 Configuration

■ MSBR1:

```
MSBR1# conf d
(config-data)# int gigabitethernet 0/0
(config-if-GE 0/0)# ip address 180.1.1.1 255.255.255.0
(config-if-GE 0/0)# no firewall enable
(config-data)# int vla 1
(config-if-VLAN 1)# ip address 192.168.11.1 255.255.255.0
(config-if-VLAN 1)# exit
(config-data)# int vla 2
(config-if-VLAN 2)# ip address 192.168.12.1 255.255.255.0
(config-if-VLAN 2)# no shutdown
(config-if-VLAN 2)# exit
(config-data)# int vla 3
(config-if-VLAN 3)# ip address 192.168.13.1 255.255.255.0
(config-if-VLAN 3)# no shutdown
(config-if-VLAN 3)# exit
(config-data)# interface gre 1
(config-if-GRE 1)# ip address 1.1.1.1 255.255.255.0
(config-if-GRE 1)# tunnel destination 180.1.1.2
(config-if-GRE 1)# no shutdown
(config-if-GRE 1)# exit
(config-data)# ip route 192.168.1.0 255.255.255.0 gre 1
(config-data)# ip route 192.168.2.0 255.255.255.0 gre 1
(config-data)# ip route 192.168.3.0 255.255.255.0 gre 1
```

■ MSBR2:

```
MSBR2# conf d
(config-data)# int gigabitethernet 0/0
(config-if-GE 0/0)# ip address 180.1.1.2 255.255.255.0
(config-if-GE 0/0)# no firewall enable
(config-data)# int vla 1
(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0
(config-if-VLAN 1)# exit
(config-data)# int vla 2
(config-if-VLAN 1)# ip address 192.168.2.1 255.255.255.0
(config-if-VLAN 1)# no shutdown
(config-if-VLAN 1)# exit
(config-data)# int vla 3
(config-if-VLAN 1)# ip address 192.168.3.1 255.255.255.0
(config-if-VLAN 1)# no shutdown
(config-if-VLAN 1)# exit
(config-data)# interface gre 1
(config-if-GRE 1)# ip address 1.1.1.2 255.255.255.0
(config-if-GRE 1)# tunnel destination 180.1.1.1
(config-if-GRE 1)# no shutdown
(config-if-GRE 1)# exit
(config-data)# ip route 192.168.11.0 255.255.255.0 gre 1
(config-data)# ip route 192.168.12.0 255.255.255.0 gre 1
(config-data)# ip route 192.168.13.0 255.255.255.0 gre 1
```

16.1.2.2 Output

■ IP routing table of MSBR1:

```
MSBR1# sh d ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C    180.1.1.0/24 is directly connected, GigabitEthernet 0/0
S    192.168.1.0/24 [1/1] is directly connected, GRE 1
S    192.168.2.0/24 [1/1] is directly connected, GRE 1
S    192.168.3.0/24 [1/1] is directly connected, GRE 1
C    192.168.11.0/24 is directly connected, VLAN 1
C    192.168.12.0/24 is directly connected, VLAN 2
C    192.168.13.0/24 is directly connected, VLAN 3
```

■ IP routing table of MSBR2:

```
MSBR2# sh d ip route
Codes: K - kernel route, C - connected, S - static,
       R - RIP, O - OSPF, B - BGP

C    180.1.1.0/24 is directly connected, GigabitEthernet 0/0
C    192.168.1.0/24 is directly connected, VLAN 1
C    192.168.2.0/24 is directly connected, VLAN 2
C    192.168.3.0/24 is directly connected, VLAN 3
S    192.168.11.0/24 [1/1] is directly connected, GRE 1
S    192.168.12.0/24 [1/1] is directly connected, GRE 1
S    192.168.13.0/24 [1/1] is directly connected, GRE 1
MSBR2#
```

To verify a connection among networks, you can ping each network from the device:

```
MSBR1# ping 192.168.11.1
Reply from 192.168.11.1: time=0 ms
Reply from 192.168.11.1: time=0 ms
Reply from 192.168.11.1: time=0 ms
3 packets transmitted, 3 packets received
Round-trip min/avg/max = 0/0/0 ms
```

```
MSBR1# ping 192.168.12.1
Reply from 192.168.12.1: time=0 ms
Reply from 192.168.12.1: time=0 ms
Reply from 192.168.12.1: time=0 ms
MSBR1# Reply from 192.168.12.1: time=0 ms
4 packets transmitted, 4 packets received
Round-trip min/avg/max = 0/0/0 ms
```

```
MSBR1# ping 192.168.13.1
Reply from 192.168.13.1: time=0 ms
Reply from 192.168.13.1: time=0 ms
Reply from 192.168.13.1: time=0 ms
3 packets transmitted, 3 packets received
Round-trip min/avg/max = 0/0/0 ms
MSBR1#
```

This page is intentionally left blank.

17 Quality of Service (QoS)

In modern networks, different types of traffic are transported over the same infrastructure: Data, Voice, Video, latency sensitive, application specific and more. In cases of network congestion, some amount of data may be delayed or dropped and retransmitted, and while some kinds of traffic are tolerant to this phenomenon, others such as video and voice are sensitive to it.

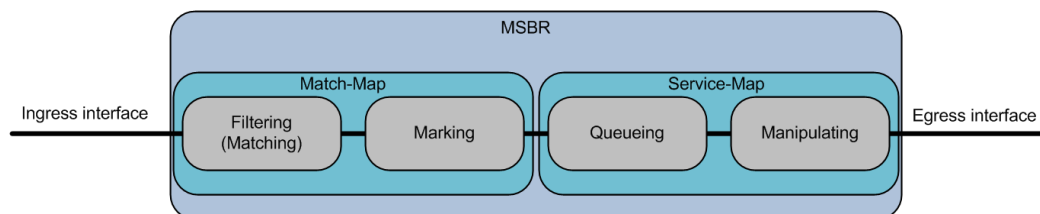
QoS is a set of mechanisms to handle the prioritization of some traffic over another to make sure it gets the amount of network bandwidth it requires, proper latency, etc.

It is important to be familiar with several concepts that are crucial for the QoS process:

- Traffic filtering: the first step in the QoS mechanism. You need to filter and define the preferred traffic"; basically stating which traffic should receive the special priority handling. This step is usually performed using ACLs, VLAN-Priority or the DSCP value.
- The DiffServ (the system behind DSCP) is a computer networking mechanism for classifying, managing and providing QoS for data in IP networks in layer 3, while TOS is quite similar, however uses a slightly different terminology and rating for traffic in layer 2.

The usual event flow of the QoS mechanism is as follows:

Figure 17-1: QOS Handling Flow-Chart



Match-maps bind the “match” statements with marking rules, meaning that once there are rules matching the specified traffic, you can mark it for further processing, using the DSCP system.

After the marking, the actual QoS mechanism is activated using the service-map objects, which are configured on the physical egress interface and contain the actual queues to which the different traffic is divided. For each queue the following actions can be performed:

- **Shaping:** assuring an amount of bandwidth for the specified traffic – usually media requires minimal bandwidth.
- **Prioritization:** setting different priorities for different traffic associated with different queues, thus providing lower delay for higher priority traffic.
- **Drop policy and queue scheduling:** setting rules for planned packet drop or sharing the bandwidth according to user-defined thresholds.



Note: It is considered good practice to perform the **matching** as close to the ingress interface as possible, and the manipulation on the physical egress interface.

17.1.1 QoS Configuration

The QoS configuration consists of several steps:

1. Defining interesting traffic.
2. Marking it.
3. Configuring a shaping policy
4. Applying it.

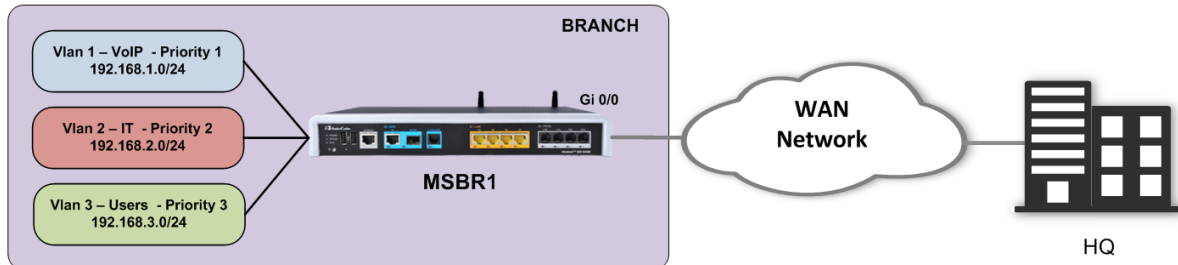
The following table describes the QoS CLI commands.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# access-list <i>acl-name</i> permit <i>protocol src dst</i> <eq/range/dscp/established/log/stat eless></code>	Configures an access-list to filter the requested “interesting traffic”.
<code>(config-data)# qos match-map <in/out> <i>map-name interface</i></code>	Configures a match-map for the QoS mechanism.
<code>(conf-m-map)# match < access-list/ any/ dscp/ length/ precedence/ priority></code>	Configures match clauses for the match-map.
<code>(conf-m-map)# set < dscp/ precedence/ priority/ queue></code>	Configures the marking for the matched traffic.
<code>(config-data)# qos service-map <i>interface output</i></code>	Configures a service-map.
<code>(conf-s-map)# bandwidth <i>bw</i></code>	Configures the maximum bandwidth for the service-map.
<code>(conf-s-map)# queue <<i>name/default</i>></code>	Configures the queue for the service-map and enter the queue configuration mode.
<code>(conf-s-map-q)# [bandwidth <i>bw</i> policy <i>policy</i> priority <i>priority</i>]</code>	Configures queue parameters.

17.1.2 Example of Weighted Bandwidth Sharing

This example includes a branch office with several network segments: VoIP, IP and Users, connected to VLANs 1, 2, and 3, respectively. The WAN interface bandwidth needs to be shared according to the network administrator's design and functional requirements, which in this example, is 40% for VoIP, 40% for IT, and 20% for Users.

Figure 17-2: Weighted QOS Handling



17.1.2.1 Configuration

```
(config-data)# ip access-list VLAN1_IN permit ip any any log
(config-data)# ip access-list VLAN2_IN permit ip any any log
(config-data)# ip access-list VLAN3_IN permit ip any any log
(config-data)# qos match-map input QOS_VOIP vlan 1
(conf-m-map)# match access-list VLAN1_IN
(conf-m-map)# set queue VoIP
(conf-m-map)# exit
(config-data)# qos match-map input QOS_IT vlan 2
(conf-m-map)# match access-list VLAN2_IN
(conf-m-map)# set queue IT
(conf-m-map)# exit
(config-data)# qos match-map input QOS_USR vlan 3
(conf-m-map)# match access-list VLAN3_IN
(conf-m-map)# set queue USR
(conf-m-map)# exit
(config-data)# qos service-map gigabitethernet 0/0 output
(conf-s-map)# queue default
(conf-s-map-q)# priority 4
(conf-s-map-q)# exit
(conf-s-map)# queue VoIP
(conf-s-map-q)# priority 1
(conf-s-map-q)# bandwidth percent 40
(conf-s-map-q)# exit
(conf-s-map)# queue IT
(conf-s-map-q)# priority 2
(conf-s-map-q)# bandwidth percent 40
(conf-s-map-q)# exit
(conf-s-map)# queue USR
(conf-s-map-q)# priority 3
(conf-s-map-q)# bandwidth percent 20
(conf-s-map-q)# exit
(conf-s-map)# exit
(config-data)#
```

17.1.2.2 Output

```
# show data qos match-map
match-map input QOS_VOIP vlan 1
  match access-list VLAN1_IN
  set queue VOIP
match-map input QOS_IT vlan 2
  match access-list VLAN2_IN
  set queue IT
match-map input QOS_USR vlan 3
  match access-list VLAN3_IN
  set queue USR
#
```

```
# show data qos service-map
LAN service map:
service map does not exist
WAN service map:
GigabitEthernet 0/0:
service map maximum bandwidth 100000
default queue:
  STRICT PRIORITY    priority 4
  reserved bandwidth 0 kbps maximum bandwidth is unlimited
VOIP queue:
  STRICT PRIORITY    priority 1
  reserved bandwidth 40 percent maximum bandwidth is unlimited
IT queue:
  STRICT PRIORITY    priority 2
  reserved bandwidth 40 percent maximum bandwidth is unlimited
USR queue:
  STRICT PRIORITY    priority 3
  reserved bandwidth 20 percent maximum bandwidth is unlimited
Fiber 0/1:
service map does not exist
#
```

```
# show data qos queue
Global statistics for LAN Queues:
No available queue statistics.

Global statistics for WAN Queues:
GigabitEthernet 0/0:
  queue name|sent packets|sent bytes|packet rate|rate(bytes/s)|packets
  delayed|packets dropped
  -----|-----|-----|-----|-----|-----
  Default   | 1           | 1234    | 20        | 40          | 0
  | 0
  VOIP      | 38          | 56378   | 16        | 32          | 0
  | 0
```



```

IT          | 24          | 35436      | 6          | 15          | 0
| 0
USR         | 1           | 34         | 4          | 10          | 0
| 0

```

```

Fiber 0/1:
No available queue statistics.

```

```

EFM 0/2:
No available queue statistics.

```

```

Note: Queue name may be truncated (limited to 20 characters).

```

```

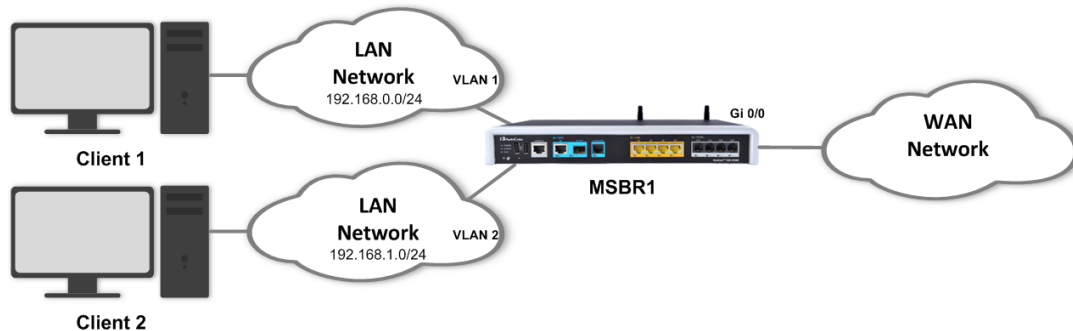
#

```

17.1.3 Example using QoS to Ensure Bandwidth for Critical Traffic

This example assumes two PC workstations, each on a different VLAN and subnet. Client 1 is running a very important and sensitive application that requires a minimum of 2 Mbits of network bandwidth for proper operation. Based on the mechanisms described in this chapter, a policy is configured to ensure the client obtains the required bandwidth.

Figure 17-3: QoS Bandwidth Shaping



17.1.3.1 Configuration

```

# configure data
(config-data)# access-list exampleList1 permit ip 192.168.0.3
0.0.0.0 any
(config-data)# qos match-map output mMap1 gigabitethernet 0/0
(conf-m-map)# match access-list exampleList1
(conf-m-map)# set queue ex1
(conf-m-map)# exit
(config-data)# qos service-map gigabitethernet 0/0 output
(conf-s-map)# queue ex1
(conf-s-map-q)# bandwidth 2048
(conf-s-map-q)# exit
(conf-s-map)# exit
(config-data)#

```

17.1.3.2 Output

```

# show data qos match-map gigabitethernet 0/0
match-map output mMap1 GigabitEthernet 0/0

```

```

match access list ex1
set queue ex1

#

# show data qos service-map
LAN service map:
service map does not exist
WAN service map:
GigabitEthernet 0/0:
service map maximum bandwidth 100000
default queue:
    STRICT PRIORITY    priority 4
    reserved bandwidth 0 kbps maximum bandwidth is unlimited
ex1 queue:
    STRICT PRIORITY    priority 4
    reserved bandwidth 2048 kbps maximum bandwidth is unlimited
Fiber 0/3:
service map does not exist

#

```

17.1.4 Remarking DSCP/P-bit for Exceeded Traffic (Over the Reserved Bandwidth)

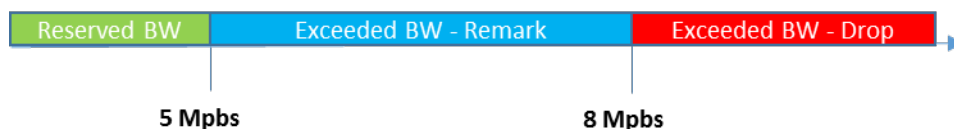
This feature allows you to remark DSCP packets and/or VLAN priority bit for traffic that exceeds the queue reserved traffic. Using this feature the service provider's network is able to determine how much traffic exceeded the reserved (committed) rate, by looking into the DSCP and P-bit fields.

The following example configures QOS parameters where remarking exceeded Bandwidth PBIT (to 6) and DSCP (to af11).

```

conf data
qos match-map output REMARK GigabitEthernet 0/0.500
match any
set queue QUEUE
exit
qos service-map GigabitEthernet 0/0 output
bandwidth 1000
queue QUEUE
bandwidth 5000 8000
priority 0
remark-above-reserved pbit 6
remark-above-reserved dscp af11

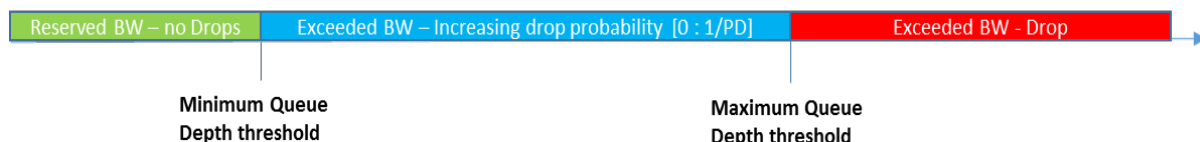
```



17.1.5 Weighted Random Early Detect

This feature allows you to define **Weighted Random Early Detection (WRED)** QOS queues. Three parameters control the drop probability of the queue as a function of the actual queue depth (measured in packets):

- **Minimum:** Below this queue depth, there is no drop probability.
- **Maximum:** Above it, there is a 100% drop probability.
- **Probability Denominator (PD):** Between minimum and maximum there is a linearly increasing drop probability from 0 to the probability defined by this parameter. The closer you get to Maximum, the more the drop probability will be close to the $1 / PD$ parameter.



Configuration Example 1: 2 RED Queues, 1 Priority Queue. Fixed Minimum and Maximum parameters, with a different Probability.

```
qos service-map lan output
  bandwidth 100000
  queue "default"
    priority 4
  exit
  queue "SOURCE1_Q"
    policy random-detect 25 100 2
    priority 0
    bandwidth 20000 20000
  exit
  queue "SOURCE2_Q"
    policy random-detect 25 100 8
    priority 0
    bandwidth 20000 20000
  exit
  queue "SOURCE3_Q"
    policy strict-priority
    priority 0
    bandwidth 20000 20000
  exit
exit
```

Traffic results example: 1000 TCP streams per Queue.

Global statistics for LAN Queues:

queue name	sent packets	sent bytes	packet rate	rate(kbit/s)	packets delayed	packets dropped
default_tx	90	4140	0	0	0	0 C(0) A(0) M(0)
SOURCE1_Q	6761484	10247593467	1648	20003	0	2209547 C(47) A(62) M(122)
SOURCE2_Q	6762575	10247411293	1648	20002	0	1939996 C(94) A(98) M(136)
SOURCE3_Q	6765065	10247373811	1648	20000	0	1223042 C(0) A(0) M(0)

SOURCE1_Q has more losses since its probability is 50% and unable to fully utilize the queue and not reaching the end of the queue (at average 62 queue depth). SOURCE2_Q has less losses and fully utilizes the queue (average of 98 queue depth).

Configuration Example 2 - 2 RED Queues, 1 Priority Queue. Different Minimum, Fixed Maximum and Probability parameters.

```

qos service-map lan output
  bandwidth 100000
  queue "default"
    priority 4
  exit
  queue "SOURCE1_Q"
    policy random-detect 25 100 4
    priority 0
    bandwidth 20000 20000
  exit
  queue "SOURCE2_Q"
    policy random-detect 50 100 4
    priority 0
    bandwidth 20000 20000
  exit
  queue "SOURCE3_Q"
    policy strict-priority
    priority 0
    bandwidth 20000 20000
  exit
exit

```

Traffic results example: 1000 TCP streams per Q.

Global statistics for LAN queues:

queue name	sent packets	sent bytes	packet rate	rate(kbit/s)	packets delayed	packets dropped
default_tx	2889	315422	0	0	0	0 C(0) A(0) M(0)
SOURCE1_Q	124892660	189312706281	1649	20012	0	40161685 C(105) A(94) M(132)
SOURCE2_Q	124890615	189309118795	1649	20012	0	40109207 C(97) A(95) M(125)
SOURCE3_Q	124954862	189306607169	1650	20011	0	25147954 C(0) A(0) M(0)

SOURCE1_Q has more losses since its minimum is lower, thus dropping starts earlier. But both queues utilizing their entire average depth since the PD is not too aggressive.

17.1.6 QoS on Mediant 500Li MSBR

17.1.6.1 Weighted Fair Queuing

There are several differences for QoS configuration between Mediant 500Li MSBR and the other Mediant MSBRs.

Mediant 500Li includes a policy called Weighted Fair Queuing (WFQ). This policy works with relative weight for the queue. The bandwidth assigned to queue is calculated as follows:

$$BW_{queue} = \frac{\text{weight of the queue}}{\text{sum of weights of all queues}} \times BW_{total}$$

Configuration example:

```
qos service-map GigabitEthernet 0/0 output
bandwidth 50000
queue "def_queue"
  priority 4
exit
queue "q1"
  policy wfq 20
  priority 1
exit
queue "q2"
  policy wfq 30
  priority 2
exit
queue "q3"
  policy wfq 10
  priority 3
exit
exit
```

The maximum bandwidth for q1 is:

$$BW_{queue\ 1} = \frac{20}{(20 + 30 + 10)} \times 50Mbps = 16\frac{2}{3} Mbps$$

The maximum bandwidth for q2 is:

$$BW_{queue\ 1} = \frac{30}{(20 + 30 + 10)} \times 50Mbps = 25 Mbps$$

The maximum bandwidth for q3 is:

$$BW_{queue\ 1} = \frac{10}{(20 + 30 + 10)} \times 50Mbps = 8\frac{1}{3} Mbps$$

The following describes the limitations of QoS operation for Mediant 500Li:

- It's not possible to set the minimum bandwidth for the QoS policy
- It's not possible to create two queues with the same priority
- In match map, a precedence cannot be matched on output of an interface
- In match map, the DSCP value cannot be set on output
- In match map, the Precedence value cannot be set
- This configuration can be applied only on the input of the interface (like for the configuration of the QoS policy for legacy MSBR products).

18 IPv6

IPv6, as described in RFC 2460, is a new version of the Internet Protocol, designed to be a successor to the IPv4 protocol. It has new features that can be described in the following categories:

- Expanded addressing capabilities. The IPv6 address size is 128 bits compared to 32bits of the IPv4 protocol.
- The IPv6 header has fewer fields than IPv4.

The IPv6 packet header is shown below:

Version[4 bits]	Traffic class [8 bits]	Flow label [20 bits]
Payload length [16 bits]	Next header [8 bits]	Hop limit [8 bits]
Source address [128 bits]		
Destination address [128 bits]		

- Improved support for extensions and options.
- Flow labeling for particular traffic flows.
- Authentication and privacy capabilities.

IPv6 addresses on the device are configured on routed interfaces, and usually are accompanied by the subnet mask, which is used for subnet calculation.

As is the case with IPv4, each Layer-3 interface can be assigned one primary IPv6 address and several secondary IPv6 addresses.

To configure IPv6 addresses per interface, use the following configuration steps:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface <interfaces number></code>	Enters the interface configuration.
<code>(conf-if-GE 0/0)# ipv6 enable</code>	Enables IPv6 on the interface.
<code>(conf-if-GE 0/0)# ipv6 address <IPv6 addr>/<mask></code>	Configures the IPv6 address and mask separated by a forward slash "/".
<code>(conf-if-GE 0/0)# ipv6 address <IPv6 addr>/<mask></code>	Configures an optional, multiple addresses using the same command (The keyword "secondary" is not required for IPv6).

18.1 Example of multiple IPv6 Address Configuration

The following is an example of multiple IPv6 Address configuration.

18.1.1 Configuration

The configuration of two IPv6 addresses is shown below:

```
# configure data
(config-data)# interface gigabitethernet 0/0

(config-if-GE 0/0)# ipv6 enable

(config-if-GE 0/0)# ipv6 address 2001:100::1/64

(config-if-GE 0/0)# ipv6 address 2001:200::1/64
```

18.1.2 Output

The output of the show commands is shown below:

```
# show data interfaces gigabitethernet 0/0

GigabitEthernet 0/0 is Connected.
Description: WAN Copper
Hardware address is 00:90:8f:4b:fc:28
Port Link:UP
Port Speed : 1Gbps
Port Duplex:FULL
State Time: 0:00:20
Time since creation: 1:13:37
Time since last counters clear : 0:00:20
mtu auto
napt
IPv6 is enabled, link-local address is
fe80::290:8fff:fe4b:fc28/64
Global unicast address(es):
    2001:200::1/64
    2001:100::1/64
Joined group address(es):
    ff02::1:ff00:0
    ff02::1:ff00:1
    ff02::1:ff4b:fc28
    ff02::1
rx_packets 16          rx_bytes 1260          rx_dropped
0          rx_errors 0
tx_packets 5          tx_bytes 454          tx_dropped
0          tx_errors 0
15-seconds input rate: 1.3 Kbps, 2 packets/sec
15-seconds output rate: 0 bits/sec, 0 packets/sec
```



```
# show data ipv6 neighbors

IPv6 Address                               MAC Address
Interface
2001:100::16
00:90:8f:48:cd:7f   Fiber 0/1
fe80::290:8fff:fe48:cd7f
00:90:8f:48:cd:7f   Fiber 0/1

End of neigh table, 2 entries displayed.

#
```

The `show data ipv6 neighbors` command is similar to the `show arp` command in the IPv4 environment, displaying the IPv6 address and MAC addresses of known neighbors on the interfaces connected to the device.

18.1.3 Example of a Dual-Stack Configuration

The following is an example of a dual-stack configuration. Dual stack is a configuration if IPv4 and IPv6 are on the same interface.

18.1.3.1 Configuration

```
# configure data
(config-data)# interface vlan 1
(conf-if-VLAN 1)# ip address 192.168.0.1 255.255.255.0
(conf-if-VLAN 1)# ipv address 2001:100::1/64
(conf-if-VLAN 1)#
```

18.1.3.2 Output

```
# show data ip interface brief

Interface                IP Address        Status        Protocol
GigabitEthernet 0/0      0.0.0.0           Enabled       Up
Fiber 0/3                0.0.0.0           Enabled       Up
VLAN 1                   192.168.0.1       Connected     Up
VLAN 4001                169.254.254.253   Connected     Up
```

```
# show data ipv6 interface brief

Interface    IP Address          Status        Protocol
VLAN 1       fe80::290:8fff:fe4a:2343   Connected     Up
VLAN 1       2001:100::1             Connected     Up
```

This page is intentionally left blank.

19 ICMPv6

The following describes the Internet Control Message Protocol Version 6 (ICMPv6) commands.

19.1 ping ipv6

The ping ipv6 tests IP reachability to a desired destination. If the destination is reachable, there will be the same amount of echo requests and replies.

Command Structure:

```
ping ipv6 <IP address / host> [source data vrf/source  
address/interface name] [repeat times] [size size] [summarized]
```

where:

- <IP address / host>: Defines the destination IP address or hostname of the node you wish to ping.
- <source>: Defines the vrf/address/interface to use as source for the ICMP requests. Typically, the device chooses the source address/interface; however, specifying one allows you to simulate testing reachability from a specific connected subnet.
- repeat: Defines the number of ICMP requests to send.
- size: Defines the size of the of the ICMP packet in bytes.
- summarized: Defines the summarized output.

Typical Output:

```
# ping ipv6 2000::1
Reply from 2000::1 : time=1 ms
Reply from 2000::1 : time=1 ms
Reply from 2000::1 : time=1 ms
Reply from 2000::1 : time=1 ms
4 packets transmitted, 4 packets received
Round-trip min/avg/max = 1/1/1 ms
#
```

19.2 Traceroute v6

The ping informs you if the destination is reachable or not. The `traceroute` command can be used to discover the path that packets travel to the remote destination.

Command Structure:

```
Traceroute ipv6 <IP Address> [vrf vrf / source address]
```

Typical Output:

```
# trace ipv6 3000::1

1  2000::1 (2000::2)  1.169 ms  *  7.346 ms
2  2020::1 (2020::2)  1.169 ms  *  7.346 ms
.
.
8  3000::1 (3000::1)  1.169 ms  *  7.346 ms
Traceroute: Destination reached

#
```

20 Track v6

This command keeps track of a destination IP address from a given source interface. The tracking is done by sending ICMPv6 probes and monitors the replies. If the destination is reachable, the Track status is 'up'. When the (configurable) number of replies are not received, the Track status moves to 'down'.

20.1 Configuring Track

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# track id icmpv6echo destIP interface [source-ip-interface interface] [interval val] [retries val]</code>	Configures a Track to monitor reachability to <i>destIP</i> from <i>interface</i> .

20.2 Output

```
# show data track brief
Track      Type                State      Max round trip time (m.s)
1          ICMP reachability   Up         37
```

Get the time of up to last 10 Track states:

```
# show data track 1 history

Track history:  New state      Date and Time [MM-DD-YYYY@hh:mm:ss]
                Up             08-28-2015@18:17:40
                Down          08-28-2015@18:25:30
                Up             08-28-2015@18:26:20
```

This page is intentionally left blank.

21 IPv6 Routing

The following describes Internet Protocol version 6 (IPv6) routing.

21.1 Static Routing

Static routing is used when the router uses pre-defined, user-configured routing entries to forward traffic. Static routes are usually manually configured by the network administrator and added to the routing table.

A common use of static routes is for providing the gateway as a last resort, meaning, providing an instruction on how to forward traffic when no other route exists.

Static routes have a much lower administrative distance in the system than the dynamic routing protocols, and in most scenarios are prioritized over the dynamic routes.

21.1.1 Configuring Static Routing

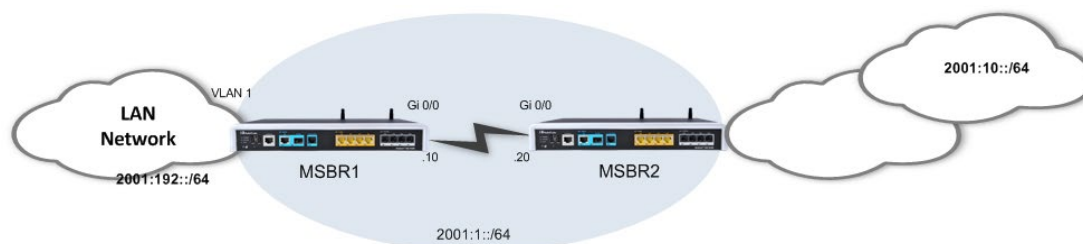
The configuration is the same as IPv4:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# ipv6 route [vrf vrf] destIP destMask next-hop interface [A-distance] [track number]</code>	Configures a static route by specifying the destination prefix, a next-hop address and optionally the administrative distance for the route and a tracking object.

21.1.2 Example of a Basic Static Route Configuration

In this example, the device needs to reach the 2001:10::/64 network segment from its LAN network. The destination segment is located somewhere in the network, behind MSBR2, and in this example, no dynamic routing is configured. For this to work, you need to configure MSBR1 to forward traffic to 2001:10::/64 through MSBR2's interface facing MSBR1 (2001:1::2).

Figure 21-1: Static Routing



21.1.2.1 Configuration

```
MSBR1# configure data
(config-data)# ipv6 route 2001:10::/64 2001:1::1 gigabitethernet
0/0
(config-data)#
```

21.1.2.2 Output

```
MSBR1# show running-config data
Configure data

*****
**
General configuration omitted, assume that configured as in
diagram
*****
**

ipv6 route 2001:10::/64 2001:1::1 GigabitEthernet 0/0 1
```

```
MSBR1# show data ipv6 route
Codes: K - kernel route, C - connected, S - static,
       R - RIPng, O - OSPFv6, B - BGP

S   2001:10::/64 [1/1] via 2001:100::10, GigabitEthernet 0/0
C   2001:100::/64 [1/4] is directly connected, GigabitEthernet
0/0
C   fe80::/64 [1/4] is directly connected, GigabitEthernet 0/0

#
```


21.2 RIPng Routing Protocol

Routing Information Protocol next generation (RIPng) is a dynamic routing protocol from the Distance Vector family which uses hop-count as a routing metric. The protocol is limited to 15 hops per route, which prevents loops; however, also limits the network size and scalability. Low metric routes are considered “better” and a route with hop count (metric) of 16 is considered “unreachable”.

RIPng is considered a “chatty” and bandwidth consuming protocol due to the fact it “floods” its routing database once in a period (default is 30 seconds).

RIPng can work both in broadcast and unicast modes (without or with peers, respectively).

The device supports RIPng, defined in RFC 2080.

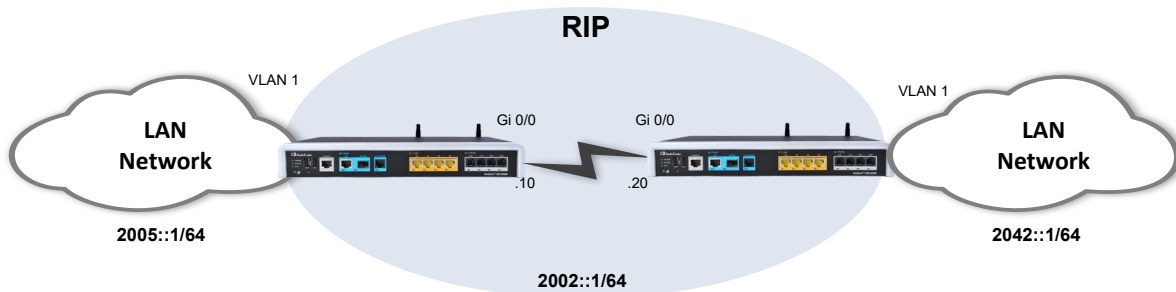
21.2.1 Configuring RIPng

Command	Description
# configure data	Enters the data configuration menu.
(config-data)# router ripng	Enters the RIPng configuration mode.
(conf-router)# default-information originate	Configures whether to advertise the default route.
(conf-router)# default-metric metric	Configures the metric for redistributed routes.
(conf-router)# distribute-list prefix list-name <in/out> interface	Configures filtering of incoming/outgoing routing updates.
(conf-router)# network interface (conf-router)# network prefix/preflen	Configures a network or interface upon which to enable RIP routing.
(conf-router)# passive-interface interface	Configures suppression of routing updates on an interface.
(conf-router)# redistribute protocol metric metric [route-map name]	Configures redistribution of routes from other protocols into RIP.
(conf-router)# route prefix/length	Adds a RIP static route.
(conf-router)# route-map RMname <in/out> interface interface	Configures a route-map for the RIP routing.
(conf-router)# timers basic value	Configures the routing table update timer.

21.2.2 Example of RIPng Routing

This example demonstrates a LAN scenario with a device, connecting to the WAN through RIP.

Figure 21-2: RIPng Routing



21.2.2.1 Configuration

■ MSBR1:

```
MSBR1# configure data
(config-data)# router ripng
(conf-router)# network GigabitEthernet 0/0
(conf-router)# redistribute connected
```

■ MSBR2:

```
MSBR2# configure data
(config-data)# router ripng
(conf-router)# network GigabitEthernet 0/0
(conf-router)# route 2001:100:2::1/64
```

21.2.2.2 Output and show Commands

```
MSBR1# show da ipv ripng
Codes: R - RIPng, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) -
redistribute,
      (i) - interface, (a/S) - aggregated/Suppressed

  Network      Next Hop      Via      Metric Tag Time
R(n) 2001:1::/64 fe80::290:8fff:fe2e:eda8 GigabitEthernet 0/0
2    0 02:38
C(i) 2001:100:1::/64
      :: self 1 0
R(n) 2001:100:2::/64
      fe80::290:8fff:fe2e:eda8 GigabitEthernet 0/0
2    0 02:38
MSBR1# show data ipv6 route ripng
Codes: K - kernel route, C - connected, S - static,
      R - RIPng, O - OSPFv6, B - BGP

R 66::/64 [120/2] via fe80::290:8fff:fe2e:eda8, VLAN 1,
00:14:29
```

```
MSBR1# show da ipv route ripng
Codes: K - kernel route, C - connected, S - static,
      R - RIPng, O - OSPFv6, B - BGP

R 2001:1::/64 [120/2] via fe80::290:8fff:fe2e:eda8,
GigabitEthernet 0/0, 00:01:53
R 2001:100:2::/64 [120/2] via fe80::290:8fff:fe2e:eda8,
GigabitEthernet 0/0, 00:01:53
```

```
MSBR1# show da ipv ripng status
Routing Protocol is "RIPng"
  Sending updates every 30 seconds with +/-50, next due in 3
seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 1, receive version 1
    Interface      Send Recv
  GigabitEthernet 0/0      1      1
Routing for Networks:
  GigabitEthernet 0/0
Routing Information Sources:
  Gateway      BadPackets BadRoutes Distance Last Update
  fe80::290:8fff:fe2e:eda8
                        0          0          120      00:00:16
```

21.3 OSPFv3 Routing Protocol

Open Shortest Path First (OSPF) is a dynamic routing protocol from the Link-State family, basing its routing decisions on the bandwidth parameter using the Dijkstra Algorithm. The protocol establishes adjacencies with other OSPF routers to which it is connected, and maintains detailed topology and routing tables. OSPF provides fast network convergence and great scalability. The version of the protocol that is being used is OSPFv3 (RFC 5340).



Note: OSPFv3 is called OSPF6 in Linux and therefore, commands that are written as `ospf6`. OSPFv3 and OSPF6 are synonymous.

21.3.1 Configuring OSPF

The following describes the commands for configuring OSPF.

21.3.1.1 Router-Configuration Level

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# router ospf6</code>	Enters the OSPF6 configuration mode.

21.3.1.2 OSPF6 Router Level

Command	Description
<code>(config-router)# area A.B.C.D</code>	Configured area parameters.
<code>(config-router)# interface interface area A.B.C.D</code>	Enables routing on an IPv6 interface and defines IPv4-formatted area to interface.
<code>(conf-router)# redistribute</code>	Redistributes routes from other protocols.

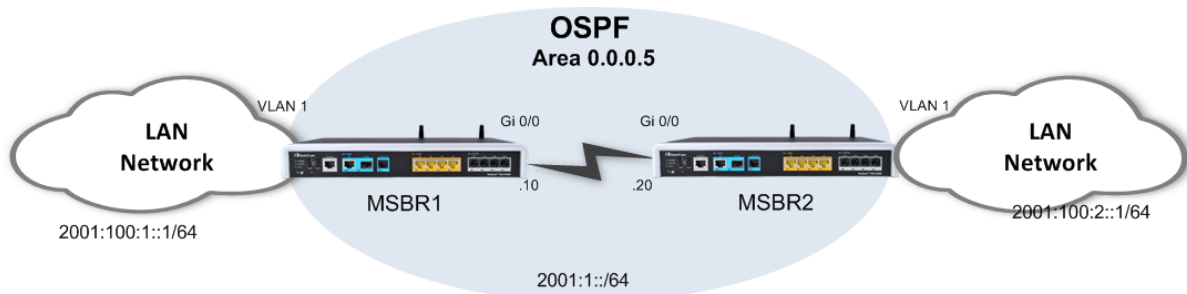
21.3.1.3 Main options for Interface-Configuration Level

Command	Description
<code>(config-data)# interface gigabitethernet 0/0</code>	Enters the interface configuration menu.
<code>(config-if-GE 0/0)# ipv6 ospf6 advertise</code>	Advertising options.
<code>(config-if-GE 0/0)# ipv6 ospf6 passive</code>	Passive interface in listen mode only.
<code>(conf-if-int)# ipv6 ospf6 cost cost</code>	Configures the OSPF6 cost for the specified interface.

21.3.2 Example of OSPFv3 Routing

This example demonstrates a typical scenario where a device acts as a default gateway for a LAN network, and connects to the WAN network using the OSPF6 protocol. This example includes a single-area (area 0.0.0.5) OSPF6 network; however, in more complex and large-scale networks, multi-area topology may be more adequate in terms of scalability.

Figure 21-3: OSPF6 Routing



The following configuration demonstrates a basic OSPF6 configuration in which OSPF6 is activated on the LAN interfaces (for advertisement) and on the WAN interfaces (for adjacency forming). The router-ids are explicitly configured to the addresses of loopback interfaces configured on the device. Adjacency change logging is activated for debugging. The OSPF6 timers are configured on the WAN interfaces of the devices and should always be matched on both ends to avoid adjacency flapping.

```
*****
IPv6 address configuration is omitted, assume it is as described
in the topology above.
*****
```

MSBR1 :

```
MSBR1# config data
(config-data)# router ospf6
(conf-router)# router-id 1.1.1.1
(conf-router)# redistribute connected
(conf-router)# interface GigabitEthernet 0/0 area 0.0.0.5
(conf-router)# exit
(config-data)# interface GigabitEthernet 0/0
(conf-if-GE 0/0)# ipv6 ospf6 hello-interval 1
(conf-if-GE 0/0)# ipv6 ospf6 dead-interval 3
```

MSBR2 :

```
MSBR2# config data
(config-data)# router ospf6
(conf-router)# router-id 1.1.1.2
(conf-router)# redistribute connected
(conf-router)# interface GigabitEthernet 0/0 area 0.0.0.5
(conf-router)# exit
(config-data)# interface GigabitEthernet 0/0
(conf-if-GE 0/0)# ipv6 ospf6 hello-interval 1
(conf-if-GE 0/0)# ipv6 ospf6 dead-interval 3
```

21.3.3 Useful Output and show Commands

```
MSBR2# show data ipv6 ospf neighbor
Neighbor ID      Pri    DeadTime  State/IfState      Duration I/F[State]
1.1.1.1          1      00:00:40   Full/DR            00:15:25 VLAN 1[BDR]
```

```
MSBR2# show data ipv6 ospf6
  OSPFv3 Routing Process (0) with Router-ID 1.1.1.2
  Running 00:16:14
  Number of AS scoped LSAs is 7
  Number of areas in this router is 1
  Area 0.0.0.5
    Number of Area scoped LSAs is 5
    Interface attached to this area: VLAN 1
```

```
MSBR2# show data ipv6 route ospf6
Codes: K - kernel route, C - connected, S - static,
       R - RIPng, O - OSPFv6, B - BGP

O   2000::33:0/124 [110/1] via fe80::290:8fff:fe2e:eda8, VLAN 1,
00:12:41
O   2002::/64 [110/2] via fe80::290:8fff:fe2e:eda8, VLAN 1, 00:12:41
O   2011:3333::/64 [110/1] is directly connected, VLAN 1, 00:22:22
O   2014:9999::/64 [110/1] via fe80::290:8fff:fe2e:eda8, VLAN 1,
00:12:41
O   fc11::/124 [110/1] via fe80::290:8fff:fe2e:eda8, VLAN 1, 00:12:41
O   fc12::/124 [110/1] via fe80::290:8fff:fe2e:eda8, VLAN 1, 00:12:41
```

21.4 Border Gateway Protocol (BGP) for IPv6

BGP is a standardized exterior gateway protocol (EGP) for exchanging routing and reachability information between routers on different Autonomous Systems (AS's) in large scale, internet provider and public internet networks.

BGP does not use the metrics used by IGP protocols (such as RIP, OSPF, EIGRP, ISIS), however makes its routing decisions based on paths, network policies and custom rules configured by network administrators.

BGP is more stable and much less “chatty” protocols than the common IGP protocols, and does not form adjacencies unless specifically configured. The formed adjacencies are connection oriented and based on TCP connections.

BGP is the main routing protocol of internet service providers and the Internet.

21.4.1 Configuring BGP

The following describes the commands for configuring BGP.

21.4.1.1 Main options for Address-Family Level Configuration

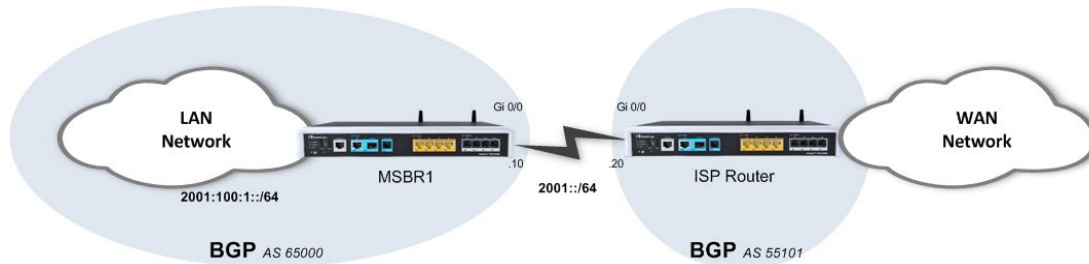
Command	Description
# configure data	Enters the data configuration menu.
(config-data)# router bgp <i>as-number</i>	Enters the BGP configuration mode and the number of the local autonomous system.
(conf-router)# address-family ipv6	Enters the BGP IPv6 Address Family configuration mode.
(conf-router-af)# neighbor <i>address</i> activate	Activate the BGP IPv6 protocol with this neighbor.
(conf-router-af)# neighbor <i>address</i> default-originate	Originate default route to this neighbor.
(conf-router-af)# neighbor <i>address</i> prefix-list	Filter updates to/from this neighbor .
(conf-router-af)# neighbor <i>address</i> route-map	Apply route map to neighbor.

21.4.2 Example of Basic BGP WAN Connectivity

This example includes a basic and very common BGP WAN connectivity scenario. The local device establishes a BGP adjacency with the ISP router and receives a default route from it, allowing it full connectivity to the “Outside World”.

Usually in scenarios like this, the internal (LAN) network segment is allocated by the ISP and allows it to be routed across the ISP network.

Figure 21-4: BGP IPv6 Example



21.4.2.1 Configuration

```
# configure data
(conf-data)# router bgp AS-Number
(conf-router)# neighbor <ISP address> remote-as 55101
(conf-router)# address-family ipv6
(conf-router-af)# neighbor <ISP address> activate
```

21.4.2.2 Output

The following output shows the local parameters of the BGP process and the established BGP adjacencies:

```
# show data ipv6 bgp summary
#
```

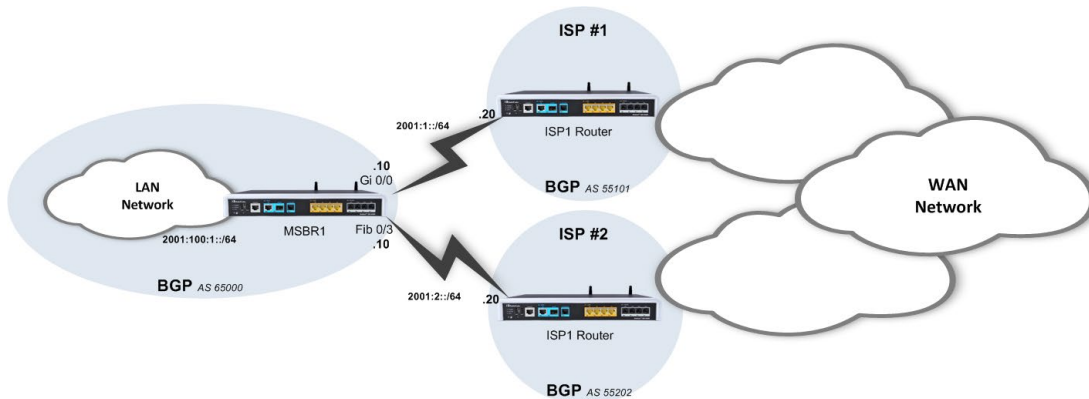
The following output shows that the router is learning a default route through the ISP BGP peer:

```
# show data ipv6 route
#
```


21.4.3 Example 2

This example shows a scenario in which an organization is connected to the public internet through two ISPs. This is often called a Multi-WAN configuration and it provides high availability and redundancy of the internet connection. It is demonstrated that both ISPs advertise a default route through the BGP protocol, and are prioritized using manual modification of the BGP Weight attribute.

Figure 21-5: BGP IPv6 Example 2



21.4.3.1 Configuration

```
*****
Basic Configuration omitted
*****
(conf-router)# router bgp 65000
(conf-router)# bgp router-id 1.1.1.1
(conf-router)# bgp log-neighbor-changes
(conf-router)# neighbor 2001:1::20 remote-as 6500
(conf-router)# neighbor 2001:2::20 remote-as 6501
(conf-router)# address-family ipv6
(conf-router)# network 2001::/64
(conf-router)# network 2001:100:1::/64
(conf-router)# neighbor 2001:1::20 activate
(conf-router)# neighbor 2001:2::20 activate
```

■ MSBR1:

```
MSBR1(conf-data)# router bgp 6500
(conf-router)# bgp router-id 10.4.4.69
(conf-router)# neighbor 2001:1::10 remote-as 65000
(conf-router)#
(conf-router)#
(conf-router)# address-family ipv6
(conf-router-af)# redistribute connected <- redistribute all
IPv6 connected routes
(conf-router-af)# neighbor 2002:1::10 activate <- activate the
bgp ipv6 with this neighbor (differently from ipv4, it is a
mandatory command)
(conf-router-af)# exit
(conf-router)# exit
```

■ MSBR2:

```
MSBR2(conf-data)# router bgp 6501
(conf-router)# bgp router-id 11.11.11.11
(conf-router)# neighbor 2001:1::10 remote-as 65000
(conf-router)# address-family ipv6
(conf-router-af)# redistribute connected
(conf-router-af)# neighbor 2002:1::10 activate
(conf-router-af)# exit
(conf-router)# exit
```

The configuration includes two important parts:

- The basic configuration defines the networks to be advertised and routed, and the neighbors to which to establish adjacency.
- The second part of the configuration deals with the prioritization of the routes received from neighbors. Given the fact that a default route is received via the BGP protocols from both neighbors, you need to give one of them a higher priority (better metric). This is performed using a route-map that fine-tunes the “Weight” BGP attribute of incoming route-updates, where the route with the higher weight value is inserted into the routing table.

21.4.3.2 Output

■ **BGP adjacency status:**

```
# show data ipv6 bgp summary
```

```
BGP router identifier 10.4.4.69, local AS number 6500
```

```
RIB entries 11, using 1056 bytes of memory
```

```
Peers 1, using 4560 bytes of memory
```

Neighbor State/PfxRcd	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
2002::5	4	6501	28	30	0	0	0	00:14:18

```
# show data ipv6 bgp
```

```
BGP table version is 0, local router ID is 10.4.4.69
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
r RIB-failure, S Stale, R Removed
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 2000::33:0/124	2002::2	3	0	6501	?
* 2002::/64	2002::2	4	0	6501	?
*> ::		4		32768	?
*> 2014:9999::/64	2002::2	3	0	6501	?
*> 3003::/64	::	4		32768	?
*> fc11::/124	2002::2	3	0	6501	?
*> fc12::/124	2002::2	3	0	6501	?

```
Total number of prefixes 6
```

```
# show data ipv6 bgp neighbors 2002::2 advertised-routes
```

```
BGP table version is 0, local router ID is 10.4.4.69
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
r RIB-failure, S Stale, R Removed
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 2002::/64	2002::3	4		32768	?
*> 3003::/64	2002::3	4		32768	?

```
Total number of prefixes 2
```

```
# show data ipv6 bgp neighbors 2002::2 routes
BGP table version is 0, local router ID is 10.4.4.69
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal,
               r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric   LocPrf   Weight Path
*> 2000::33:0/124    2002::2         3         0         6501 ?
*  2002::/64         2002::2         4         0         6501 ?
*> 2014:9999::/64    2002::2         3         0         6501 ?
*> fc11::/124        2002::2         3         0         6501 ?
*> fc12::/124        2002::2         3         0         6501 ?

Total number of prefixes 5
```

■ MSBR routing table:

```
# show data ipv6 route
Codes: K - kernel route, C - connected, S - static,
       R - RIPng, O - OSPFv6, B - BGP

B  2000::33:0/124 [200/3] via fe80::290:8fff:fe40:3e1c, VLAN
1, 00:00:14
C  2002::/64 [1/4] is directly connected, VLAN 1
B  2014:9999::/64 [200/3] via fe80::290:8fff:fe40:3e1c, VLAN
1, 00:00:14
B  3003::/64 [200/4] via fe80::290:8fff:fe40:3e1c, VLAN 1,
00:00:14
B  4004::/64 [200/4] via fe80::290:8fff:fe40:3e1c, VLAN 1,
00:00:14
B  5050::/64 [200/0] via fe80::290:8fff:fe40:3e1c, VLAN 1,
00:00:29
B  fc11::/124 [200/3] via fe80::290:8fff:fe40:3e1c, VLAN 1,
00:00:14
B  fc12::/124 [200/3] via fe80::290:8fff:fe40:3e1c, VLAN 1,
00:00:14
C  fe80::/64 [1/4] is directly connected, VLAN 1
```

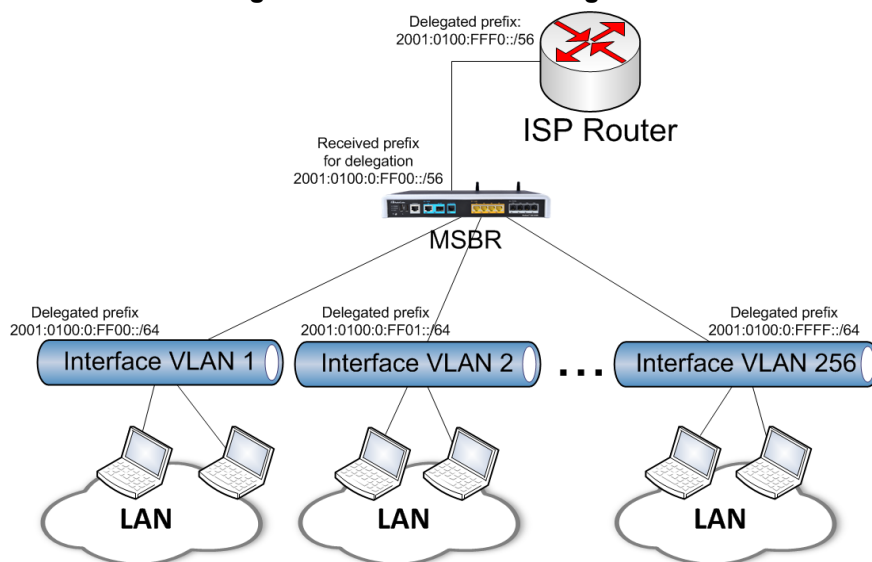
21.5 DHCPv6

DHCPv6 is the DHCP protocol that runs with IPv6. This protocol works in a different way on IPv6 than on IPv4; however, the goal of the protocol remains the same.

The device can obtain configuration if it's WAN interface using two modes: stateful or stateless. In stateful mode, the entire configuration is provided using the DHCP server. In stateless mode, the IP configuration can be provided using the Network Discovery Protocol (NDP), and other configuration protocols such as NTP. In addition, a DNS address can be provided using the DHCP server, and also the NDP protocol can be used. In both cases, the hosts cannot obtain an IP address using Prefix Delegation. If the WAN address is dynamically configured, the hosts can obtain dynamic IP addresses using Router Advertisement (RA) or it can be configured as a static address.

Some routers connected to ISPs require IPv6 addresses not only for their WAN interfaces, but also for hosts connected to their LAN interfaces. In the IPv4 world, the ISP provides the router with one or more IP addresses for the WAN interface. The network operator uses NAT with a local DHCP server to assign IP addresses to the hosts on the LAN side. However, in the IPv6 world, there is no NAT protocol because there is no need to save IPv6 addresses - they are abundant. In the IPv6 world, the IPv6 addresses are provided by the ISP using prefix delegation. Prefix delegation, described in RFC 3769, is used to assign a router IP prefix which can be delegated to the LAN side as networks. Hosts will receive IPv6 addresses in these networks.

Figure 21-6: IPv6 Prefix Delegation



The figure above shows an example of a network topology using the IPv6 prefix delegation. The ISP router delegates the prefix 2001:0100:0:FFF0::/56 to the device. The device needs to assign addresses to three LAN networks: Interface VLAN 10, Interface VLAN 20 and Interface VLAN 30. Every host on the LAN network is assigned with an address with prefix /64. This means that the device can assign every LAN interface with a network in an amount of $2^{64-56} = 2^8 = 256$. This means that device can assign addresses on 256 VLANs. The computers attached to interface VLAN 1 will have IPs in the network 2001:100:0:FF00::/64, on VLAN 2, the computers will have IPs in the network 2001:100:0:FF01::/64 etc.

21.5.1 Configuring Stateless DHCP

To configure stateless IP address, use the following commands:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface <WAN Interface></code>	Configures a WAN interface.
<code>(conf-if-WAN int)# ipv6 address autoconfig</code>	Uses autoconfig, stateless mode to configure an IP address on the interface.

21.5.2 Configuring Stateful DHCP

To configure stateful IP addresses, use the following commands:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface <WAN Interface></code>	Configures a WAN interface.
<code>(conf-if-WAN int)# ipv6 address dhcp [rapid-commit]</code>	Uses DHCP stateful mode to configure an IP address on the interface.

21.5.3 Configuring Router Advertisement

For stateful and stateless IP address configuration, router advertisement (RA) can be configured for hosts to allow dynamic IP allocation. Use the configuration steps described in the table below to configure RA.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# VLAN <No></code>	Enters LAN interface configuration.
<code>(conf-if-VLAN 1)# ipv6 address 2001:100:1::1/64</code>	Configures a static IP address for the LAN address.
<code>(conf-if-VLAN 1)# ipv6 nd prefix 2001:100:1:: default</code>	Configures an RA prefix with default timers. Instead of default timers, lifetime timers can be used, according to RFC 4861.
<code>(conf-if-VLAN 1)# no ipv6 nd ra suppress</code>	By default, the RA is suppressed and not operational. Use the <code>no</code> command to stop the suppression and activate RA.

21.5.4 Configuring Prefix Delegation

For the configuration of the prefix delegation, the interface VLAN on the LAN side needs to know from where to receive the IPv6 prefix delegation, and the WAN interface needs to know from where to receive DHCPv6 data. To configure prefix delegation, use the configuration steps that are described in the following table .

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface <WAN interface></code>	Enters the WAN interface that is connected to the WAN.
<code>(conf-if-WAN int)# ipv6 dhcp-client pd [rapid-commit]</code>	Configures the WAN interface to receive PD messages. Rapid-commit – uses two-message exchange rather than four-message exchange to obtain an IP address according to RFC 4039.
<code>(config-data)# interface vlan <number></code>	Enters the LAN interface configuration.
<code>(config-data)# ipv6 enable</code>	Enables IPv6 on the interface.
<code>(config-data)# ipv6 dhcp server enable</code>	Enables DHCP service on the interface. For the interface of the device to obtain an IPv6 address using DHCPv6, the managed bit in the RA packet of the DHCP server, must be ON.
<code>(conf-if-VLAN <No>)# ipv6 nd pd <WAN interface> <IPv6 Prefix></code>	Configures the LAN interface to obtain IPv6 prefix from the <WAN interface>. <IPv6 Prefix> is the prefix delegated to the hosts attached to the LAN interface. According to the example, if the configured device is on interface VLAN 2, the prefix should be 2001:100:100:ff01::/64.

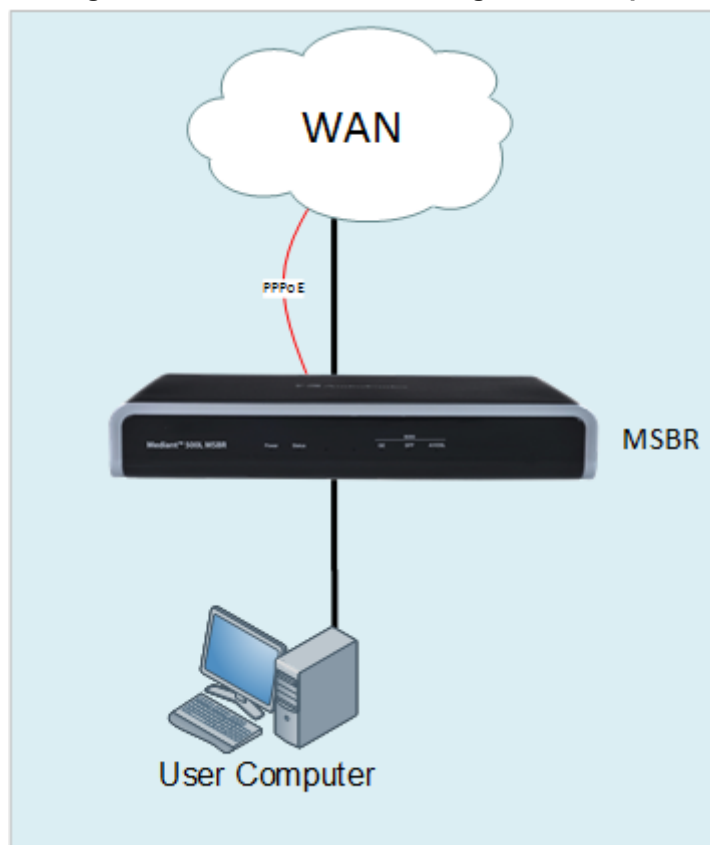
21.5.5 Example of DHCPv6 Prefix Delegation with Autoconfig

The following is an example of DHCPv6 Prefix Delegation. The WAN address of the device is configured using autoconfig, which sends Router Advertisement (RA) messages.

21.5.5.1 Configuration of Prefix Delegation

The configuration is based on the following example scenario:

Figure 21-7: DHCPv6 Prefix Delegation Example



In the configuration, the device is attached to the WAN network with the PPPoE interface. The device needs to be configured as follows:

Configuration	Description
<pre>interface pppoe 0 firewall enable napt mtu auto ppp user <user> pass <password> ppp authentication chap ppp authentication ms-chap ppp authentication ms-chap-v2 no ppp authentication pap ppp lcp-echo 6 5 no ppp compression</pre>	<p>The following command enables prefix delegation:</p> <pre>ipv6 dhcp-client pd</pre> <p>The command</p> <pre>ipv6 address autoconfig</pre> <p>configures the IPv6 address if the PPPoE interface using autoconfig - ra messages.</p>

Configuration	Description
<pre> no ip address ipv6 enable ipv6 address autoconfig ipv6 dhcp-client pd ip dns server auto underlying GigabitEthernet 0/0 no shutdown exit </pre>	
<pre> interface VLAN 1 ip address 192.168.0.1 255.255.255.0 mtu auto desc "LAN switch VLAN 1" ipv6 enable ip dhcp-server network 192.168.0.3 192.168.0.8 255.255.255.0 ip dhcp-server dns-server 0.0.0.0 ip dhcp-server netbios-name- server 0.0.0.0 ip dhcp-server lease 0 1 0 ip dhcp-server provide-host- name ip dhcp-server ntp-server 0.0.0.0 ip dhcp-server tftp-server 0.0.0.0 ip dhcp-server override- router-address 0.0.0.0 ip dhcp-server next-server 0.0.0.0 service dhcp ip dns server static no napt no firewall enable no link-state monitor ipv6 nd ra interval 4 3 ipv6 nd pd PPPOE 0 ::A:0:0:0:0/64 no ipv6 nd ra suppress no shutdown exit </pre>	<p>The</p> <pre> ipv6 nd pd PPPOE 0 ::A:0:0:0:0/64 </pre> <p>command enables prefix delegation from the WAN interface PPPoE 0, to the current interface and applies the "tail" A:0:0:0:0. The zero will be replaced with IP address based on EUI-64 (Extended Unique Identifier) standard.</p> <p>The</p> <pre> no ipv6 nd ra suppress </pre> <p>command forbids the device to suppress router advertisements in the VLAN 1 interface.</p> <p>The VLAN 10 address is not assigned by the PD.</p>

21.5.5.2 Output

ISP CISCO 7200 output is as follows.

```
ISP# show ipv6 dhcp pool
Client: FE80::4084:208F:1C9:3472
  DUID: 0001000120D154D100908F4BACD3
  Username : tomer
  VRF : default
  Interface : Virtual-Access2.1
  IA PD: IA ID 0x00000000, T1 300, T2 480
    Prefix: 2000:2000::/48
            preferred lifetime 600, valid lifetime 1800
            expires at Aug 31 2017 06:23 AM (1692 seconds)
ISP#
```

The following host's output shows that the host received an IPv6 prefix and generated an IP address for itself:

```
>ipconfig
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 
2000:2000:0:a:1585:733c:b8ef:1f45
    Temporary IPv6 Address. . . . . : 
2000:2000:0:a:8072:e00d:5d81:1251
    Link-local IPv6 Address . . . . . : 
fe80::1585:733c:b8ef:1f45%10
    Default Gateway . . . . . : fe80::290:8fff:fe4b:acd3%10
```

The following is the ISP router configuration. Irrelevant configuration was omitted. The ISP router is a Cisco router.

```
ipv6 unicast-routing

ipv6 dhcp pool TEST
  prefix-delegation pool TEST lifetime 1800 600

username tomer password 0 tomer

bba-group pppoe GROUPA
  virtual-template 1

interface Loopback1
  no ip address
  ipv6 address 2000:2000:2000::1/48
  ipv6 address 2001:DB8:1::1/96

interface GigabitEthernet 0/2
  description "to MSBR WAN"
  no ip address
  negotiation auto
  ipv6 enable
```

```
pppoe enable group GROUPA

interface Virtual-Templat1
mtu 1492
no ip address
ipv6 unnumbered Loopback1
ipv6 nd other-config-flag
ipv6 nd ra interval 4
ipv6 dhcp server TEST
ppp authentication chap pap ms-chap callin

ipv6 local pool TEST 2000:2000::/40 48
```

21.5.6 Example of RA Configuration

The following is an example of Router Advertisement (RA) configuration.

21.5.6.1 Configuration

In this example, a host is connected to the LAN interface of the device on VLAN 1.

```
# configure data
(config-data)# interface vlan 1
(conf-if-VLAN 1)# ipv6 enable
(conf-if-VLAN 1)# ipv6 address 2001:100:1::1/64
(conf-if-VLAN 1)# ipv6 nd prefix 2001:100:1:: default
(conf-if-VLAN 1)# no ipv6 nd ra suppress
(conf-if-VLAN 1)#
```

21.5.6.2 Output

The following is the output of the `ipconfig` command at the host connected to the device:

```
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 
2001:100:1:0:808e:a770:deb7:1cd3
    Link-local IPv6 Address . . . . . : 
fe80::808e:a770:deb7:1cd3%12
    IPv4 Address. . . . . : 180.1.1.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::c800:24ff:fe90:8%12
                                fe80::c801:24ff:fe90:8%12
```

21.5.7 DHCPv6 advertised information

Following items can be configured for the DHCPv6 Router Advertisement message.

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface <LAN interface></code>	Enters the WAN interface that is connected to the LAN.
<code>(conf-if-WAN int)# ipv6 dhcp-server dns-server <primary ip> <secondary ip></code>	Configures the name-server IP. “.” means LAN interface’s IP.
<code>(conf-if-WAN int)# ipv6 dhcp-server domain-name</code>	Configures the domain name
<code>(conf-if-WAN int)# ipv6 dhcp-server ntp-name</code>	Configures the NTP or SNTP server IP
<code>(conf-if-WAN int)# ipv6 dhcp-server sip-server-<ip name></code>	Configures the SIP server IP and name

21.5.8 DHCPv6 Client

The DHCPv6 client's default behavior is to set a default route through the interface running the client and connected to DHCPv6 server.

However, that behavior can be overridden by the following CLI command:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface <WAN interface></code>	Enters the WAN interface that is connected to the WAN.
<code>(conf-if-WAN int)# no ipv6 nd autoconfig default-route</code>	Configures the WAN interface to not create default route to DHCPv6 address.

In this example, a host is connected to the LAN interface of the device on VLAN 1 and we cancel the auto-created default route:

```
# configure data
(config-data)# interface vlan 1
(conf-if-VLAN 1)# no ipv6 nd autoconfig default-route
```

21.6 DNSv6

DNS is a hierarchical naming system for computers, devices, or any resources connected to a network. DNS is used to resolve hostnames into IP addresses, and to enforce naming conventions for devices in the network and/or domain.

DNS configuration for devices can be either static – administrator configured – or acquired dynamically through DHCP.

While working with DHCPv6 and DNSv6, the DNS server IPv6 address is not sent to the clients if Neighbor Discovery or Router Advertisement is used. For this scenario, static IPv6 addresses need to be configured.

21.6.1 DNSv6 Configuration

The following describes DNSv6 configuration..

21.6.1.1 Global Configuration

The following is the global configuration of DNS:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# ip dns server <all static></code>	Configures the DNS configuration method (static or dynamic).
<code>(config-data)# ip name-server server1ipv6 [server2ip] all</code>	Configures the DNS server(s) IPv6 address in case of static configuration.

21.6.1.2 Interface-Specific Configuration

The following is the configuration of the DNS per interface:

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>(config-data)# interface int_name</code>	Selects an interface to configure.
<code>(config-if-name)# ip dns server <all static></code>	Configures an interface-specific DNS configuration method (static or dynamic).
<code>(config-if-name)# ip name-server server1ipv6 [server2ipv6] all</code>	Configures DNS server(s) IPv6 address in case of static configuration on the interface.

The device can act as a DNS server. To configure the device to act as a DNS server, use the following commands:

Command	Description
<code># configure data</code>	Enters the data configuration menu.

```
(config-data)# ip host <name>
<ip | IPv6> <TTL>
```

- <Name>: any name for the host.
- <IP | IPv6>: configure IPv4 or IPv6 for the name.
- <TTL>: Time to live of the DNS record.

21.6.2 Example of Basic Static DNS Configuration

This example configures a DNS record on the device. nslookup is used in the Windows workstation and another device unit is used to lookup the record. A Windows 7 workstation and another device (MSBR2) are connected to the LAN ports of the device. This example assumes that the DNS server IPv6 is 2001::1.

```
MSBR1# configure data
(config-data)# ip host audioCodes 2001::1 10
```

At the Window workstation, run *cmd*, type “nslookup”, and then do the following:

```
C:\Users\timg>nslookup
Default Server:  AudioCodes
Address:  2001::1
> set srchlist=
> set type=AAAA
> Audiocodes
Server:  AudioCodes
Address:  2001::1

Name:    Audiocodes
Addresses:  2001::1
           2001::1
>
```

On MSBR2, attached to the MSBR, use the following commands:

```
# configure gigabitethernet 0/0 to get IP from the MSBR1

MSBR2# configure data
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ipv6 address autoconfig

# Configure Static DNS Server
(conf-if-GE 0/0)# ip dns server static
(conf-if-GE 0/0)# ip name-server 2001::1

# Get IPv6 Record from the DNS
nslookup AudioCodes type aaaa
AudioCodes resolved to 2001::1
AudioCodes resolved to 2001::1

#
```

This page is intentionally left blank.

22 IP Multicast – PIM Sparse Mode

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism; however, instead uses routing information supplied by other routing protocols.

There are four variants of PIM. AudioCodes supports the most common variant:

PIM Sparse Mode (PIM-SM) explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage.

22.1 Feature Key

Advanced routing feature key must be enabled. Some networks require dynamic routing protocols- OSPF\BGP and VRF capabilities. To support these capabilities, the appropriate Feature key should be set.

22.2 CLI Configuration and Status Commands

The following describes the CLI Configuration and Status commands.

22.2.1 Configuration Commands

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>ip multicast-routing</code>	Enables the multicast protocol on the device.
<code>mode pim</code> <code>exit</code>	Sets multicast mode to PIM and returns to configure data .
<code>ip pim rp-address <ip> group <Multicast group prefix></code>	Sets static RP address for router, should be configured on all related PIM routers.
<code>ip pim rp-candidate <IP Interface> priority <0-255> time <0-3600></code>	<ul style="list-style-type: none"> Sets router to be a candidate RP, chosen by priority. Sets router to be a candidate RP, Advertising Interval in seconds. When interface is used – the RP candidate will be set to interface IP.
<code>ip pim bsr-candidate <IP Interface> priority <0-255></code>	<ul style="list-style-type: none"> Sets router to be a BSR candidate, chosen by priority when Interface is used – the BSR candidate will be set to interface IP.

Command	Description
<pre>ip pim spt-threshold infinity OR ip pim spt-threshold packets <number of packets> interval <sec> OR ip pim spt-threshold rate <kpps> interval <sec></pre>	<p>Sets threshold for moving to shortest path tree between the multicast server and the client.</p> <ul style="list-style-type: none"> ▪ infinity - Never switch to shortest path ▪ packets – Move to shortest path tree when number of packets threshold was crossed during the specified interval ▪ rate - Move to shortest path tree when packet rate threshold was crossed during the specified interval
group-prefix	Group Prefixes supported by RP Candidate. Up to 255 groups are supported.

22.2.2 Status Commands

Command	Description
show data ip mroute	Displays Multicast route information.
show data ip mroute interfaces	Displays Multicast route interface information.
show data ip mroute detail	Displays Detailed multicast route information.
show data ip pim bsr-router	Displays PIM BSR information.
show data ip pim groups	Displays PIM group information.
show data ip pim interfaces	Displays PIM interface and neighbor information.
show data ip pim rp	Displays PIM RP information.

```
# show data ip mroute
(Source, Multicast Group)      Input Interface      Output
Interface
(192.168.10.3, 232.0.0.42)     VLAN 1              Fiber 0/1

Show data ip mroute interfaces
500L - MSBR2*# show data ip mroute interfaces
  Interface      BytesIn  PktsIn  BytesOut  PktsOut  Flags      Local
Remote
  0 VLAN 1       26082   162     6956      7        NONE
192.168.2.1     0.0.0.0
  2 Giga 0/0      0        0        0          0        NONE
172.17.116.22   0.0.0.0
  3 Fiber 0/1     6956    7        0          0        NONE
200.200.200.2   0.0.0.0
```

```

 4 PIM          0      0      0      0      REGISTER
192.168.2.1     0.0.0.0

500L - MSBR2*#

```

show data ip mroute detail

Iif - Incoming interface, Oif - Outgoing interface

Origin	Group	Iif	Pkts	Bytes	Wrong
Oifs:TTL					
192.168.10.3	232.0.0.42	VLAN 1	36	27360	0

Fiber 0/1:1 PIM:1

show data ip pim groups

Multicast Group Routing Table - Legend:

Flags:

SPT Shortest Path Tree, internal interface toward source
 WC (*,G) entry
 RP internal interface iif toward RP
 CACHE a mirror for the kernel cache
 SG (S,G) pure, not hanging off of (*,G)
 CLONE_SG clone (S,G) from (*,G) or (*,*,RP)

Multicast Group Routing Table

Source	Group	RP addr	Flags
----- (*,G) -----			
INADDR_ANY	232.0.0.42	200.0.0.2	WC RP

Joined oifs: Fiber 0/1

Pruned oifs:

Leaves oifs:

Asserted oifs:

Outgoing oifs: Fiber 0/1

Incoming : PIM_FORWARDING

TIMERS:	Entry	Joine-Prune	Register-Suppression	Assert
	165	20	0	0

VLAN 1 : 0

Fiber 0/1 : 165

GigabitEthernet 0/0 : 0

PIM_FORWARDING : 0

Source	Group	RP addr	Flags
----- (S,G) -----			

192.168.10.3	232.0.0.42	200.0.0.2	SPT CACHE SG
--------------	------------	-----------	--------------

Joined oifs: Fiber 0/1 PIM_FORWARDING

Pruned oifs:

Leaves oifs:

Asserted oifs:

```

Outgoing oifs: Fiber 0/1 PIM_FORWARDING
Incoming      : VLAN 1

TIMERS:  Entry   Joine-Prune   Register-Suppression   Assert
          180     30           0                       0

VLAN 1                               : 0
Fiber 0/1                           : 180
GigabitEthernet 0/0                 : 0
PIM_FORWARDING                      : 0

Source          Group          RP addr          Flags
----- (*,*,RP) -----
Number of Groups: 1
Number of Cache MIRRORS: 1

show data ip pim interfaces
Virtual Interface Table - Flag Legend:
----
DOWN           Kernel state of interface
DISABLED       Administratively disabled
DR             Specified interface is the designated router
NO-NBR        No PIM neighbors on virtual interface
PIM           PIM neighbor on virtual interface
DVMRP        DVMRP neighbor on virtual interface
----

Virtual Interface Table
Vif  Local address  Interface  Thresh  Flags
Neighbors      (Expire)
  0  192.168.0.1    BVI 1      1       DR
NO-NBR
  2  10.31.2.86    GigabitEthernet 0/0  1
DISABLED
  3  200.0.0.1     Fiber 0/1    1       PIM
200.0.0.2      (00:01:30)

# show data ip pim rp
RP address      Interface      Group prefix  Priority
Holdtime (Seconds)
200.0.0.2      Fiber 0/1      224.0.0.0/4   1
65535

```

22.2.3 Multicast Example - Static RP

The concept of setting a static RP involves forcing the PIM protocol to use a specific IP address as the Rendezvous Point.

Use "ip multicast-routing" to enter the multicast routing configuration mode and activate the PIM protocol on the device.

```

ip multicast-routing
    mode pim
exit

```

Next, each interface that is used for multicast traffic should be specifically turned on:

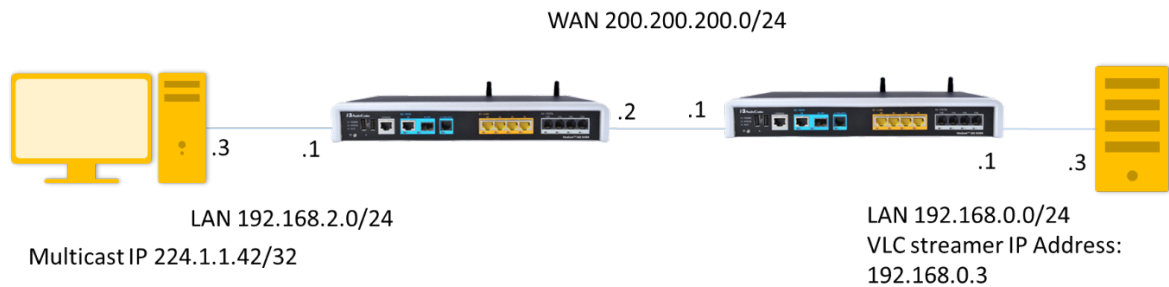
```
interface Fiber 0/1
  ip pim sparse-mode
exit
```

Setting static RP – the join-group packet will be sent to the RP IP address, in case the RP support the desired group – multicast streaming will be performed.

```
ip pim rp-address 200.0.0.2
```

The example below shows an implementation of media streaming using VLC free software.

Figure 22-1: Multicast Example - Static RP



- PC IP – 192.168.2.3 is the rtp receiver
- PC IP – 192.168.0.3 is the rtp transmitter

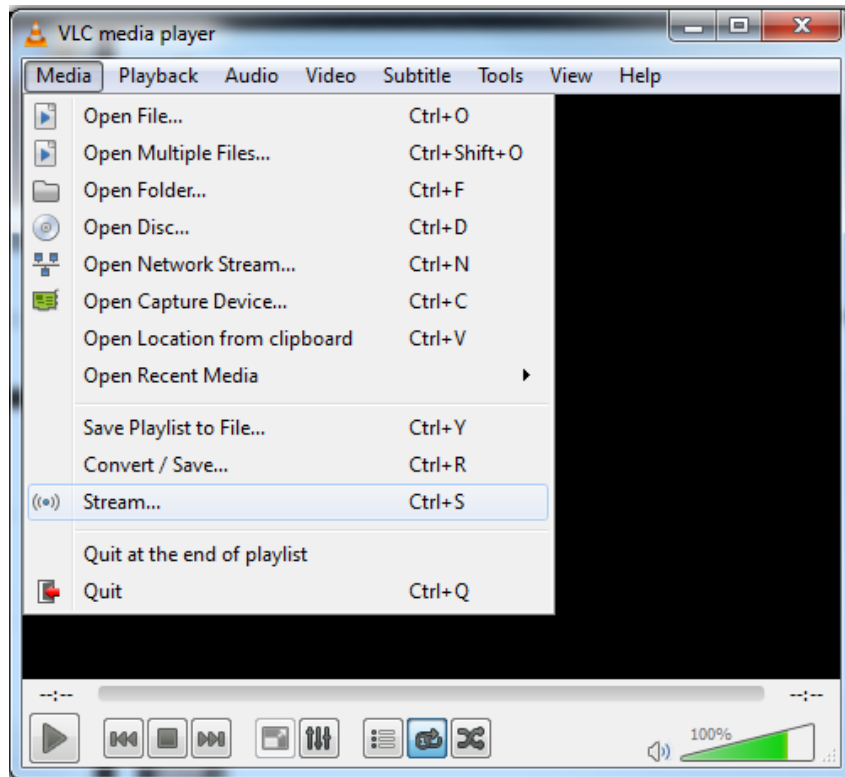
Setting Multicast Streamer and Receiver using VLC player :

<http://get.videolan.org/vlc/2.1.5/win32/vlc-2.1.5-win32.exe>

The example below shows an implementation of media streaming using VLC on the client side for receiving multicast traffic.

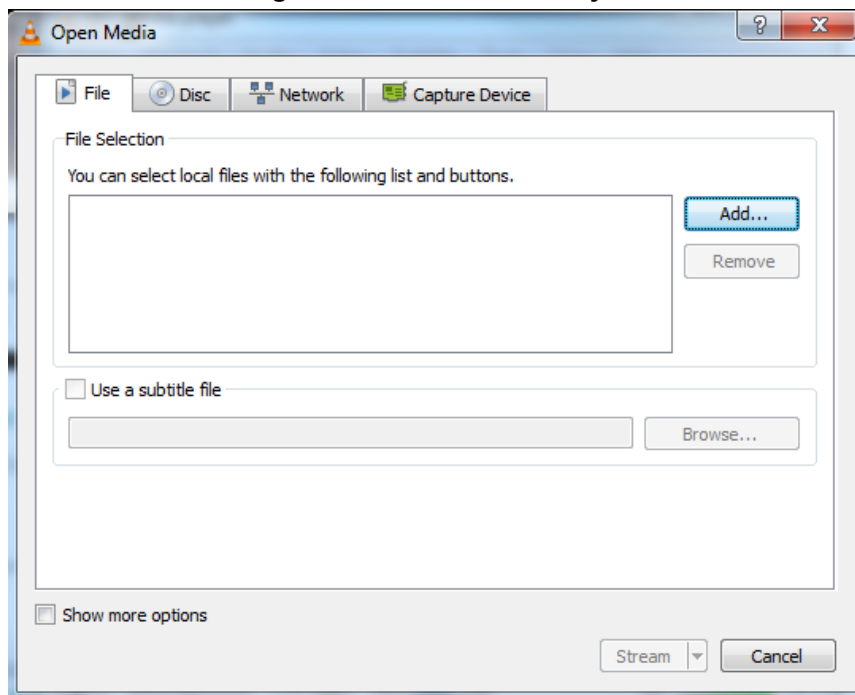
- To implement media streaming on the server side:
- 1. Open VLC:

Figure 22-2: VLC Media Player

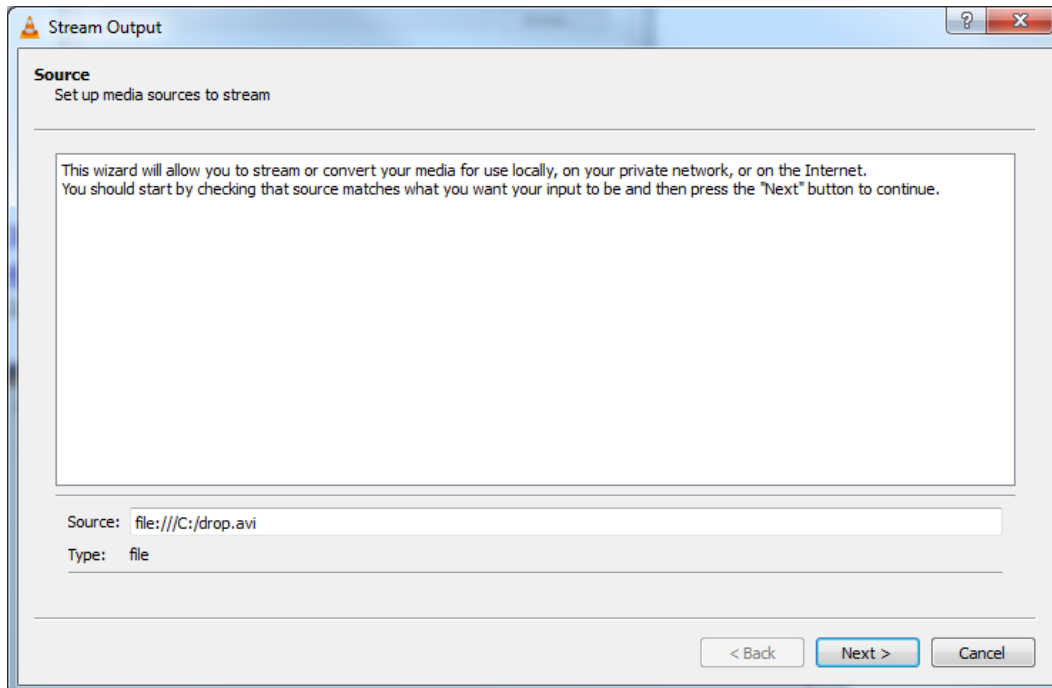


- 2. Add the media file to the stream and then select the stream.

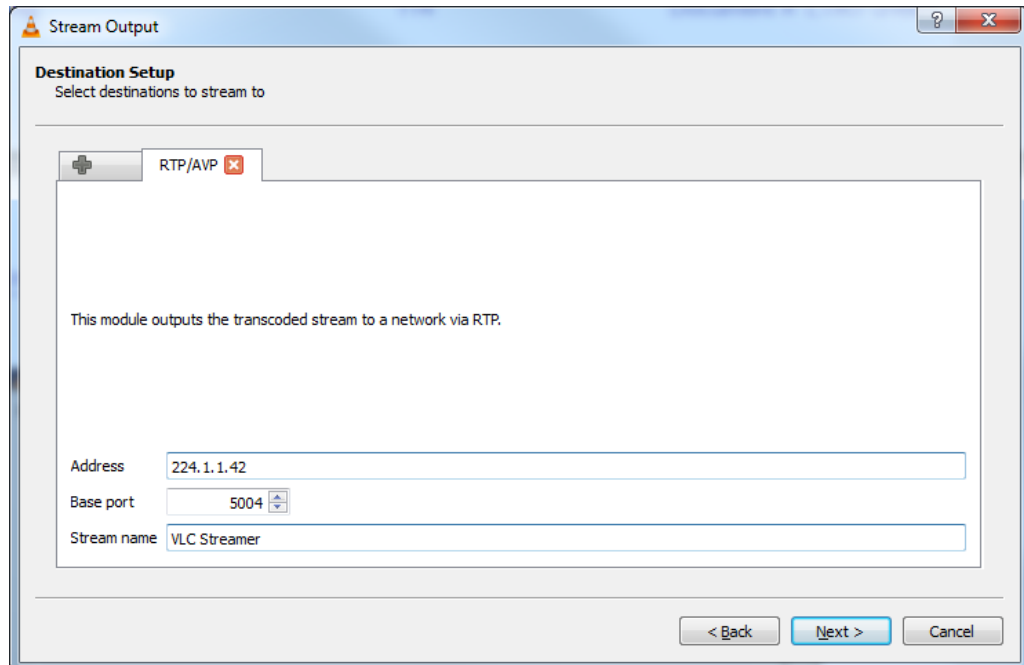
Figure 22-3: VLC Media Player



3. Continue with streaming wizard, and click **Next**.

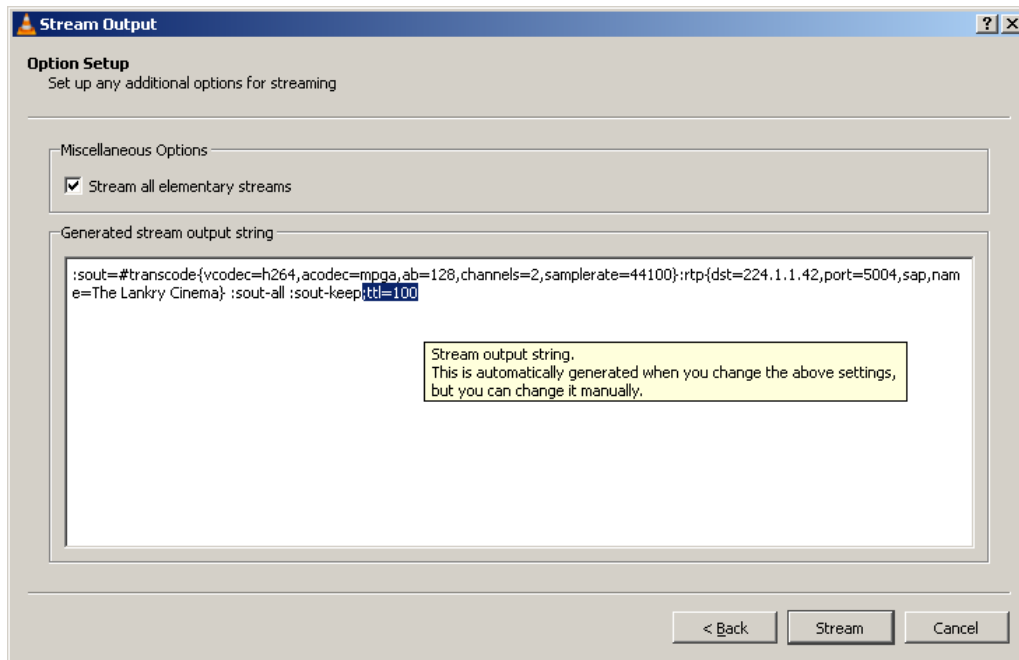
Figure 22-4: Stream Output

4. Stream to multicast address:

Figure 22-5: Stream Output-Destination Setup

5. Update the stream TTL manually.

Figure 22-6: Stream Output-Destination Setup-Option Setup

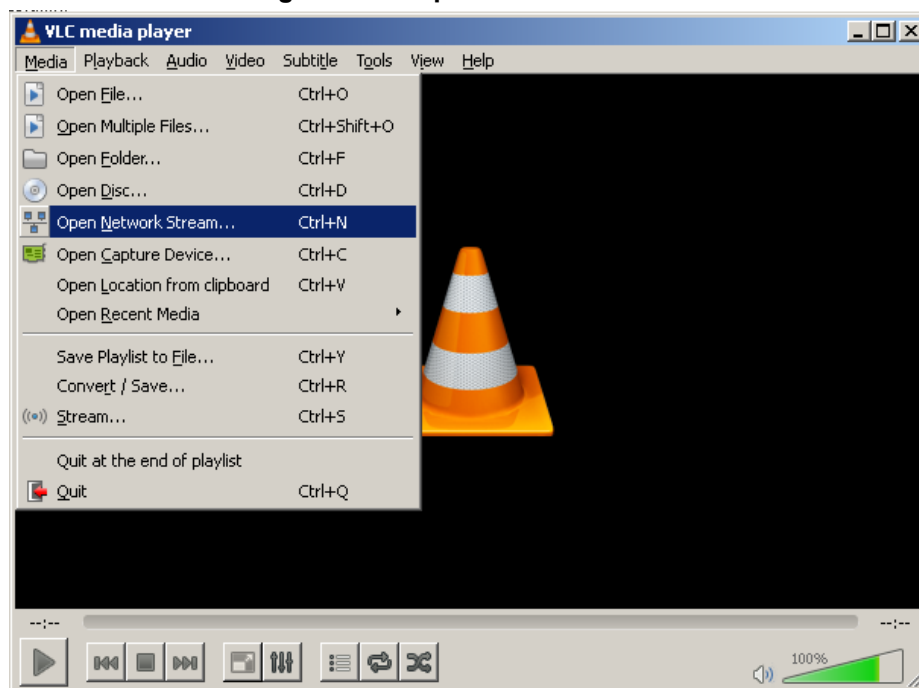


6. Click the **Stream** button to start streaming the movie.

➤ **To implement media streaming on the receiver side:**

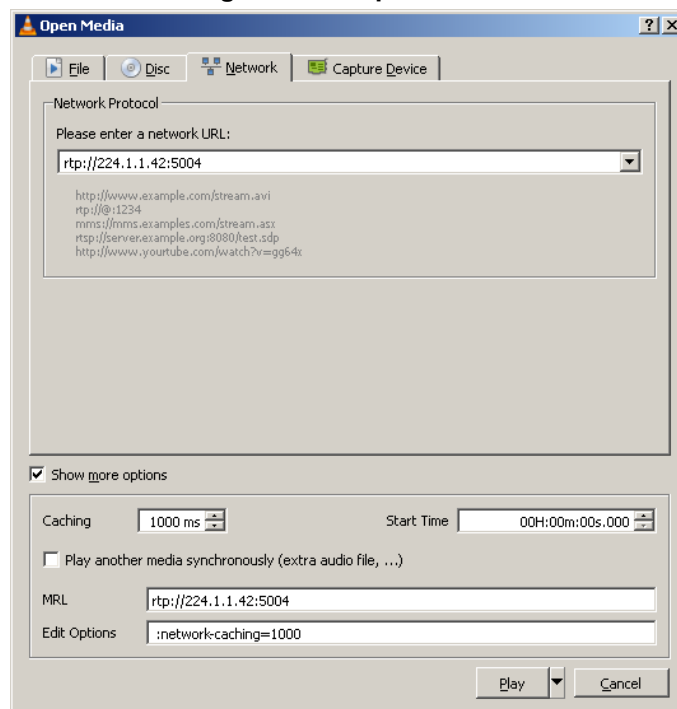
1. Open VLC.

Figure 22-7: Open Network Stream



2. Stream from multicast address.

Figure 22-8: Open Media



3. Watch Movie.

The following is an example of a *show run* command for two devices:

```
M500_Transmitter*# show run data

configure data
  ip multicast-routing
  mode pim
  exit
  interface GigabitEthernet 0/0
    ip address dhcp
    ip dhcp-client default-route
    mtu auto
    desc "WAN Copper"
    no ipv6 enable
    speed auto
    duplex auto
    no service dhcp
    ip dns server auto
    napt
    firewall enable
    no shutdown
  exit
  interface Fiber 0/1
    ip address 200.0.0.2 255.255.255.252
    ip pim sparse-mode
    mtu auto
    desc "WAN Fiber"
    no ipv6 enable
    no service dhcp
    ip dns server static
    no napt
    no firewall enable
    no shutdown
  exit
  interface dsl 0/2
    #DSL configuration is automatic
    #Termination cpe
    mode adsl
    shutdown
  exit
  interface EFM 0/2
    #This interface is DISABLED due to physical layer configuration
    no ip address
    mtu auto
    desc "WAN DSL"
    no ipv6 enable
    no service dhcp
    ip dns server static
```

```
no shutdown
exit
interface GigabitEthernet 1/1
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface GigabitEthernet 1/2
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface GigabitEthernet 1/3
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface GigabitEthernet 1/4
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface VLAN 1
  ip address 192.168.10.1 255.255.255.0
  ip pim sparse-mode
  mtu auto
  desc "LAN switch VLAN 1"
  no ipv6 enable
  ip dhcp-server network 192.168.10.3 192.168.10.8 255.255.255.0
  ip dhcp-server dns-server 0.0.0.0
  ip dhcp-server netbios-name-server 0.0.0.0
  ip dhcp-server lease 0 1 0
  ip dhcp-server provide-host-name
  ip dhcp-server ntp-server 0.0.0.0
  ip dhcp-server tftp-server 0.0.0.0
  ip dhcp-server override-router-address 0.0.0.0
  ip dhcp-server next-server 0.0.0.0
  service dhcp
  ip dns server static
  no napt
  no firewall enable
  no link-state monitor
  no shutdown
exit
```

```

ip pim rp-address 200.0.0.2
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 86400
ip nat translation icmp-timeout 6
# Note: The following WAN ports are in use by system services,
#       conflicting rules should not be created:
#       Ports 80 - 80 --> HTTP
#       Ports 23 - 23 --> Telnet CLI
#       Ports 22 - 22 --> SSH CLI
#       Ports 82 - 82 --> TR069
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
exit

```

Running Configuration M500_Reciver

Data Configuration

```

configure data
radio shutdown
ip multicast-routing
mode pim
exit

interface GigabitEthernet 0/0
ip address dhcp
ip dhcp-client default-route
mtu auto
desc "WAN Copper"
no ipv6 enable
speed auto
duplex auto
no service dhcp
ip dns server auto
napt
firewall enable
no shutdown
exit
interface Fiber 0/1
ip address 200.0.0.1 255.255.255.252
ip pim sparse-mode
mtu auto
desc "WAN Fiber"
no ipv6 enable
no service dhcp
ip dns server static
no napt

```

```
no firewall enable
no shutdown
exit
interface dsl 0/2
#DSL configuration is automatic
#Termination cpe
mode adsl
shutdown
exit
interface EFM 0/2
#This interface is DISABLED due to physical layer configuration
no ip address
mtu auto
desc "WAN DSL"
no ipv6 enable
no service dhcp
ip dns server static
no shutdown
exit
interface GigabitEthernet 1/1
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/2
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/3
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/4
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface VLAN 1
no ip address
bridge-group 1
mtu auto
```

```

desc "LAN switch VLAN 1"
no ipv6 enable
no service dhcp
no link-state monitor
no shutdown
exit
interface BVI 1
ip address 192.168.0.1 255.255.255.0
ip pim sparse-mode
mtu auto
desc "LAN Bridge"
ip dhcp-server network 192.168.0.3 192.168.0.8 255.255.255.0
ip dhcp-server dns-server 0.0.0.0
ip dhcp-server netbios-name-server 0.0.0.0
ip dhcp-server lease 0 1 0
ip dhcp-server provide-host-name
ip dhcp-server ntp-server 0.0.0.0
ip dhcp-server tftp-server 0.0.0.0
ip dhcp-server override-router-address 0.0.0.0
ip dhcp-server next-server 0.0.0.0
service dhcp
ip dns server static
no napt
no firewall enable
no shutdown
exit
interface dot11radio 1
#This interface is DISABLED due to physical layer configuration
no ip address
bridge-group 1
mtu auto
desc "LAN Wireless 802.11n Access Point"
no ipv6 enable
no service dhcp
ssid MSBR
broadcast
security mode NONE
no security mac mode
mode ngb
channel width 40/20
channel auto
wmm
exit
ip pim rp-address 200.0.0.2
router ospf
redistribute connected
network 200.0.0.0/30 area 1.1.1.1
exit
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 86400
ip nat translation icmp-timeout 6

```

```
# Note: The following WAN ports are in use by system services,
#       conflicting rules should not be created:
#       Ports 80 - 80 --> HTTP
#       Ports 23 - 23 --> Telnet CLI
#       Ports 22 - 22 --> SSH CLI
#       Ports 82 - 82 --> TR069
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
exit
```

22.2.4 Multicast Example - Dynamic RP – Bootstrap Router Elects RP

This section includes multicast examples for Dynamic RP – Bootstrap Router Elects RP. The VLC configuration and example from the “static multicast” chapter can be reused to run multicast traffic for demonstrating this section.

■ Making the device look for best RP:

Bootstrap Router publishes its multicast properties – the network selects the best Bootstrap Router as the multicast manager that indicates for the best Rendezvous Point as a multicast streamer.

Use “ip multicast-routing” to enter multicast configuration mode and “mode pim” to activate PIM protocol on the device.

Next, each interface that will be used for multicast traffic should be specifically turned on:

```
interface Fiber 0/1
    ip pim sparse-mode
exit
```

■ Server/Media Streaming Side:

Setting BSR – for the media streaming side we define the Giga 0/0 as the BSR. The BSR will define the best RP for IP multicast traffic.

```
ip pim bsr-candidate Fiber 0/1 priority 1
```

Setting RP defines the VLAN 1 IP address to be the device RP point;. the join-group packet is sent to the RP IP address. In case the RP supports the desired group, then multicast streaming will be made.

```
ip pim rp-candidate VLAN 1 priority 1
```

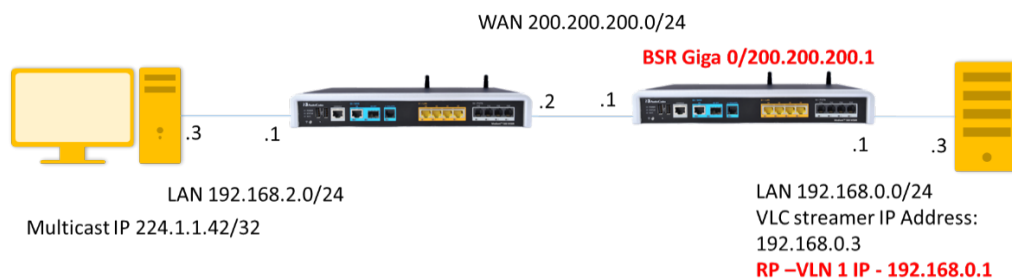
22.2.4.1 On the Client \ Media Receiving Side

No special configuration should be added. The user should activate “mode pim” in “ip multicast-routing” and specifically on each interface that uses the multicast traffic, the PIM protocol should be enabled.

```
configure data
ip multicast-routing
mode pim
exit
interface Fiber 0/1
ip pim sparse-mode
no shutdown
exit
interface BVI 1
ip pim sparse-mode
no shutdown
exit
```

The figure below illustrates the implementation of media streaming using VLC free software on the server side, and using VLC on the client side for receiving multicast traffic.

Figure 22-9: Setup Description



Voice and System configurations were not changed and are written in the static RP example.

23 IP Multicast – IGMP Proxy

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast. The group refers to the multicast address (224.0.0.0/4).

The IGMP proxy feature allows the device to forward clients' IGMP messages for multicast services from the LAN towards the multicast source via the WAN interface. When the device receives multicast traffic on the WAN interface, it forwards the traffic towards any LAN interface that has previously sent an IGMP join message to the device.

When a client in the LAN wishes to leave the multicast group, it sends an IGMP Leave message to the device on the LAN interface. If this is the last client to leave the group from the LAN interface, then the device will not forward the multicast traffic to the interface. If this is the last client to leave the group from all the LAN interfaces of the device, the device sends an IGMP Leave message to the multicast source.

23.1 Feature Key

Advanced routing feature key must be enabled.

23.2 CLI Configuration and Status Commands

23.2.1 Configuration Commands

Command	Description
<code># configure data</code>	Enters the data configuration menu.
<code>ip multicast-routing</code>	Enters the multicast protocol menu
<code>mode igmp-proxy</code>	Sets multicast mode to IGMP Proxy
<code>igmp fast-leave</code> <code>exit</code>	Stops multicast forwarding to interfaces on last IGMP leave message, exit back to configure data
<code>Interface <interface></code>	Enters interface to enable igmp proxy
<code>igmp enable-proxy</code>	Enables igmp proxy on interface <ul style="list-style-type: none">• Same command for LAN and WAN interfaces

23.2.2 Status Commands

Command	Description
show data ip igmp proxy groups	IGMP proxy group information
show data ip igmp proxy lan-interface <interface>	IGMP proxy information per LAN interface
show data ip igmp proxy lan-interfaces	IGMP proxy LAN interfaces information

```
# show data ip igmp proxy groups
Active WAN Interfaces with IGMPv3 proxies
GigabitEthernet 0/0
VLAN 1

Group                Subscriber IFs on Group  Timer for Unsolicited
Report
232.3.4.111          2                        Done Sending
232.3.4.119          1                        Done Sending
232.3.4.1             1                        1.1
232.131.41.101        1                        2.91
232.9.9.9             1                        Done Sending
232.9.9.19            1                        Done Sending
232.9.9.191           1                        Done Sending
232.31.4.111          1                        Done Sending
```

```
# show data ip igmp proxy lan-interfaces
Interface: VLAN 2
IGMPv3 State: Querier
Groups: 1
[0]: group 232.3.4.111
    filter mode: Exclude
    group timer: 156 seconds left
    client(s): 00:90:8f:4b:fb:61
Interface: VLAN 4
IGMPv3 State: Querier
Groups: 0
```

```
# show data ip igmp proxy lan-interface <interface>

Interface: VLAN 2
IGMPv3 State: Querier
Groups: 1
[0]: group 232.3.4.111
    filter mode: Exclude
    group timer: 194 seconds left
    client(s): 00:90:8f:4b:fb:61
```

23.2.3 Multicast Example

The minimal configuration has one LAN interface with igmp proxy enabled and one LAN interface with igmp proxy enabled. A LAN interface will receive IGMP messages from clients and will forward traffic related to the clients' groups accordingly. A WAN interface will forward IGMP messages to the WAN for the relevant groups, and listen for multicast traffic from that group.

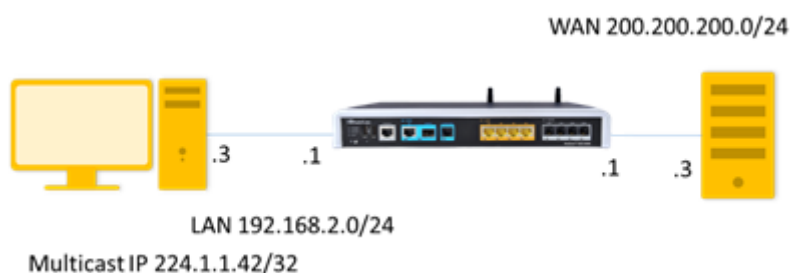
First, enable igmp-proxy mode from the data configuration mode:

```
configure data
  ip multicast-routing
    mode igmp-proxy
  exit
```

Next, enable igmp-proxy on a LAN interface and a WAN interface

```
interface GigabitEthernet 0/0
  ip igmp enable-proxy
exit
interface VLAN 1
  ip igmp enable-proxy
exit
```

Figure 23-1 Multicast Example – IGMP Proxy



- PC IP – 192.168.2.3 is the rtp receiver
- PC IP – 200.200.200.3 is the rtp transmitter.

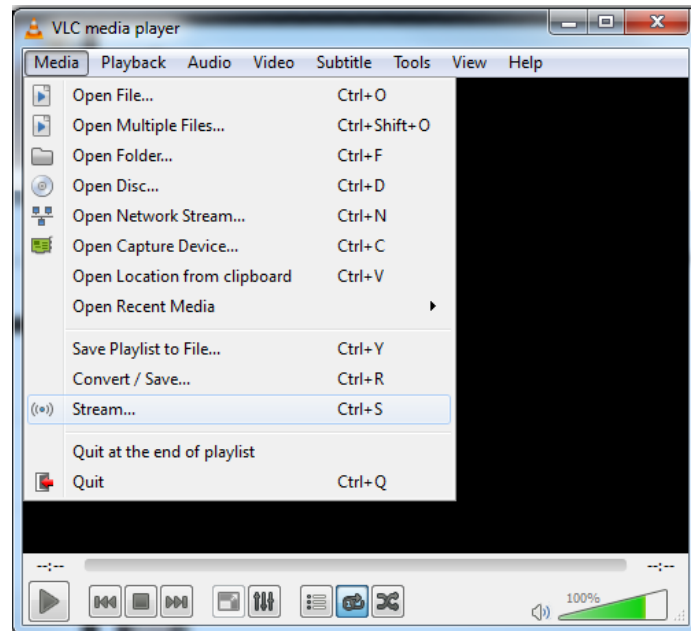
Setting Multicast Streamer and Receiver using VLC player:

<http://get.videolan.org/vlc/2.1.5/win32/vlc-2.1.5-win32.exe>

The example below shows an implementation of media streaming using VLC on the client side for receiving multicast traffic.

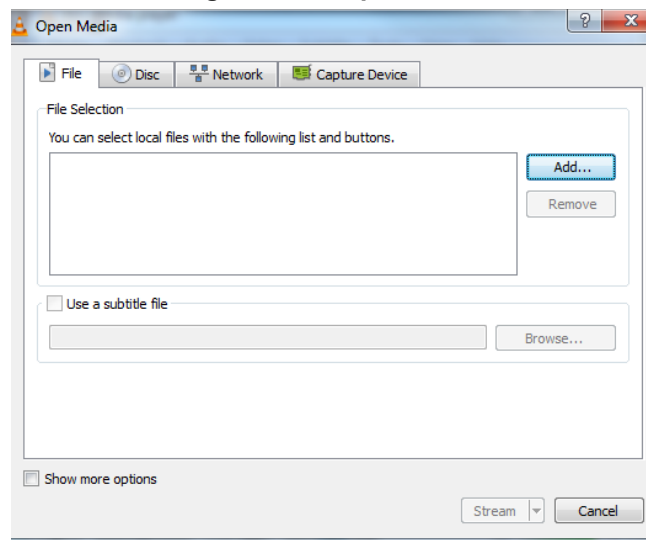
- To implement media streaming on the server side:
1. Open VLC; the following screen appears.

Figure 23-2: VLC Media Player

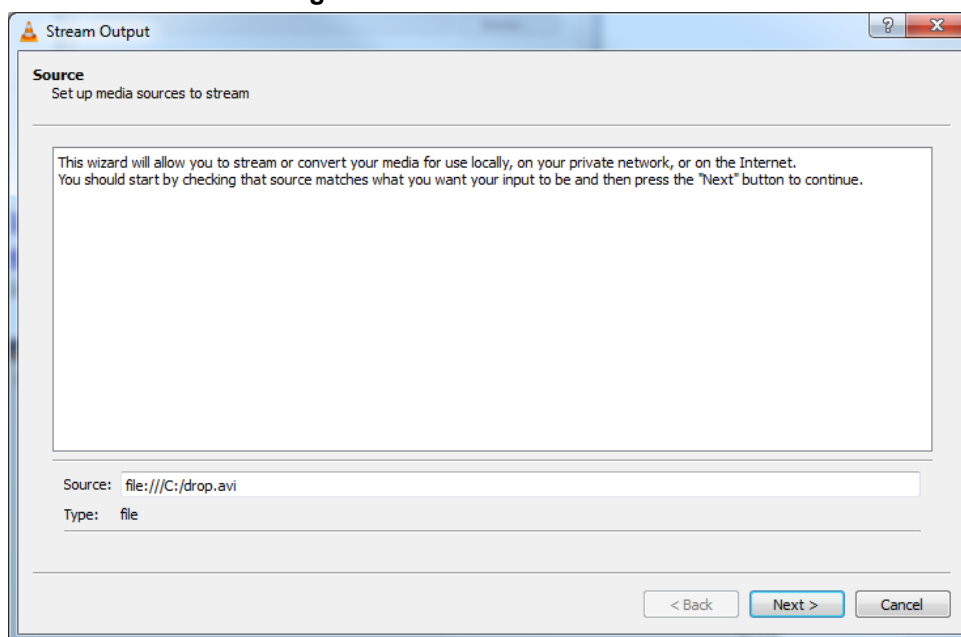


2. Add the media file to the stream and then click **Stream**.

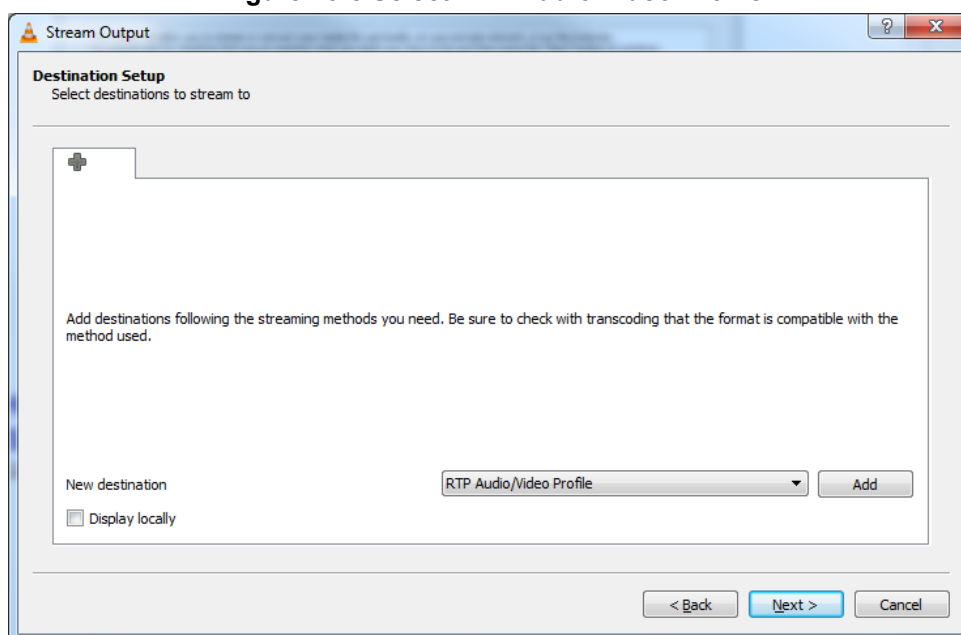
Figure 23-3: Open Media



3. Continue with the streaming wizard.

Figure 23-4 Add Media to Stream

4. From the 'New destination' drop-down list, select **RTP Audio/Video Profile** and then click **Add**.

Figure 23-5 Select RTP Audio/Video Profile

5. Stream to the multicast address.

Figure 23-6: Stream Output-Destination Setup

6. Update the stream TTL manually.

Figure 23-7: Stream Output-Destination Setup-Option Setup

7. Click **Stream** to start streaming the movie.

➤ **To implement media streaming on the receiver side:**

1. Open VLC.

Figure 23-8: VLC Media Player

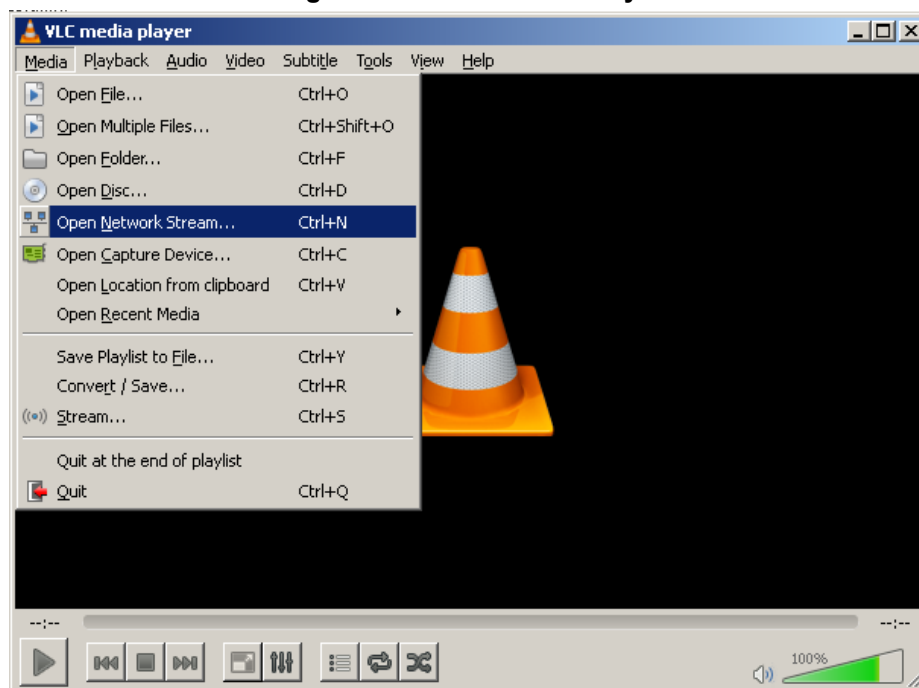
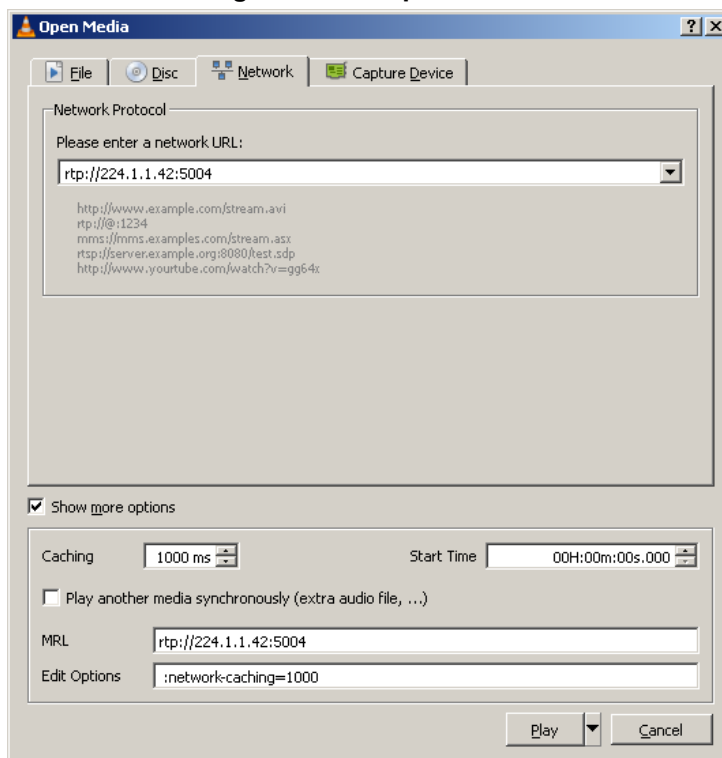


Figure 23-9 Open Network Stream

2. Stream from the multicast address.

Figure 23-10: Open Media



3. Click **Play** to watch the movie.

The following is an example of a *show run* command for the device:

```
M500 *# show run data

configure data
  ip multicast-routing
  mode igmp-proxy
exit
interface GigabitEthernet 0/0
  ip address dhcp
  ip dhcp-client default-route
  mtu auto
  desc "WAN Copper"
  no ipv6 enable
  speed auto
  duplex auto
  no service dhcp
  ip dns server auto
  napt
  firewall enable
  no shutdown
exit
interface Fiber 0/1
  ip address 200.0.0.2 255.255.255.252
  ip igmp enable-proxy
  mtu auto
  desc "WAN Fiber"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no napt
  no firewall enable
  no shutdown
exit
interface dsl 0/2
  #DSL configuration is automatic
  #Termination cpe
  mode adsl
  shutdown
exit
interface EFM 0/2
  #This interface is DISABLED due to physical layer configuration
  no ip address
  mtu auto
  desc "WAN DSL"
  no ipv6 enable
  no service dhcp
  ip dns server static
  no shutdown
exit
```



```
interface GigabitEthernet 1/1
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface GigabitEthernet 1/2
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface GigabitEthernet 1/3
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface GigabitEthernet 1/4
  speed auto
  duplex auto
  switchport mode trunk
  switchport trunk native vlan 1
  no shutdown
exit
interface VLAN 1
  ip address 192.168.10.1 255.255.255.0
  ip igmp enable-proxy
  mtu auto
  desc "LAN switch VLAN 1"
  no ipv6 enable
  ip dhcp-server network 192.168.10.3 192.168.10.8 255.255.255.0
  ip dhcp-server dns-server 0.0.0.0
  ip dhcp-server netbios-name-server 0.0.0.0
  ip dhcp-server lease 0 1 0
  ip dhcp-server provide-host-name
  ip dhcp-server ntp-server 0.0.0.0
  ip dhcp-server tftp-server 0.0.0.0
  ip dhcp-server override-router-address 0.0.0.0
  ip dhcp-server next-server 0.0.0.0
  service dhcp
  ip dns server static
  no napt
  no firewall enable
  no link-state monitor
  no shutdown
exit
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 86400
```

```
ip nat translation icmp-timeout 6
# Note: The following WAN ports are in use by system services,
#       conflicting rules should not be created:
#       Ports 80 - 80 --> HTTP
#       Ports 23 - 23 --> Telnet CLI
#       Ports 22 - 22 --> SSH CLI
#       Ports 82 - 82 --> TR069
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
exit
```

A Mediant 500 Transmitter Examples

M500_Transmitter

```
configure data
ip multicast-routing
interface GigabitEthernet 0/0
ip address dhcp
ip dhcp-client default-route
mtu auto
desc "WAN Copper"
no ipv6 enable
speed auto
duplex auto
no service dhcp
ip dns server auto
napt
firewall enable
no shutdown
exit
interface Fiber 0/1
ip address 200.0.0.2 255.255.255.252
ip pim sparse-mode
mtu auto
desc "WAN Fiber"
no ipv6 enable
no service dhcp
ip dns server static
no napt
no firewall enable
no shutdown
exit
interface dsl 0/2
#DSL configuration is automatic
#Termination cpe
mode adsl
shutdown
exit
interface EFM 0/2
#This interface is DISABLED due to physical layer configuration
no ip address
mtu auto
desc "WAN DSL"
no ipv6 enable
no service dhcp
ip dns server static
no shutdown
exit
interface GigabitEthernet 1/1
speed auto
duplex auto
```

```

switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/2
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/3
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/4
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface VLAN 1
ip address 192.168.10.1 255.255.255.0
ip pim sparse-mode
mtu auto
desc "LAN switch VLAN 1"
no ipv6 enable
ip dhcp-server network 192.168.10.3 192.168.10.8 255.255.255.0
ip dhcp-server dns-server 0.0.0.0
ip dhcp-server netbios-name-server 0.0.0.0
ip dhcp-server lease 0 1 0
ip dhcp-server provide-host-name
ip dhcp-server ntp-server 0.0.0.0
ip dhcp-server tftp-server 0.0.0.0
ip dhcp-server override-router-address 0.0.0.0
ip dhcp-server next-server 0.0.0.0
service dhcp
ip dns server static
no napt
no firewall enable
no link-state monitor
no shutdown
exit
ip pim bsr-candidate Fiber 0/1 priority 1
ip pim rp-candidate VLAN 1 priority 1
ip pim spt-threshold packets 10 interval 10
router ospf
redistribute connected

```

```
network 200.0.0.0/30 area 1.1.1.1
exit
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 86400
ip nat translation icmp-timeout 6
# Note: The following WAN ports are in use by system services,
#       conflicting rules should not be created:
#       Ports 80 - 80 --> HTTP
#       Ports 23 - 23 --> Telnet CLI
#       Ports 22 - 22 --> SSH CLI
#       Ports 82 - 82 --> TR069
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
exit
```

M500_Receiver

```
configure data
radio shutdown
ip multicast-routing
interface GigabitEthernet 0/0
ip address dhcp
ip dhcp-client default-route
mtu auto
desc "WAN Copper"
no ipv6 enable
speed auto
duplex auto
no service dhcp
ip dns server auto
napt
firewall enable
no shutdown
exit
interface Fiber 0/1
ip address 200.0.0.1 255.255.255.252
ip pim sparse-mode
mtu auto
desc "WAN Fiber"
no ipv6 enable
no service dhcp
ip dns server static
no napt
no firewall enable
no shutdown
exit
interface dsl 0/2
#DSL configuration is automatic
```

```
#Termination cpe
mode adsl
shutdown
exit
interface EFM 0/2
#This interface is DISABLED due to physical layer configuration
no ip address
mtu auto
desc "WAN DSL"
no ipv6 enable
no service dhcp
ip dns server static
no shutdown
exit
interface GigabitEthernet 1/1
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/2
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/3
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface GigabitEthernet 1/4
speed auto
duplex auto
switchport mode trunk
switchport trunk native vlan 1
no shutdown
exit
interface VLAN 1
no ip address
bridge-group 1
mtu auto
desc "LAN switch VLAN 1"
no ipv6 enable
no service dhcp
no link-state monitor
no shutdown
```

```
exit
interface BVI 1
 ip address 192.168.0.1 255.255.255.0
 ip pim sparse-mode
 mtu auto
 desc "LAN Bridge"
 ip dhcp-server network 192.168.0.3 192.168.0.8 255.255.255.0
 ip dhcp-server dns-server 0.0.0.0
 ip dhcp-server netbios-name-server 0.0.0.0
 ip dhcp-server lease 0 1 0
 ip dhcp-server provide-host-name
 ip dhcp-server ntp-server 0.0.0.0
 ip dhcp-server tftp-server 0.0.0.0
 ip dhcp-server override-router-address 0.0.0.0
 ip dhcp-server next-server 0.0.0.0
 service dhcp
 ip dns server static
 no napt
 no firewall enable
 no shutdown
exit
interface dot11radio 1
#This interface is DISABLED due to physical layer configuration
 no ip address
 bridge-group 1
 mtu auto
 desc "LAN Wireless 802.11n Access Point"
 no ipv6 enable
 no service dhcp
 ssid MSBR
 broadcast
 security mode NONE
 no security mac mode
 mode ngb
 channel width 40/20
 channel auto
 wmm
exit
router ospf
 redistribute connected
 network 200.0.0.0/30 area 1.1.1.1
exit
ip nat translation udp-timeout 120
ip nat translation tcp-timeout 86400
ip nat translation icmp-timeout 6
# Note: The following WAN ports are in use by system services,
#       conflicting rules should not be created:
#       Ports 80 - 80 --> HTTP
#       Ports 23 - 23 --> Telnet CLI
#       Ports 22 - 22 --> SSH CLI
#       Ports 82 - 82 --> TR069
```

```
ip domain name home
ip domain localhost msbr
pm sample-interval minute 5
pm sample-interval seconds 15
exit
```


This page is intentionally left blank.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com/>

©2020 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VolPerfect, VolPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-31748

