ARCHIVED DOCUMENT

This document is archived and should only be used as a historical reference and should not be used for new deployments for one of the following reasons:

- SD-WAN guides are the recommended alternative.

- This document is outdated. There are no plans to update the content.

For the latest guides, please refer to:
https://cisco.com/go/cvd

CISCO VALIDATED DESIGN

Intelligent WAN Multiple VRFs Deployment Guide

September 2017

Table of Contents

Deploying the Cisco Intelligent WAN

This guide is one in a series of IWAN advanced deployment guides that focus on how to deploy the advanced features of the Cisco Intelligent WAN (IWAN). These guides build on the configurations deployed in the Intelligent WAN Deployment Guide and are optional components of its base IWAN configurations.

The advanced guides are as follows:

- IWAN High Availability and Scalability Deployment Guide
- IWAN Multiple Data Center Deployment Guide
- IWAN Multiple Transports Deployment Guide
- IWAN Multiple VRF Deployment Guide (this guide)
- IWAN Public Key Infrastructure Deployment Guide
- IWAN NetFlow Monitoring Deployment Guide
- IWAN Remote Site 4G LTE Deployment Guide

For design details, see Intelligent WAN Design Summary.

For configuration details, see Intelligent WAN Configuration Files Guide.

For an automated way to deploy IWAN, use the APIC-EM IWAN Application. For more information, see the Cisco IWAN Application on APIC-EM User Guide.

If want to use TrustSec with your IWAN deployment, see “Configuring SGT Propagation” in the User-to-Data-Center Access Control Using TrustSec Deployment Guide.

Deploying the Cisco IWAN Multiple VRFs

Virtual routing and forwarding instances (VRFs) are important for isolating end-to-end traffic among multiple independent servers inside the same data center (DC)—for example, private contractor servers and Internet of Things (IoT) servers operating in the same DC. Similarly, on the remote location client side, private contractor computers and IoT devices can co-exist inside the same physical hardware as the common employee network.

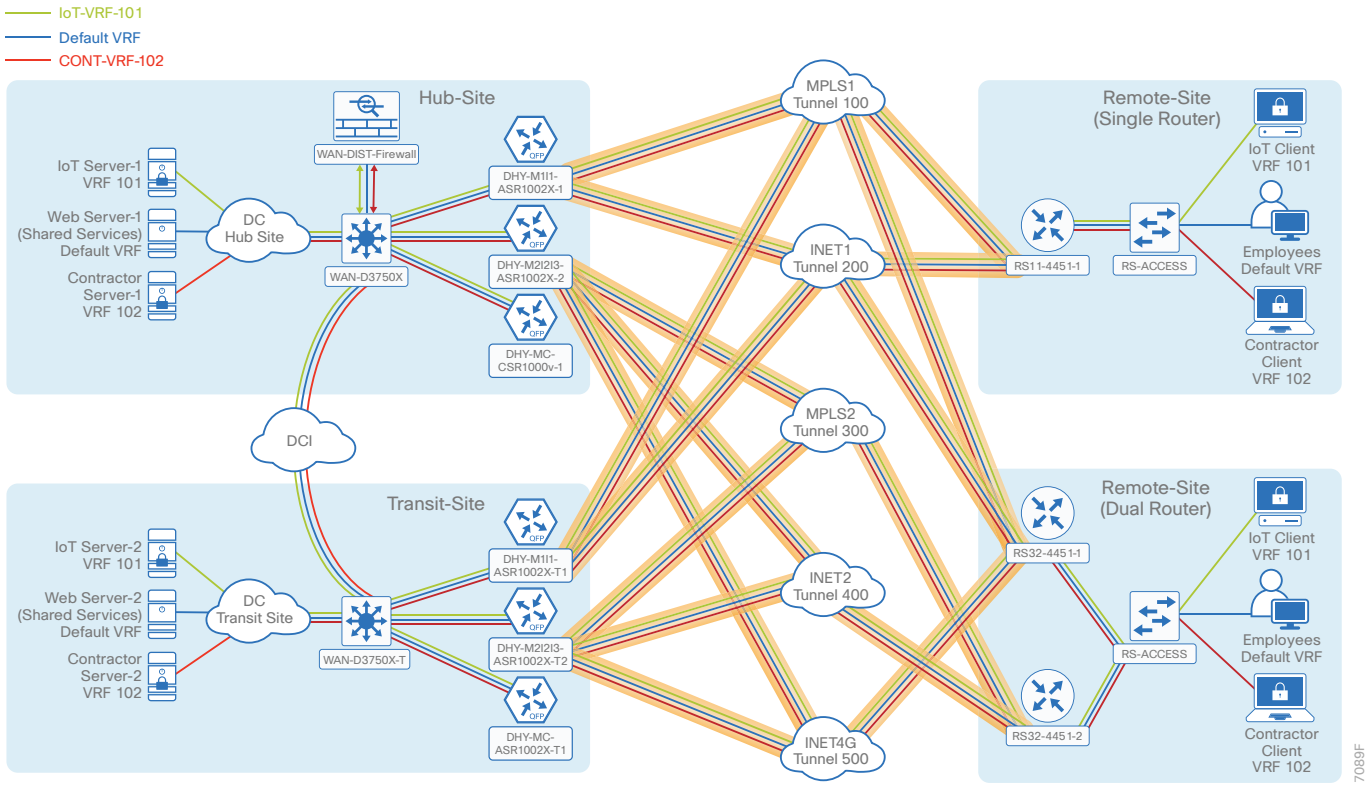
IWAN multiple VRF deployments require additional VLANs, loopback interfaces, IP subnets, routing protocol instances, and IWAN domains to keep the traffic properly segmented from one end of the WAN to the other. This separation on the WAN allows an organization to carry isolated traffic from the DC to the remote site LAN, while only allowing it to mix at designated points with very strict access policies.

On the DMVPN side, a single IPsec session is established between routers for all VRFs using the same physical interface on the router. This means the individual tunnels which share a tunnel source interface must use the same IPsec profile, and unlike a standard IWAN deployment, they must have shared tunnel protection configured. To allow the router to differentiate between the individual tunnels after decryption, a unique tunnel key value is required per VRF.

Inter-VRF route leaking is used to share global services such as DNS, DHCP, the company web portal, etc. between the different isolated segments. This design uses a firewall, attached to the WAN distribution switch at the hub-site location, to import and export individual VRF route information to and from the global routing tables. This gives the network administrator a secure device to manage the separation between the logical networks

The following figure depicts the overall architecture. The hub-site and transit-site are connected by a data center interconnect (DCI) link. Both sites are further connected to the remote sites via a dynamic multipoint virtual private network (DMVPN) over multiple wide-area network (WAN) transports.

Figure 1 *Multi VRF overview topology*



The design uses three inside VRFs (IVRFs) as follows:

- **Default VRF** (in diagrams, using a blue connector)—Traditional employee traffic and shared services (DNS, DHCP and AD, etc.)
- **IoT-VRF-101** (green connector)—IoT related traffic
- **CONT-VRF-102** (red connector)—Limited access for contractors

Reader Tip

In order for PfR route-control to function properly, traffic must ingress an interface on the LAN side that resides in the same VRF as the egress tunnel interface that PfR is monitoring. The network should be designed according to this requirement and is demonstrated in the diagram above as well as throughout this CVD

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

PROCESS

Configuring the Hub-Site WAN Distribution Switch

1. Configure the IVRF definitions and loopbacks
2. Create VLANs and switched virtual interfaces
3. Configure the port-channels
4. Define the static routes for Inter-VRF route leaking
5. Configure the routing protocol for OSPF

This process assumes that the distribution switch has already been configured following the guidance in the Campus LAN Layer 2 Access with Simplified Distribution Deployment Guide. Only the procedures required to support the integration of the WAN aggregation router into the deployment are included.

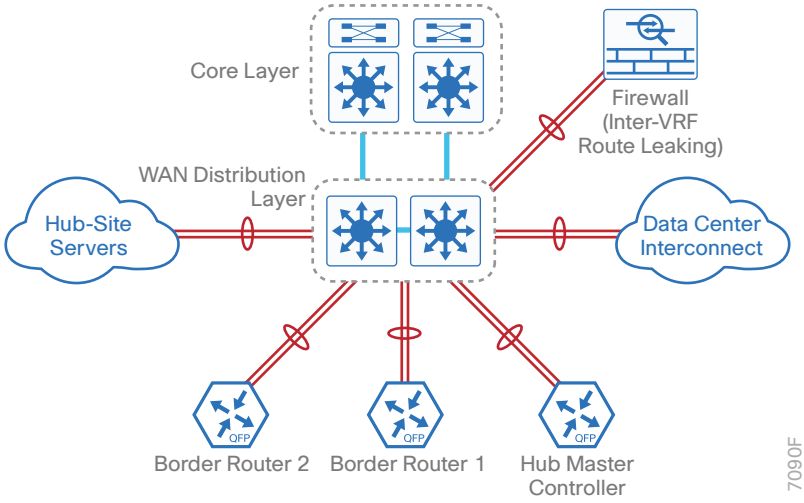
The hub-site WAN distribution switch is the path to the organization's main campus and DC. It is also an aggregation point between the firewall and rest of the network for multi-VRF traffic. This design uses the virtual local area network (VLAN) trunking with Layer 2 port-channel interfaces between the distribution switch and connected devices to carry multi-VRF traffic.

Tech Tip

As a best practice, use the same channel numbering on both sides of the link where possible.

The following figure describes the physical network connections for inside the hub-site.

Figure 2 *Physical view of WAN distribution at hub-site location*



The diagram below shows three different colored lines (green, blue and red)—one for each of the VRFs described in the previous section.

Figure 3 *Logical view of WAN distribution at hub-site location*

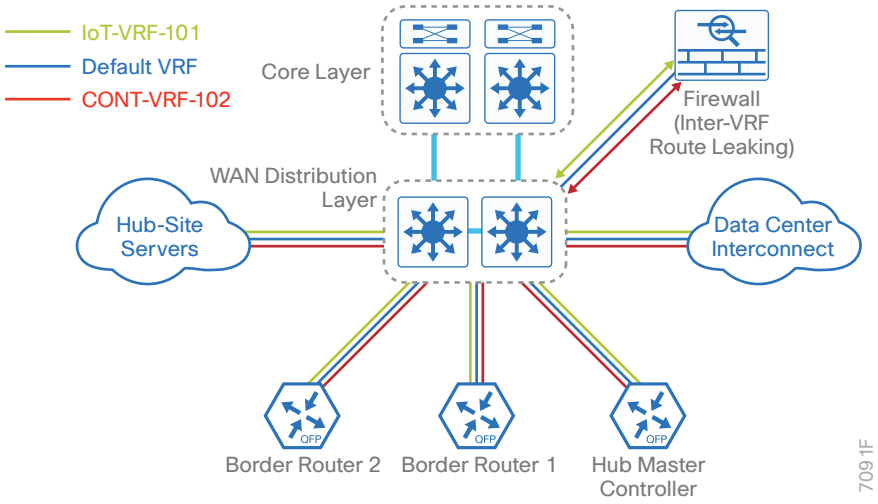


Table 1 *IP address information of hub-site WAN distribution switch*

VRF name	Loopback interface	IP address	OSPF process-id
Default	Loopback 0	10.6.32.240/32	100
IoT-VRF-101	Loopback 101	10.21.32.240/32	101
CONT-VRF-102	Loopback 102	10.25.32.240/32	102

Procedure 1 Configure the IVRF definitions and loopbacks

In this procedure, you configure the definitions for the two new IVRFs and their associated loopbacks.

Step 1: Configure the IVRFs.

```
vrf definition IoT-VRF-101
 rd 101:1

 address-family ipv4
 exit-address-family

vrf definition CONT-VRF-102
 rd 102:1

 address-family ipv4
 exit-address-family
```

Step 2: Configure the loopback interfaces.

```
interface Loopback101
 description IoT-VRF-101
 vrf forwarding IoT-VRF-101
 ip address 10.21.32.240 255.255.255.255
 ip pim sparse-mode

interface Loopback102
 description CONT-VRF-102
 vrf forwarding CONT-VRF-102
 ip address 10.25.32.240 255.255.255.255
 ip pim sparse-mode
```

Procedure 2 Create VLANs and switched virtual interfaces

In this procedure, you create the VLANs and switched virtual interfaces (SVI) interfaces.

Step 1: Create VLANs for the default VRF. You should repeat this step for each VLAN using the parameters in the table below.

Table 2 VLAN information for hub-site WAN distribution switch

Connected devices	Default VRF	IoT-VRF-101	CONT-VRF-102
DHY-MC-CSR1000v-1 (MC)	VLAN 1100	VLAN 1101	VLAN 1102
DHY-M1I1-ASR1002X-1 (BR1)	VLAN 1110	VLAN 1111	VLAN 1112
DHY-M2I2I3-ASR1002X-2 (BR2)	VLAN 1120	VLAN 1121	VLAN 1122
DCI	VLAN 10	VLAN 11	VLAN 12
Firewall (for route leaking)	VLAN 20	VLAN 21	VLAN 22
Hub-Site Shared Services	VLAN 30	VLAN 31	VLAN 32

Example: VLAN database configuration for default VRF

```
vlan 1100
 name DHY_WAN_Srvcs_DefaultVRF
```

Step 2: Create SVI interfaces for the default VRF. You should repeat this step for each SVI interface using the parameters in the table below.

Table 3 Default VRF IP addresses for hub-site WAN distribution switch

Connected devices	VLAN-ID	IP address	Subnet mask
DHY-MC-CSR1000v-1 (MC)	VLAN 1100	10.6.32.129	255.255.255.224
DHY-M1I1-ASR1002X-1 (BR1)	VLAN 1110	10.6.32.5	255.255.255.252
DHY-M2I2I3-ASR1002X-2 (BR2)	VLAN 1120	10.6.32.1	255.255.255.252
DCI	VLAN 10	10.8.32.97	255.255.255.252
Firewall (for route leaking)	VLAN 20	10.6.32.25	255.255.255.248
Hub-Site Shared Services	VLAN 30	10.6.32.33	255.255.255.248

Example: SVI interface configuration for default VRF

```
interface Vlan1100
 description DHY_WAN_Srvcs_DefaultVRF
 ip address 10.6.32.129 255.255.255.224
 ip pim sparse-mode
```

Step 3: Create SVI interfaces for IoT-VRF-101 using the parameters in the table below.

Table 4 IoT-VRF-101 IP addresses for hub-site WAN distribution switch

Connected devices	VLAN-ID	IP address	Subnet mask
DHY-MC-CSR1000v-1 (MC)	VLAN 1101	10.21.32.129	255.255.255.224
DHY-M1I1-ASR1002X-1 (BR1)	VLAN 1111	10.21.32.5	255.255.255.252
DHY-M2I2I3-ASR1002X-2 (BR2)	VLAN 1121	10.21.32.1	255.255.255.252
DCI	VLAN 11	10.23.32.97	255.255.255.252
Firewall (for route leaking)	VLAN 21	10.21.32.25	255.255.255.248
Hub-Site Shared Services	VLAN 31	10.21.32.33	255.255.255.248

Step 4: Create SVI interfaces for CONT-VRF-102 using the parameters in the table below.

Table 5 CONT-VRF-102 IP addresses for hub-site WAN distribution switch

Connected devices	VLAN-ID	IP address	Subnet mask
DHY-MC-CSR1000v-1 (MC)	VLAN 1102	10.25.32.129	255.255.255.224
DHY-M1I1-ASR1002X-1 (BR1)	VLAN 1112	10.25.32.5	255.255.255.252
DHY-M2I2I3-ASR1002X-2 (BR2)	VLAN 1122	10.25.32.1	255.255.255.252
DCI	VLAN 12	10.27.32.97	255.255.255.252
Firewall (for route leaking)	VLAN 22	10.25.32.25	255.255.255.248
Hub-Site Shared Services	VLAN 32	10.25.32.33	255.255.255.248

Procedure 3 Configure the port-channels

In this procedure, you create the port-channels and assign the interface members to the port-channels. This procedure should be repeated for all the port-channels listed in the table below.

Table 6 Port-channels information for hub-site WAN distribution switch

Connected devices	Port-channel	VLAN-ID range	Physical interface
DHY-MC-CSR1000v-1 (MC)	Port-channel 21	VLAN 1100 - 1102	Gig 1/0/15 Gig 2/0/15
DHY-M1I1-ASR1002X-1 (BR1)	Port-channel 1	VLAN 1110 - 1112	Gig 1/0/1 Gig 2/0/1
DHY-M2I2I3-ASR1002X-2 (BR2)	Port-channel 2	VLAN 1120 - 1122	Gig 1/0/2 Gig 2/0/2
DCI	Port-channel 10	VLAN 10 - 12	Gig 1/0/24 Gig 2/0/24
Firewall (for route leaking)	Port-channel 20	VLAN 20 - 22	Gig 1/0/23 Gig 2/0/23
Hub-Site Shared Services	Port-channel 30	VLAN 30 - 32	Gig 1/0/18 Gig 2/0/18

Step 1: Create the port-channel.

```
interface Port-channel21
 description DHY-MC-CSR1000v-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1100-1102
 switchport mode trunk
```

Step 2: Add the interfaces to the port-channel.

```
interface range GigabitEthernet1/0/15, GigabitEthernet2/0/15
 description DHY-MC-CSR1000v-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1100-1102
 switchport mode trunk
 logging event trunk-status
 logging event bundle-status
 channel-group 21 mode on
```

Procedure 4 Define the static routes for Inter-VRF route leaking

Using static routes, route leaking between the global routing table (GRT) and VRF table is quite easy. You either provide the next-hop IP address (for multi-access segment) or point the route out of an interface (point-to-point interface).

In this procedure, you define the next-hop IP address.

Step 1: Define next-hop IP address for multi VRF routes from the GRT.

```
ip route 10.20.0.0 255.252.0.0 10.6.32.26
ip route 10.24.0.0 255.252.0.0 10.6.32.26
ip route 10.201.240.0 255.255.252.0 10.6.32.26
ip route 10.202.240.0 255.255.252.0 10.6.32.26
```

Step 2: Define next-hop IP address for the GRT from IoT-VRF-101.

```
ip route vrf IoT-VRF-101 0.0.0.0 0.0.0.0 10.21.32.26
```

Step 3: Define next-hop IP address for the GRT from CONT-VRF-102.

```
ip route vrf CONT-VRF-102 0.0.0.0 0.0.0.0 10.25.32.26
```

Procedure 5 Configure the routing protocol for OSPF

Step 1: Configure OSPF for the default VRF.

```
router ospf 100
 router-id 10.6.32.240
 redistribute static subnets
 passive-interface default
 no passive-interface Vlan10
 no passive-interface Vlan20
 no passive-interface Vlan30
 no passive-interface Vlan1100
 no passive-interface Vlan1110
 no passive-interface Vlan1120
 network 10.6.0.0 0.1.255.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
```

Step 2: Configure OSPF for the IoT-VRF-101 VRF.

```
router ospf 101 vrf IoT-VRF-101
 router-id 10.21.32.240
 redistribute static subnets
 passive-interface default
 no passive-interface Vlan11
 no passive-interface Vlan21
 no passive-interface Vlan31
 no passive-interface Vlan1101
 no passive-interface Vlan1111
 no passive-interface Vlan1121
 no passive-interface Loopback101
 network 10.21.0.0 0.0.255.255 area 0
 network 10.23.0.0 0.0.255.255 area 0
 default-information originate
```

Step 3: Configure OSPF for the CONT-VRF-102 VRF.

```
router ospf 102 vrf CONT-VRF-102
 router-id 10.25.32.240
 redistribute static subnets
 passive-interface default
 no passive-interface Vlan12
 no passive-interface Vlan22
 no passive-interface Vlan32
 no passive-interface Vlan1102
 no passive-interface Vlan1112
 no passive-interface Vlan1122
 no passive-interface Loopback 102
 network 10.25.0.0 0.0.255.255 area 0
 network 10.27.0.0 0.0.255.255 area 0
 default-information originate
```

PROCESS

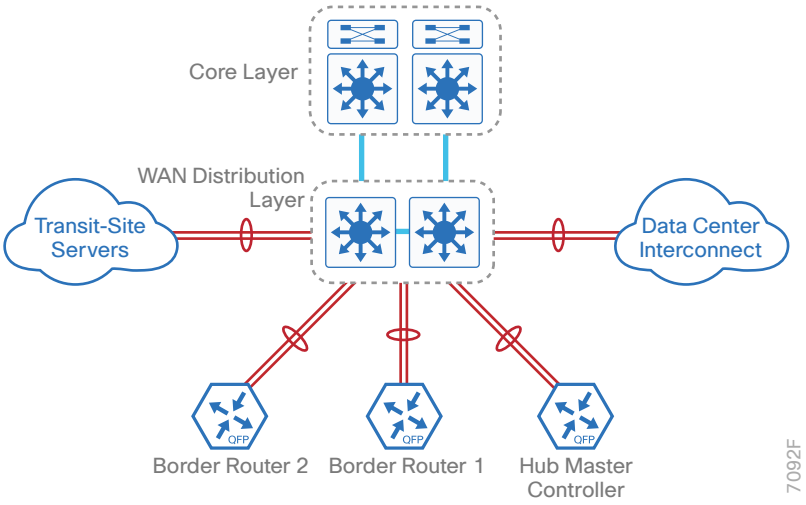
Configuring the Transit-Site WAN Distribution Switch

1. Configure the IVRF definitions and loopbacks
2. Create VLANs and SVIs
3. Configure the port-channels
4. Configure the routing protocol for OSPF

This design also uses the VLAN trunking with Layer 2 port-channel interfaces between the distribution switch and connected devices to carry multi-VRF traffic.

The following figure describes the physical network connections for the transit-site.

Figure 4 *Physical view of WAN distribution at transit-site location*



The diagram below shows three different colored lines (green, blue and red)—one for each of the VRFs described in the previous section.

Figure 5 *Logical view of WAN distribution at transit-site location*

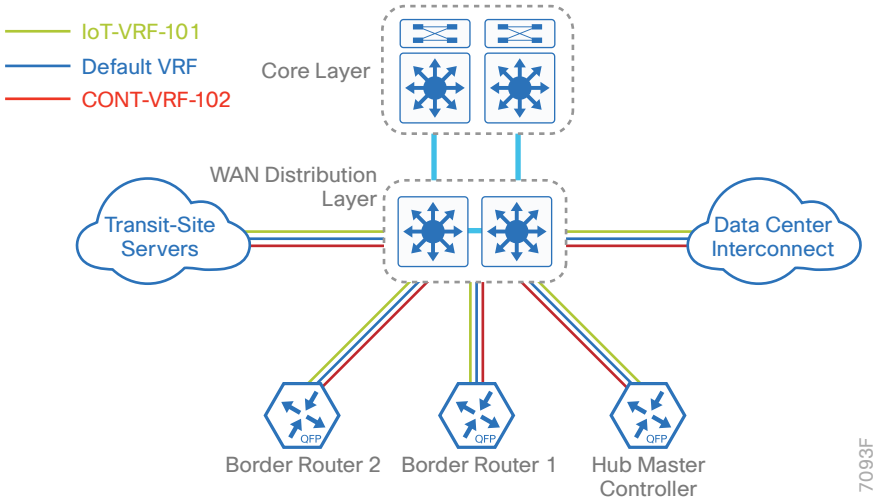


Table 7 *VRFs and loopback interfaces for transit-site WAN distribution switch*

VRF name	Loopback interface	IP address	OSPF process-id
Default	Loopback 0	10.8.32.240/32	100
IoT-VRF-101	Loopback 101	10.23.32.240/32	101
CONT-VRF-102	Loopback 102	10.27.32.240/32	102

Procedure 1 Configure the IVRF definitions and loopbacks

In this procedure, you configure the definitions for the two new IVRFs and their associated loopbacks.

Step 1: Configure the IVRFs.

```
vrf definition IoT-VRF-101
 rd 101:1

 address-family ipv4
 exit-address-family

vrf definition CONT-VRF-102
 rd 102:1

 address-family ipv4
 exit-address-family
```

Step 2: Configure the loopback interfaces.

```
interface Loopback101
 description IoT-VRF-101
 vrf forwarding IoT-VRF-101
 ip address 10.23.32.240 255.255.255.255
 ip pim sparse-mode

interface Loopback102
 description CONT-VRF-102
 vrf forwarding CONT-VRF-102
 ip address 10.27.32.240 255.255.255.255
 ip pim sparse-mode
```

Procedure 2 Create VLANs and SVIs

Step 1: Create VLANs for the default VRF. You should repeat this step for each VLAN by using the parameters in the table below.

Table 8 VLAN information for transit-site WAN distribution switch

Connected devices	Default VRF	IoT-VRF-101	CONT-VRF-102
DHY-MC-ASR1002X-T1 (MC)	VLAN 1100	VLAN 1101	VLAN 1102
DHY-M1I1-ASR1002X-T1 (BR1)	VLAN 1110	VLAN 1111	VLAN 1112
DHY-M2I2I3-ASR1002X-T2 (BR2)	VLAN 1120	VLAN 1121	VLAN 1122
DCI	VLAN 10	VLAN 11	VLAN 12
Transit-Site Shared Services	VLAN 30	VLAN 31	VLAN 32

Example: VLAN database configuration

```
vlan 1100
 name DHY_WAN_Srvcs_DefaultVRF
```

Step 2: Create SVI interfaces for the default VRF. You should repeat this step for each SVI interface by using the parameters in the table below.

Table 9 Global VRF IP addresses for transit-site WAN distribution switch

Connected devices	VLAN-ID	IP address	Subnet mask
DHY-MC-ASR1002X-T1 (MC)	VLAN 1100	10.8.32.129	255.255.255.224
DHY-M1I1-ASR1002X-T1 (BR1)	VLAN 1110	10.8.32.5	255.255.255.252
DHY-M2I2I3-ASR1002X-T2 (BR2)	VLAN 1120	10.8.32.1	255.255.255.252
DCI	VLAN 10	10.8.32.98	255.255.255.252
Transit-Site Shared Services	VLAN 30	10.8.32.33	255.255.255.248

Example: SVI interface configuration for default VRF

```
interface Vlan1100
 description DHY_WAN_Srvcs_DefaultVRF
 ip address 10.8.32.129 255.255.255.224
 ip pim sparse-mode
```

Step 3: Create SVI interfaces for IoT-VRF-101 by using the parameters in the table below.

Table 10 IoT-VRF-101 IP addresses for transit-site WAN distribution switch

Connected devices	VLAN-ID	IP address	Subnet mask
DHY-MC-ASR1002X-T1 (MC)	VLAN 1101	10.23.32.129	255.255.255.224
DHY-M1I1-ASR1002X-T1 (BR1)	VLAN 1111	10.23.32.5	255.255.255.252
DHY-M2I2I3-ASR1002X-T2 (BR2)	VLAN 1121	10.23.32.1	255.255.255.252
DCI	VLAN 11	10.23.32.98	255.255.255.252
Transit-Site Shared Services	VLAN 31	10.23.32.33	255.255.255.248

Step 4: Create SVI interfaces for CONT-VRF-102 by using the parameters in the table below.

Table 11 CONT-VRF-102 IP addresses for transit-site WAN distribution switch

Connected devices	VLAN-ID	IP address	Subnet mask
DHY-MC-ASR1002X-T1 (MC)	VLAN 1102	10.27.32.129	255.255.255.224
DHY-M1I1-ASR1002X-T1 (BR1)	VLAN 1112	10.27.32.5	255.255.255.252
DHY-M2I2I3-ASR1002X-T2 (BR2)	VLAN 1122	10.27.32.1	255.255.255.252
DCI	VLAN 12	10.27.32.98	255.255.255.252
Transit-Site Shared Services	VLAN 32	10.27.32.33	255.255.255.248

Procedure 3 Configure the port-channels

In this procedure, you create the port-channels and assign the interface members to the port-channels. This procedure should be repeated for all the port-channels listed in the table.

Table 12 Port-channels information for transit-site WAN distribution switch

Connected devices	Port-channel	VLAN-ID range	Physical interface
DHY-MC-ASR1002X-T1 (MC)	Port-channel 21	VLAN 1100 - 1102	Gig 1/0/3 Gig 2/0/3
DHY-M1I1-ASR1002X-T1 (BR1)	Port-channel 1	VLAN 1110 - 1112	Gig 1/0/1 Gig 2/0/1
DHY-M2I2I3-ASR1002X-T2 (BR2)	Port-channel 2	VLAN 1120 - 1122	Gig 1/0/2 Gig 2/0/2
DCI	Port-channel 10	VLAN 10 - 12	Gig 1/0/24 Gig 2/0/24
Transit-site shared services	Port-channel 30	VLAN 30 - 32	Gig 1/0/18 Gig 2/0/18

Step 1: Create the port-channel.

```
interface Port-channel21
 description DHY-MC-ASR1002X-T1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1100-1102
 switchport mode trunk
```

Step 2: Add the interfaces to the port-channel.

```
interface range GigabitEthernet1/0/3, GigabitEthernet2/0/3
 description DHY-MC-ASR1002X-T1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1100-1102
 switchport mode trunk
 logging event trunk-status
 logging event bundle-status
 channel-group 21 mode on
```

Procedure 4 Configure the routing protocol for OSPF

Step 1: Configure OSPF for default VRF.

```
router ospf 100
 router-id 10.8.32.240
 redistribute static subnets
 passive-interface default
 no passive-interface Vlan10
 no passive-interface Vlan30
 no passive-interface Vlan1100
 no passive-interface Vlan1110
 no passive-interface Vlan1120
 network 10.8.0.0 0.1.255.255 area 0
```

Step 2: Configure OSPF for IoT-VRF-101.

```
router ospf 101 vrf IoT-VRF-101
 router-id 10.23.32.240
 redistribute static subnets
 passive-interface default
 no passive-interface Vlan11
 no passive-interface Vlan31
 no passive-interface Vlan1101
 no passive-interface Vlan1111
 no passive-interface Vlan1121
 no passive-interface Loopback101
 network 10.21.0.0 0.0.255.255 area 0
 network 10.23.0.0 0.0.255.255 area 0
 default-information originate
```

Step 3: Configure OSPF for CONT-VRF-102.

```
router ospf 102 vrf CONT-VRF-102
 router-id 10.27.32.240
 redistribute static subnets
 passive-interface default
 no passive-interface Vlan12
```

```
no passive-interface Vlan32
no passive-interface Vlan1102
no passive-interface Vlan1112
no passive-interface Vlan1122
no passive-interface Loopback102
network 10.25.0.0 0.0.255.255 area 0
network 10.27.0.0 0.0.255.255 area 0
default-information originate
```

PROCESS

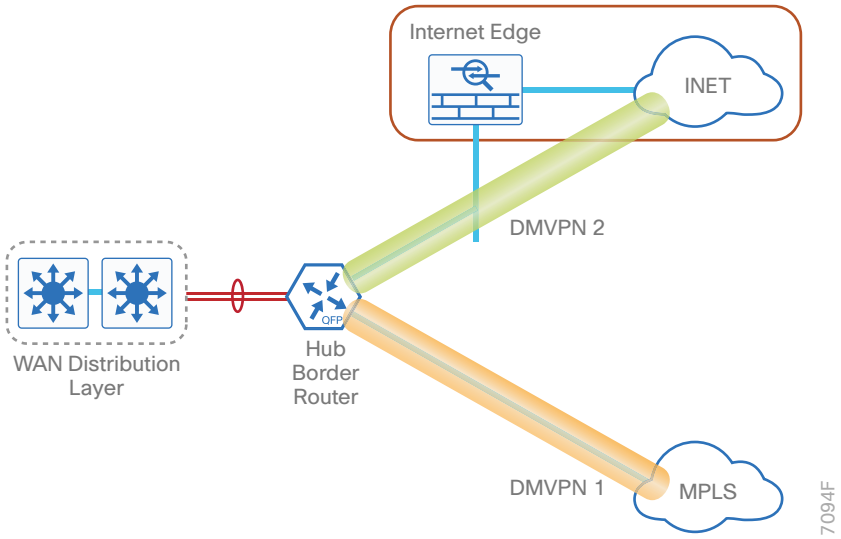
Configuring the DMVPN Hub Border Routers

1. Configure the IVRF definitions and loopbacks
2. Configure the connections to WAN distribution switch
3. Configure IKEv2 and IPsec profiles
4. Configure the mGRE tunnel
5. Configure the routing protocol for OSPF
6. Configure the routing protocol for BGP
7. Configure the prefix-lists for OSPF and BGP
8. Configure the prefix route maps for OSPF and BGP
9. Configure the static null routes and EOT

Use this process to configure the DMVPN hub border routers and repeat it for each DMVPN hub router.

The diagram below shows the physical connections between the WAN distribution switch and the hub router, as well as the connections for the MPLS and Internet transports.

Figure 6 *Physical view of border router at hub location*



The diagram below shows the Multi-VRF connections between the WAN distribution switch and the hub router, as well as the connections for the MPLS and Internet transports.

Figure 7 *Multi-VRF view of border router at hub location*

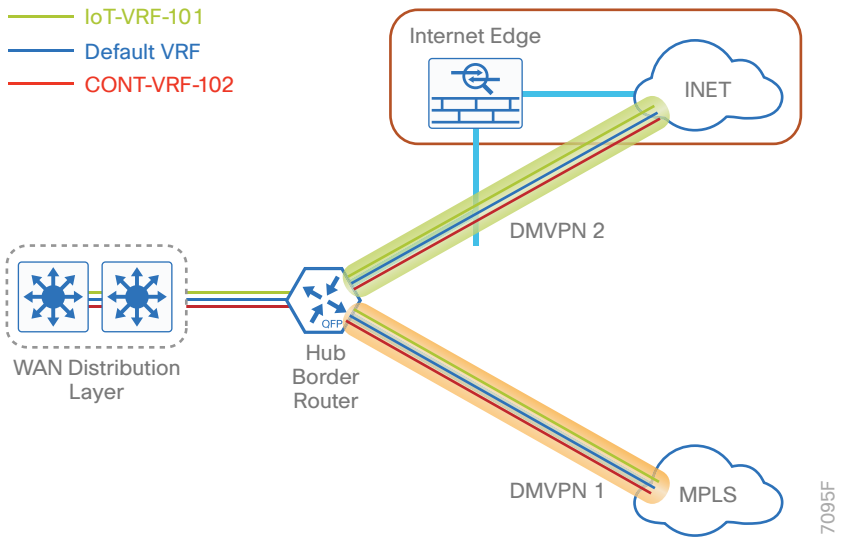


Table 13 VRFs and loopback interfaces for hub-site border router 1 (DHY-M1I1-ASR1002X-1)

VRF name	Loopback interface	IP address	OSPF process-id
Default VRF	Loopback 0	10.6.32.241/32	100
IoT-VRF-101	Loopback 101	10.21.32.241/32	101
CONT-VRF-102	Loopback 102	10.25.32.241/32	102

Table 14 VRFs and loopback interfaces for hub-site border router 2 (DHY-M2I2I3-ASR1002X-2)

VRF name	Loopback interface	IP address	OSPF process-id
Default VRF	Loopback 0	10.6.32.241/32	100
IoT-VRF-101	Loopback 101	10.21.32.241/32	101
CONT-VRF-102	Loopback 102	10.25.32.241/32	102

Table 15 VRFs and loopback interfaces for transit-site border router 1 (DHY-M1I1-ASR1002X-T1)

VRF name	Loopback interface	IP address	OSPF process-id
Default VRF	Loopback 0	10.6.32.241/32	100
IoT-VRF-101	Loopback 101	10.21.32.241/32	101
CONT-VRF-102	Loopback 102	10.25.32.241/32	102

Table 16 VRFs and loopback interfaces for transit-site border router 2 (DHY-M2I2I3-ASR1002X-T2)

VRF name	Loopback interface	IP address	OSPF process-id
Default VRF	Loopback 0	10.6.32.241/32	100
IoT-VRF-101	Loopback 101	10.21.32.241/32	101
CONT-VRF-102	Loopback 102	10.25.32.241/32	102

Reader Tip

Whenever IWAN is designed with WAAS leveraging AppNav, please ensure that the Loopback IP address that is being used for PfR is not also used as the AppNav Service Controller address. This is applicable for any Hub IWAN router that is part of an AppNav Cluster.

Procedure 1 Configure the IVRF definitions and loopbacks

In this procedure, you configure the definitions for the two new IVRFs and their associated loopbacks.

Step 1: Configure the IVRFs.

```
vrf definition IoT-VRF-101
 rd 101:1

 address-family ipv4
 exit-address-family

vrf definition CONT-VRF-102
 rd 102:1

 address-family ipv4
 exit-address-family
```

Step 2: Create the loopback interfaces.

```
interface Loopback101
 description IoT-VRF-101
 vrf forwarding IoT-VRF-101
 ip address 10.21.32.241 255.255.255.255
 ip pim sparse-mode

interface Loopback102
 description CONT-VRF-102
 vrf forwarding CONT-VRF-102
 ip address 10.25.32.241 255.255.255.255
```

Step 3: Using the parameters in the tables above, repeat the previous step for all border routers.

Procedure 2 Configure the connections to WAN distribution switch

In this procedure, you configure the port-channels and port-channel sub-interfaces, then add the local interface members to the respective port-channels.

Table 17 Physical connections to WAN distribution switch

Border routers	Local interfaces	WAN distribution switch	Port-channel
DHY-M1I1-ASR1002X-1	Gig 0/0/0 Gig 0/0/1	IW-WAN-D3750X	Port-channel 1
DHY-M2I2I3-ASR1002X-2	Gig 0/0/0 Gig 0/0/1	IW-WAN-D3750X	Port-channel 1
DHY-M1I1-ASR1002X-T1	Gig 0/0/0 Gig 0/0/1	IW-WAN-D3750X-T	Port-channel 1
DHY-M2I2I3-ASR1002X-T2	Gig 0/0/0 Gig 0/0/1	IW-WAN-D3750X-T	Port-channel 1

Table 18 Sub port-channel information for hub-site border router 1

VRF name	VLAN-ID	IP address	Trunk interface
Default VRF	VLAN 1110	10.6.32.2/30	Port-channel 1.1110
IoT-VRF-101	VLAN 1111	10.21.32.2/30	Port-channel 1.1111
CONT-VRF-102	VLAN 1112	10.25.32.2/30	Port-channel 1.1112

Table 19 Sub port-channel information for hub-site border router 2

VRF name	VLAN-ID	IP address	Trunk interface
Default VRF	VLAN 1110	10.6.32.2/30	Port-channel 1.1110
IoT-VRF-101	VLAN 1111	10.21.32.2/30	Port-channel 1.1111
CONT-VRF-102	VLAN 1112	10.25.32.2/30	Port-channel 1.1112

Table 20 Sub port-channel information for transit-site border router 1

VRF name	VLAN-ID	IP address	Trunk interface
Default VRF	VLAN 1110	10.6.32.2/30	Port-channel 1.1110
IoT-VRF-101	VLAN 1111	10.21.32.2/30	Port-channel 1.1111
CONT-VRF-102	VLAN 1112	10.25.32.2/30	Port-channel 1.1112

Table 21 Sub port-channel information for transit-site border router 2

VRF name	VLAN-ID	IP address	Trunk interface
Default VRF	VLAN 1110	10.6.32.2/30	Port-channel 1.1110
IoT-VRF-101	VLAN 1111	10.21.32.2/30	Port-channel 1.1111
CONT-VRF-102	VLAN 1112	10.25.32.2/30	Port-channel 1.1112

Step 1: Create the port-channel.

```
interface Port-channel1
 description IWAN-D3750X
 no ip address
 ip nbar protocol-discovery
 ip pim sparse-mode
 no negotiation auto
```

Step 2: Configure the interface members of the port-channel.

```
interface GigabitEthernet0/0/0
 description IWAN-D3750X Gig1/0/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 1

interface GigabitEthernet0/0/1
 description IWAN-D3750X Gig2/0/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 1
```

Step 3: Create and configure the port-channel sub-interfaces.

```
interface Port-channel1.1110
 encapsulation dot1Q 1110
 ip address 10.6.32.2 255.255.255.252
 ip nbar protocol-discovery
 ip pim sparse-mode

interface Port-channel1.1111
 description WAN-D3750X VRF-101
 encapsulation dot1Q 1111
 vrf forwarding IoT-VRF-101
 ip address 10.21.32.2 255.255.255.252
 ip nbar protocol-discovery
```

```
 ip pim sparse-mode

interface Port-channel1.1112
 description WAN-D3750X VRF-102
 encapsulation dot1Q 1112
 vrf forwarding CONT-VRF-102
 ip address 10.25.32.2 255.255.255.252
 ip nbar protocol-discovery
 ip pim sparse-mode
```

Step 4: Using the parameters in the tables above, repeat the previous steps for all border routers.

Procedure 3 Configure IKEv2 and IPsec profiles

To complete the IKEv2 and IPsec configuration for this router, follow the steps in "Configuring IKEv2 and IPsec for a remote site router" in Appendix B.

Procedure 4 Configure the mGRE tunnel

In this procedure, you create mGRE tunnels for DMVPN in each of the new VRFs. This type of tunnel requires a source interface only. Use the same source interface that you used to connect to the default VRF.

In a multi-VRF deployment, all tunnels with the same tunnel source interface must use the same IPsec profile and must have the **tunnel protection shared** command configured. To differentiate tunnels after decryption, a different **tunnel key** is used per VRF.

Table 22 DMVPN tunnel information for hub border routers

Transport name	IPSEC profile	Bandwidth	FVRF	Tunnel source
MPLS1	DMVPN-IPSEC-PROFILE-MPLS1	600000	IWAN-TRANSPORT-1	Gig 0/0/3
INET1	DMVPN-IPSEC-PROFILE-INET1	900000	IWAN-TRANSPORT-2	Gig 0/0/4
MPLS2	DMVPN-IPSEC-PROFILE-MPLS2	500000	IWAN-TRANSPORT-3	Gig 0/0/3
INET2	DMVPN-IPSEC-PROFILE-INET2	1000000	IWAN-TRANSPORT-4	Gig 0/0/4
INET4G	DMVPN-IPSEC-PROFILE-INET4G	400000	IWAN-TRANSPORT-5	Gig 0/0/5

Step 1: Create mGRE tunnels for each VRF on border router DHY-M1I1-ASR1002X-1.

Table 23 Tunnel information for border router DHY-M1I1-ASR1002X-1 (MPLS1)

VRF name	Tunnel ID	IP address	NHRP network-ID/ Tunnel-key
Default VRF	100	10.6.34.1/23	1100
IoT-VRF-101	101	10.21.34.1/23	1101
CONT-VRF-102	102	10.25.34.1/23	1102

Table 24 Tunnel information for border router DHY-M1I1-ASR1002X-1 (INET1)

VRF name	Tunnel ID	IP address	NHRP network-ID/ Tunnel-key
Default VRF	200	10.6.36.1/23	1200
IoT-VRF-101	201	10.21.36.1/23	1201
CONT-VRF-102	202	10.25.36.1/23	1202

Example: DHY-M1I1-ASR1002X-1

```
interface Tunnel101
 description IoT-VRF-101 tunnel via MPLS
 bandwidth 600000
 vrf forwarding IoT-VRF-101
 ip address 10.21.34.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp network-id 1101
 ip nhrp server-only
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/3
 tunnel mode gre multipoint
 tunnel key 1101
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-MPLS1 shared
 hold-queue 4096 in
 hold-queue 4096 out
```

```
interface Tunnel102
 description CONT-VRF-102 tunnel via MPLS1
 bandwidth 600000
 vrf forwarding CONT-VRF-102
 ip address 10.25.34.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-mode
 ip nhrp authentication cisco123
 ip nhrp network-id 1102
 ip nhrp server-only
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/3
 tunnel mode gre multipoint
 tunnel key 1102
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-MPLS1 shared
 hold-queue 4096 in
 hold-queue 4096 out
```

Step 2: Using the parameters in the tables below, create mGRE tunnels for border router DHY-M2I2-AS-R1002X-2.

Table 25 *Tunnel information for border router DHY-M2I2I3-ASR1002X-2 (MPLS2)*

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	300	10.6.38.1/23	1300
IoT-VRF-101	301	10.21.38.1/23	1301
CONT-VRF-102	302	10.25.38.1/23	1302

Table 26 *Tunnel information for border router DHY-M2I2I3-ASR1002X-2 (INET2)*

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	400	10.6.40.1/23	1400
IoT-VRF-101	401	10.21.40.1/23	1401
CONT-VRF-102	402	10.25.40.1/23	1402

Table 27 Tunnel information for border router DHY-M2I2I3-ASR1002X-2 (INET4G)

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	500	10.6.44.1/23	1500
IoT-VRF-101	501	10.21.44.1/23	1501
CONT-VRF-102	502	10.25.44.1/23	1502

Step 3: Using the parameters in the tables below, create mGRE tunnels for border router DHY-M1I1-ASR1002X-T1.

Table 28 Tunnel information for border router DHY-M1I1-ASR1002X-T1 (INET1)

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	200	10.6.36.2/23	1200
IoT-VRF-101	201	10.21.36.2/23	1201
CONT-VRF-102	202	10.25.36.2/23	1202

Table 29 Tunnel information for border router DHY-M1I1-ASR1002X-T1 (INET1)

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	200	10.6.36.2/23	1200
IoT-VRF-101	201	10.21.36.2/23	1201
CONT-VRF-102	202	10.25.36.2/23	1202

Step 4: Using the parameters in the tables below, create mGRE tunnels for border router DHY-M2I2I3-AS-R1002X-T2.

Table 30 Tunnel information for border router DHY-M2I2I3-ASR1002X-T2 (MPLS2)

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	300	10.6.38.2/23	1300
IoT-VRF-101	301	10.21.38.2/23	1301
CONT-VRF-102	302	10.25.38.2/23	1302

Table 31 Tunnel information for border router DHY-M2I2I3-ASR1002X-T2 (INET2)

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	400	10.6.40.2/23	1400
IoT-VRF-101	401	10.21.40.2/23	1401
CONT-VRF-102	402	10.25.40.2/23	1402

Table 32 Tunnel information for border router DHY-M2I2I3-ASR1002X-T2 (INET4G)

Multi VRF	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	500	10.6.44.2/23	1500
IoT-VRF-101	501	10.21.44.2/23	1501
CONT-VRF-102	502	10.25.44.2/23	1502

Procedure 5 Configure the routing protocol for OSPF

Use the parameters from the tables below to configure OSPF on the hub border routers.

Table 33 OSPF information for hub-site border router DHY-M1I1-ASR1002X-1

OSPF process-ID	VRF name	Router-ID	LAN interface	LAN IP network/ subnet mask
100	Default VRF	10.6.32.241	Port-channel 1.1110	10.6.0.0/15
101	IoT-VRF-101	10.21.32.241	Port-channel 1.1111	10.20.0.0/15
102	CONT-VRF-102	10.25.32.241	Port-channel 1.1112	10.24.0.0/15

Table 34 OSPF information for hub-site border router DHY-M2I2I3-ASR1002X-2

OSPF process-ID	VRF name	Router-ID	LAN interface	LAN IP network/ subnet mask
100	Default VRF	10.6.32.242	Port-channel 2.1120	10.6.0.0/15
101	IoT-VRF-101	10.21.32.242	Port-channel 2.1121	10.20.0.0/15
102	CONT-VRF-102	10.25.32.242	Port-channel 2.1122	10.24.0.0/15

Table 35 OSPF information for transit-site border router DHY-M1I1-ASR1002X-T1

OSPF process-ID	VRF name	Router-ID	LAN interface	LAN IP network/ subnet mask
100	Default VRF	10.8.32.241	Port-channel 1.1110	10.6.0.0/15 10.8.0.0/15
101	IoT-VRF-101	10.23.32.241	Port-channel 1.1111	10.23.0.0/16
102	CONT-VRF-102	10.27.32.241	Port-channel 1.1112	10.27.0.0/16

Table 36 OSPF information for transit-site border router DHY-M2I2I3-ASR1002X-T2

OSPF process-ID	VRF name	Router-ID	LAN interface	LAN IP network/ Subnet mask
100	Default VRF	10.8.32.242	Port-channel 2.1120	10.6.0.0/15 10.8.0.0/15
101	IoT-VRF-101	10.23.32.242	Port-channel 2.1121	10.23.0.0/16
102	CONT-VRF-102	10.27.32.242	Port-channel 2.1122	10.27.0.0/16

Step 1: Configure an OSPF routing protocol on the hub border router.

Example: DHY-M1I1-ASR1002X-1

```
router ospf 101 vrf IoT-VRF-101
 router-id 10.21.32.241
 capability vrf-lite
 passive-interface default
 no passive-interface Port-channel1.1111
 network 10.20.0.0 0.1.255.255 area 0

router ospf 102 vrf CONT-VRF-102
 router-id 10.25.32.241
 capability vrf-lite
 passive-interface default
 no passive-interface Port-channel1.1112
 network 10.24.0.0 0.1.255.255 area 0
```

Step 2: Using the parameters in the tables above, repeat the previous step for all border routers.

Procedure 6 Configure the routing protocol for BGP

Use the parameters from the table below to configure BGP on the hub border routers.

Table 37 BGP routing information for border router DHY-M1I1-ASR1002X-1

VRF name	Router-ID	Peer-group	Tunnel-subnet	Tunnel ID	LAN IP network/ subnet mask
Default VRF	10.6.32.241	-	-	-	0.0.0.0 10.0.0.0 10.4.0.0/14 10.6.0.0/16 10.6.32.251/32
		MPLS1-SPOKES	10.6.34.0/23	100	-
		INET1-SPOKES	10.6.36.0/23	200	-
IoT-VRF-101	10.21.32.241	-	-	-	0.0.0.0 10.20.0.0/15 10.21.0.0/16 10.21.32.251/32
		MPLS1-SPOKES-VRF101	10.21.34.0/23	101	-
		INET1-SPOKES-VRF101	10.21.36.0/23	201	-
CONT-VRF-102	10.25.32.241	-	-	-	0.0.0.0 10.24.0.0/15 10.25.0.0/16 10.25.32.251/32
		MPLS1-SPOKES-VRF102	10.25.34.0/23	102	-
		INET1-SPOKES-VRF102	10.25.36.0/23	202	-

Step 1: Configure BGP routing protocol for IoT-VRF-101.

Example: DHY-M1I1-ASR1002X-1

```
router bgp 65100
 bgp listen range 10.21.34.0/23 peer-group MPLS1-SPOKES-VRF101

 address-family ipv4 vrf IoT-VRF-101
  bgp router-id 10.21.32.241
  network 0.0.0.0
  network 10.20.0.0 mask 255.254.0.0
  network 10.21.0.0 mask 255.255.0.0
  network 10.21.32.251 mask 255.255.255.255
  neighbor MPLS1-SPOKES-VRF101 peer-group
  neighbor MPLS1-SPOKES-VRF101 remote-as 65100
  neighbor MPLS1-SPOKES-VRF101 description MPLS1 Route Reflector
  neighbor MPLS1-SPOKES-VRF101 update-source Tunnel101
  neighbor MPLS1-SPOKES-VRF101 timers 20 60
  neighbor MPLS1-SPOKES-VRF101 send-community
  neighbor MPLS1-SPOKES-VRF101 route-reflector-client
  neighbor MPLS1-SPOKES-VRF101 next-hop-self all
  neighbor MPLS1-SPOKES-VRF101 weight 50000
  neighbor MPLS1-SPOKES-VRF101 soft-reconfiguration inbound
  maximum-secondary-paths ibgp 1
  distance bgp 201 19 200
 exit-address-family
```

Step 2: Repeat the previous step for each peer-group in IoT-VRF-101.

Step 3: Configure BGP routing protocol for VRF CONT-VRF-102.

Example: DHY-M1I1-ASR1002X-1

```
router bgp 65100
 bgp listen range 10.25.34.0/23 peer-group MPLS1-SPOKES-VRF102

 address-family ipv4 vrf CONT-VRF-102
  bgp router-id 10.25.32.241
  network 0.0.0.0
  network 10.24.0.0 mask 255.254.0.0
  network 10.25.0.0 mask 255.255.0.0
  network 10.25.32.251 mask 255.255.255.255
  neighbor MPLS1-SPOKES-VRF102 peer-group
  neighbor MPLS1-SPOKES-VRF102 remote-as 65100
  neighbor MPLS1-SPOKES-VRF102 description MPLS1 Route Reflector
  neighbor MPLS1-SPOKES-VRF102 update-source Tunnel102
  neighbor MPLS1-SPOKES-VRF102 timers 20 60
  neighbor MPLS1-SPOKES-VRF102 send-community
  neighbor MPLS1-SPOKES-VRF102 route-reflector-client
  neighbor MPLS1-SPOKES-VRF102 next-hop-self all
  neighbor MPLS1-SPOKES-VRF102 weight 50000
  neighbor MPLS1-SPOKES-VRF102 soft-reconfiguration inbound
  maximum-secondary-paths ibgp 1
  distance bgp 201 19 200
 exit-address-family
```

Step 4: Repeat the previous step for each Peer-Groups in CONT-VRF-102.

Step 5: Using the parameters in the tables below, repeat the previous steps to configure the BGP routing protocol for the other border routers.

Table 38 BGP routing information for border router DHY-M2I2I3-ASR1002X-2

VRF name	Router-ID	Peer-group	Tunnel-subnet	Tunnel ID	LAN IP network/ subnet mask
Default VRF	10.6.32.242	-	-	-	0.0.0.0 10.0.0.0 10.4.0.0/14 10.6.0.0/16 10.6.32.251/32
		MPLS2-SPOKES	10.6.38.0/23	300	-
		INET2-SPOKES	10.6.40.0/23	400	-
		INET4G-SPOKES	10.6.44.0/23	500	-
IoT-VRF-101	10.21.32.242	-	-	-	0.0.0.0 10.20.0.0/15 10.21.0.0/16 10.21.32.251/32
		MPLS2-SPOKES-VRF101	10.21.38.0/23	301	-
		INET2-SPOKES-VRF101	10.21.40.0/23	401	-
		INET4G-SPOKES-VRF101	10.21.44.0/23	501	-
CONT-VRF-102	10.25.32.242	-	-	-	0.0.0.0 10.24.0.0/15 10.25.0.0/16 10.25.32.251/32
		MPLS2-SPOKES-VRF102	10.25.38.0/23	302	-
		INET2-SPOKES-VRF102	10.25.40.0/23	402	-
		INET4G-SPOKES-VRF102	10.25.44.0/23	502	-

Table 39 BGP routing information for border router DHY-M1I1-ASR1002X-T1

VRF name	Router-ID	Peer-group	Tunnel-subnet	Tunnel ID	LAN IP network/ subnet mask
Default VRF	10.8.32.241	-	-	-	0.0.0.0 10.0.0.0 10.4.0.0/14 10.8.0.0/16 10.8.32.251/32
		MPLS1-SPOKES	10.6.34.0/23	100	-
		INET1-SPOKES	10.6.36.0/23	200	-
IoT-VRF-101	10.23.32.241	-	-	-	0.0.0.0 10.23.0.0/16 10.23.32.251/32
		MPLS1-SPOKES-VRF101	10.21.34.0/23	101	-
		INET1-SPOKES-VRF101	10.21.36.0/23	201	-
CONT-VRF-102	10.27.32.241	-	-	-	0.0.0.0 10.27.0.0/16 10.27.32.251/32
		MPLS1-SPOKES-VRF102	10.25.34.0/23	102	-
		INET1-SPOKES-VRF102	10.25.36.0/23	202	-

Table 40 BGP routing information for border router DHY-M2I2I3-ASR1002X-T2

VRF name	Router-ID	Peer-group	Tunnel-subnet	Tunnel ID	LAN IP network/ subnet mask
Default VRF	10.8.32.242	-	-	-	0.0.0.0 10.0.0.0 10.4.0.0/14 10.8.0.0/16 10.8.32.251/32
		MPLS2-SPOKES	10.6.38.0/23	300	-
		INET2-SPOKES	10.6.40.0/23	400	-
		INET4G-SPOKES	10.6.44.0/23	500	-
IoT-VRF-101	10.23.32.242	-	-	-	0.0.0.0 10.23.0.0/16 10.23.32.251/32
		MPLS2-SPOKES-VRF101	10.21.38.0/23	301	-
		INET2-SPOKES-VRF101	10.21.40.0/23	401	-
		INET4G-SPOKES-VRF101	10.21.44.0/23	501	-
CONT-VRF-102	10.27.32.242	-	-	-	0.0.0.0 10.23.0.0/16 10.27.32.251/32
		MPLS2-SPOKES-VRF102	10.25.38.0/23	302	-
		INET2-SPOKES-VRF102	10.25.40.0/23	402	-
		INET4G-SPOKES-VRF102	10.25.44.0/23	502	-

Procedure 7 Configure the prefix-lists for OSPF and BGP

Step 1: Create the default route and site-specific prefix-lists for all border routers.

```
ip prefix-list DEFAULT-ROUTE-101 seq 10 permit 0.0.0.0/0
ip prefix-list DEFAULT-ROUTE-102 seq 10 permit 0.0.0.0/0
ip prefix-list ENTERPRISE-PREFIX-101 seq 10 permit 10.4.0.0/14
ip prefix-list ENTERPRISE-PREFIX-102 seq 10 permit 10.4.0.0/14
```

Step 2: Using the parameters in the tables below, create the local DC prefix-list for the border routers.

Table 41 Local DC prefix-list for border router DHY-M1I1-ASR1002X-1

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALDC-PREFIX	10.6.0.0/16
IoT-VRF-102	LOCALDC-PREFIX-101	10.21.0.0/16
CONT-VRF-102	LOCALDC-PREFIX-102	10.25.0.0/16

Example: DHY-M1I1-ASR1002X-1

```
ip prefix-list LOCALDC-PREFIX-101 seq 20 permit 10.21.0.0/16
ip prefix-list LOCALDC-PREFIX-102 seq 20 permit 10.25.0.0/16
```

Table 42 Local DC prefix-list for border router DHY-M2I2I3-ASR1002X-2

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALDC-PREFIX	10.8.0.0/16
IoT-VRF-102	LOCALDC-PREFIX-101	10.23.0.0/16
CONT-VRF-102	LOCALDC-PREFIX-102	10.27.0.0/16

Table 43 Local DC prefix-list for border router DHY-M1I1-ASR1002X-T1

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALDC-PREFIX	10.6.0.0/16
IoT-VRF-102	LOCALDC-PREFIX-101	10.21.0.0/16
CONT-VRF-102	LOCALDC-PREFIX-102	10.25.0.0/16

Table 44 Local DC prefix-list for border router DHY-M2I2I3-ASR1002X-T2

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALDC-PREFIX	10.8.0.0/16
IoT-VRF-102	LOCALDC-PREFIX-101	10.23.0.0/16
CONT-VRF-102	LOCALDC-PREFIX-102	10.27.0.0/16

Step 3: Using the parameters in the tables below, create the local MC loopback prefix-list for the border routers.

Table 45 Local MC loopback prefix-list for border router DHY-M1I1-ASR1002X-1

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALMCLOOPBACK	10.6.32.251/32
IoT-VRF-102	LOCALMCLOOPBACK-101	10.21.32.251/32
CONT-VRF-102	LOCALMCLOOPBACK-102	10.25.32.251/32

Example: DHY-M1I1-ASR1002X-1

```
ip prefix-list LOCALMCLOOPBACK-101 seq 10 permit 10.21.32.251/32
ip prefix-list LOCALMCLOOPBACK-102 seq 10 permit 10.25.32.251/32
```

Table 46 Local MC loopback prefix-list for border router DHY-M2I2I3-ASR1002X-2

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALMCLOOPBACK	10.8.32.251/32
IoT-VRF-102	LOCALMCLOOPBACK-101	10.23.32.251/32
CONT-VRF-102	LOCALMCLOOPBACK-102	10.27.32.251/32

Table 47 Local MC loopback prefix-list for border router DHY-M1I1-ASR1002X-T1

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALMCLOOPBACK	10.6.32.251/32
IoT-VRF-102	LOCALMCLOOPBACK-101	10.21.32.251/32
CONT-VRF-102	LOCALMCLOOPBACK-102	10.25.32.251/32

Table 48 Local MC loopback prefix-list for border router DHY-M2I2I3-ASR1002X-T2

VRF name	Prefix-list	IP-subnet
Default VRF	LOCALMCLOOPBACK	10.8.32.251/32
IoT-VRF-102	LOCALMCLOOPBACK-101	10.23.32.251/32
CONT-VRF-102	LOCALMCLOOPBACK-102	10.27.32.251/32

Step 4: Create the TUNNEL-DMVPN prefix-list on all border routers.

```
ip prefix-list TUNNEL-DMVPN-101 seq 10 permit 10.21.34.0/23
ip prefix-list TUNNEL-DMVPN-101 seq 20 permit 10.21.36.0/23
ip prefix-list TUNNEL-DMVPN-101 seq 30 permit 10.21.38.0/23
ip prefix-list TUNNEL-DMVPN-101 seq 40 permit 10.21.40.0/23
ip prefix-list TUNNEL-DMVPN-101 seq 50 permit 10.21.44.0/23

ip prefix-list TUNNEL-DMVPN-102 seq 10 permit 10.25.34.0/23
ip prefix-list TUNNEL-DMVPN-102 seq 20 permit 10.25.36.0/23
ip prefix-list TUNNEL-DMVPN-102 seq 30 permit 10.25.38.0/23
ip prefix-list TUNNEL-DMVPN-102 seq 40 permit 10.25.40.0/23
ip prefix-list TUNNEL-DMVPN-102 seq 50 permit 10.25.44.0/23
```

Procedure 8 Configure the prefix route maps for OSPF and BGP

Table 49 Prefix list information for all hub border routers

Prefix list name	Prefix list value
Prefix list default VRF (IN)	DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LOCALMCLOOPBACK TUNNEL-DMVPN
Prefix list default VRF (OUT)	DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LOCALMCLOOPBACK
Prefix list IoT-VRF-101 (IN)	DEFAULT-ROUTE-101 ENTERPRISE-PREFIX-101 LOCALDC-PREFIX-101 LOCALMCLOOPBACK-101 TUNNEL-DMVPN-101
Prefix list IoT-VRF-101 (OUT)	DEFAULT-ROUTE-101 ENTERPRISE-PREFIX-101 LOCALDC-PREFIX-101 LOCALMCLOOPBACK-101
Prefix list CONT-VRF-102 (IN)	DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PREFIX-102 LOCALMCLOOPBACK-102 TUNNEL-DMVPN-102
Prefix list CONT-VRF-102 (OUT)	DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PREFIX-102 LOCALMCLOOPBACK-102

Step 1: Using the parameters in the tables, create and apply the prefix route-map for BGP on border router DHY-M1I1-ASR1002X-1.

Table 50 Route-map information for border router DHY-M1I1-ASR1002X-1

WAN transport name	Local-preference-value	Community-value
MPLS1	800	65100:100
INET1	780	65100:200

Table 51 Prefix list information for border router DHY-M1I1-ASR1002X-1

Route-map	IN	OUT
Default VRF (MPLS1)	MPLS1-IN	MPLS1-OUT
IoT-VRF-101 (MPLS1)	MPLS1-VRF101-IN	MPLS1-VRF101-OUT
CONT-VRF-102 (MPLS1)	MPLS1-VRF102-IN	MPLS1-VRF102-OUT
Default VRF (INET1)	INET1-IN	INET1-OUT
IoT-VRF-101 (INET1)	INET1-VRF101-IN	INET1-VRF101-OUT
CONT-VRF-102 (INET1)	INET1-VRF102-IN	INET1-VRF102-OUT

Example: DHY-M1I1-ASR1002X-1

```
ip bgp-community new-format

route-map MPLS1-VRF101-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE-101 ENTERPRISE-PREFIX-101 LOCALDC-PREFIX-101 LOCALMCLOOPBACK-101 TUNNEL-DMVPN-101

route-map MPLS1-VRF101-IN permit 1000
 description Allow Everything Else

route-map MPLS1-VRF101-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
 match ip address prefix-list DEFAULT-ROUTE-101 LOCALDC-PREFIX-101 ENTERPRISE-PREFIX-101 LOCALMCLOOPBACK-101
 set local-preference 800
 set community 65100:100

route-map INET1-VRF101-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE-101 LOCALDC-PREFIX-101 LOCALMCLOOP-BACK-101 TUNNEL-DMVPN-101

route-map INET1-VRF101-IN permit 1000
 description Allow Everything Else

route-map INET1-VRF101-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
```

```
 match ip address prefix-list DEFAULT-ROUTE-101 LOCALDC-PREFIX-101 ENTERPRISE-PREFIX-101 LOCALMCLOOPBACK-101
 set local-preference 780
 set community 65100:200

route-map MPLS1-VRF102-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PREFIX-102 LOCALMCLOOPBACK-102 TUNNEL-DMVPN-102

route-map MPLS1-VRF102-IN permit 1000
 description Allow Everything Else

route-map MPLS1-VRF102-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
 match ip address prefix-list DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PREFIX-102 LOCALMCLOOPBACK-102
 set local-preference 800
 set community 65100:100

route-map INET1-VRF102-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PREFIX-102 LOCALMCLOOPBACK-102 TUNNEL-DMVPN-102

route-map INET1-VRF102-IN permit 1000
 description Allow Everything Else

route-map INET1-VRF102-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
 match ip address prefix-list DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PREFIX-102 LOCALMCLOOPBACK-102
 set local-preference 780
 set community 65100:200

router bgp 65100
address-family ipv4 vrf IoT-VRF-101
```

```
 neighbor INET1-SPOKES-VRF101 route-map INET1-VRF101-IN in
 neighbor INET1-SPOKES-VRF101 route-map INET1-VRF101-OUT out
 neighbor MPLS1-SPOKES-VRF101 route-map MPLS1-VRF101-IN in
 neighbor MPLS1-SPOKES-VRF101 route-map MPLS1-VRF101-OUT out

address-family ipv4 vrf CONT-VRF-102
 neighbor INET1-SPOKES-VRF102 route-map INET1-VRF102-IN in
 neighbor INET1-SPOKES-VRF102 route-map INET1-VRF102-OUT out
 neighbor MPLS1-SPOKES-VRF102 route-map MPLS1-VRF102-IN in
 neighbor MPLS1-SPOKES-VRF102 route-map MPLS1-VRF102-OUT out
```

Step 2: Using the parameters in the tables, repeat the previous step for border router DHY-M2I2I3-ASR1002X-2.

Table 52 Route-map information for border router DHY-M2I2I3-ASR1002X-2

WAN transport name	Local-preference-value	Community-value
MPLS2	790	65100:300
INET2	770	65100:400
INET4G	760	65100:500

Table 53 Prefix List information for border router DHY-M2I2I3-ASR1002X-2

Route-map	IN	OUT
Default VRF (MPLS2)	MPLS2-IN	MPLS2-OUT
IoT-VRF-101 (MPLS2)	MPLS2-VRF101-IN	MPLS2-VRF101-OUT
CONT-VRF-102 (MPLS2)	MPLS2-VRF102-IN	MPLS2-VRF102-OUT
Default VRF (INET2)	INET2-IN	INET2-OUT
IoT-VRF-101 (INET2)	INET2-VRF101-IN	INET2-VRF101-OUT
CONT-VRF-102 (INET2)	INET2-VRF102-IN	INET2-VRF102-OUT
Default VRF (INET4G)	INET4G-IN	INET4G-OUT
IoT-VRF-101 (INET4G)	INET4G-VRF101-IN	INET4G-VRF101-OUT
CONT-VRF-102 (INET4G)	INET4G-VRF102-IN	INET4G-VRF102-OUT

Step 3: Using the parameters in the tables, repeat the previous step for border router DHY-M1I1-ASR1002X-T1.

Table 54 Route-map information for border routers DHY-M1I1-ASR1002X-T1

WAN transport name	Local-preference-value	Community-value
MPLS1	600	65100:101
INET1	580	65100:201

Table 55 Prefix list information for border router DHY-M1I1-ASR1002X-T1

Route-map	IN	OUT
Default VRF (MPLS1)	MPLS1-IN	MPLS1-OUT
IoT-VRF-101 (MPLS1)	MPLS1-VRF101-IN	MPLS1-VRF101-OUT
CONT-VRF-102 (MPLS1)	MPLS1-VRF102-IN	MPLS1-VRF102-OUT
Default VRF (INET1)	INET1-IN	INET1-OUT
IoT-VRF-101 (INET1)	INET1-VRF101-IN	INET1-VRF101-OUT
CONT-VRF-102 (INET1)	INET1-VRF102-IN	INET1-VRF102-OUT

Step 4: Using the parameters in the tables, repeat the previous step for border router DHY-M2I2I3-ASR1002X-T2.

Table 56 Route-map information for border router DHY-M2I2I3-ASR1002X-T2

WAN transport name	Local-preference-value	Community-value
MPLS2	590	65100:301
INET2	570	65100:401
INET4G	560	65100:501

Table 57 Prefix list information for border router DHY-M2I2I3-ASR1002X-T2

Route-map	IN	OUT
Default VRF (MPLS2)	MPLS2-IN	MPLS2-OUT
IoT-VRF-101 (MPLS2)	MPLS2-VRF101-IN	MPLS2-VRF101-OUT
CONT-VRF-102 (MPLS2)	MPLS2-VRF102-IN	MPLS2-VRF102-OUT
Default VRF (INET2)	INET2-IN	INET2-OUT
IoT-VRF-101 (INET2)	INET2-VRF101-IN	INET2-VRF101-OUT
CONT-VRF-102 (INET2)	INET2-VRF102-IN	INET2-VRF102-OUT
Default VRF (INET4G)	INET4G-IN	INET4G-OUT
IoT-VRF-101 (INET4G)	INET4G-VRF101-IN	INET4G-VRF101-OUT
CONT-VRF-102 (INET4G)	INET4G-VRF102-IN	INET4G-VRF102-OUT

Step 5: Using the parameters in the table below, create and apply the prefix route-map for OSPF on hub-site border router DHY-M1I1-ASR1002X-1.

Table 58 OSPF route map information for both hub-site border routers

Field name	Field value
Route map default VRF	REDIST-BGP-TO-OSPF
Prefix list default VRF	DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX
Route map IoT-VRF-101	REDIST-BGP-TO-OSPF-101
Prefix list IoT-VRF-101	DEFAULT-ROUTE-101 ENTERPRISE-PREFIX-101 LOCALDC-PREFIX-101
Route map CONT-VRF-102	REDIST-BGP-TO-OSPF-102
Prefix list CONT-VRF-102	DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PRE-FIX-102
Community name	POP2-SPOKES
Metric-value-1	2000
Metric-value-2	1000
Description-1	POP2
Description-2	POP1

Example: DHY-M1I1-ASR1002X-1

```
route-map REDIST-BGP-TO-OSPF-101 permit 10
 description Secondary POP2 with higher Metric
 match community POP2-SPOKES
 set metric 2000
 set metric-type type-1
 set tag 0

route-map REDIST-BGP-TO-OSPF-101 deny 20
 description Block Null routes to be distributed from BGP to OSPF
 match ip address prefix-list DEFAULT-ROUTE-101 ENTERPRISE-PREFIX-101 LOCALDC-
PREFIX-101

route-map REDIST-BGP-TO-OSPF-101 permit 1000
 description Prefer POP1 with lower Metric
 set metric 1000
 set metric-type type-1
 set tag 0

route-map REDIST-BGP-TO-OSPF-102 permit 10
```

```
 description Secondary POP2 with higher Metric
 match community POP2-SPOKES
 set metric 2000
 set metric-type type-1
 set tag 0

route-map REDIST-BGP-TO-OSPF-102 deny 20
 description Block Null routes to be distributed from BGP to OSPF
 match ip address prefix-list DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-
PREFIX-102

route-map REDIST-BGP-TO-OSPF-102 permit 1000
 description Prefer POP1 with lower Metric
 set metric 1000
 set metric-type type-1
 set tag 0

router ospf 100
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF

router ospf 101 vrf IoT-VRF-101
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF-101

router ospf 102 vrf CONT-VRF-102
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF-102
```

Step 6: Repeat the previous step for hub-site border router DHY-M2I2I3-ASR1002X-2.

Step 7: Using the parameters in the table below, repeat the previous step for transit-site border router DHY-M1I1-ASR1002X-T1.

Table 59 OSPF route map information for both transit-site border routers

Field name	Field value
Route map default VRF	REDIST-BGP-TO-OSPF
Prefix list default VRF	DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX
Route map IoT-VRF-101	REDIST-BGP-TO-OSPF-101
Prefix list IoT-VRF-101	DEFAULT-ROUTE-101 ENTERPRISE-PREFIX-101 LOCALDC-PREFIX-101
Route map CONT-VRF-102	REDIST-BGP-TO-OSPF-102
Prefix list CONT-VRF-102	DEFAULT-ROUTE-102 ENTERPRISE-PREFIX-102 LOCALDC-PRE-FIX-102
Community name	POP1-SPOKES
Metric-value-1	2100
Metric-value-2	1100
Description-1	POP1
Description-2	POP2

Step 8: Repeat the previous step for transit-site border router DHY-M2I2I3-ASR1002X-T2.

Procedure 9 Configure the static null routes and EOT

Step 1: Configure the static null routes and EOT for both hub-site border routers.

```
track 11 ip route 10.21.32.240 255.255.255.255 reachability
 ip vrf IoT-VRF-101

track 21 ip route 10.25.32.240 255.255.255.255 reachability
 ip vrf CONT-VRF-102

ip route vrf IoT-VRF-101 10.20.0.0 255.252.0.0 Null0 254 track 11
ip route vrf CONT-VRF-102 10.24.0.0 255.252.0.0 Null0 254 track 21
```

Step 2: Configure the static null routes and EOT for both transit-site border routers.

```
track 11 ip route 10.23.32.240 255.255.255.255 reachability
 ip vrf IoT-VRF-101

track 21 ip route 10.27.32.240 255.255.255.255 reachability
 ip vrf CONT-VRF-102

ip route vrf IoT-VRF-101 10.23.0.0 255.252.0.0 Null0 254 track 11
ip route vrf CONT-VRF-102 10.27.0.0 255.252.0.0 Null0 254 track 21
```

PROCESS

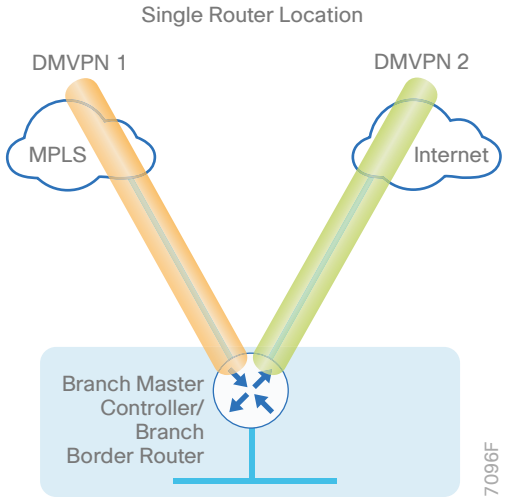
Configuring the Remote-Site DMVPN Router

1. Configure the IVRF definitions and loopbacks
2. Configure the connections to the access switch
3. Configure IKEv2 and IPsec profiles
4. Configure the mGRE tunnel
5. Configure the routing protocol for OSPF
6. Configure the routing protocol for BGP
7. Configure the prefix-lists for OSPF and BGP
8. Create and apply the prefix route maps for OSPF and BGP
9. Create the static null routes for non-default VRFs

Use this process to connect remote site router to the WAN transports.

The following diagram shows the physical connection between the remote site border-router and the MPLS and Internet transports.

Figure 8 *Physical view of single router at remote-site location*



The following diagram shows the logical view of the multi-VRF traffic between the remote site border-router and the tunnels over MPLS and Internet transports.

Figure 9 *Multi VRF view of single router at remote-site location*

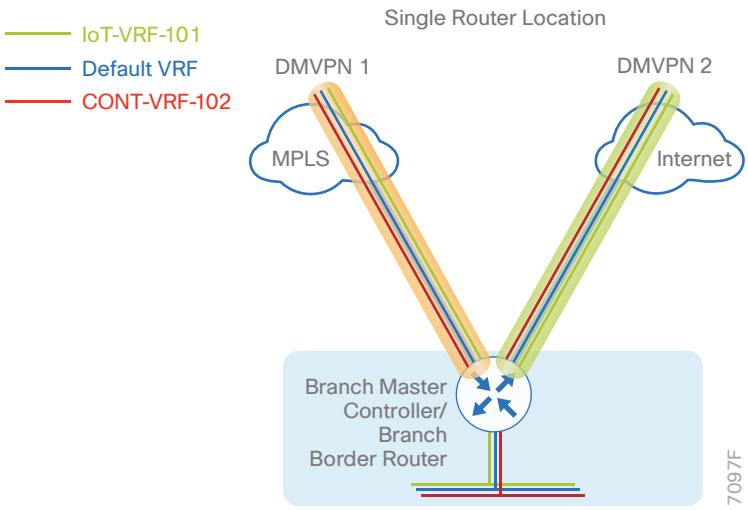


Table 60 VRFs and loopback interfaces for remote-site router (RS11-2921)

VRF name	Loopback interface	IP address	OSPF process-id
Default VRF	Loopback 0	10.255.241.11/32	100
IoT-VRF-101	Loopback 101	10.201.241.11/32	101
CONT-VRF-102	Loopback 102	10.202.241.11/32	102

Reader Tip

Whenever IWAN is designed with WAAS leveraging AppNav/WCCP, please ensure that the Loopback IP address that is being used for PfR is not also used as the AppNav Service Controller address or WCCP router ID. This is applicable for any Branch IWAN router that is part of an AppNav/WCCP Cluster.

Procedure 1 Configure the IVRF definitions and loopbacks

In this procedure, you configure the IVRF definition and their associated loopback interfaces for the remote-site border routers.

Step 1: Configure the two IVRF definitions.

```
vrf definition IoT-VRF-101
 rd 101:1

 address-family ipv4
 exit-address-family

vrf definition CONT-VRF-102
 rd 102:1

 address-family ipv4
 exit-address-family
```

Step 2: Configure the loopback interfaces.

Example: RS11-2921

```
interface Loopback101
 description IoT-VRF-101
 vrf forwarding IoT-VRF-101
 ip address 10.201.241.11 255.255.255.255
 ip pim sparse-mode
 hold-queue 1024 in
 hold-queue 1024 out

interface Loopback102
 description CONT-VRF-102
 vrf forwarding CONT-VRF-102
 ip address 10.202.241.11 255.255.255.255
 ip pim sparse-mode
 hold-queue 1024 in
 hold-queue 1024 out
```

Procedure 2 Configure the connections to the access switch

In this procedure, you configure the router with connectivity to the access layer switch. In the access layer design, the remote sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer.

Step 1: Create VLANs for data and voice traffic for the all VRFs.

```
vlan 521
 name IoT-VRF-101 Data
vlan 522
 name CONT-VRF-102 Data
vlan 531
 name IoT-VRF-101 Voice
vlan 532
 name CONT-VRF-102 Voice
```

Step 2: Configure the trunk on the access layer switch.

Use an 802.1Q trunk for the connection, which allows the router to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are pruned to only the VLANs that are active on the access switch. DHCP snooping and ARP inspection are set to *trust*.

```
interface GigabitEthernet1/0/48
 description RS11-2921 Gig0/2
 switchport trunk allowed vlan 521-522,531-532
 switchport mode trunk
 ip arp inspection trust
 spanning-tree portfast trunk
 logging event link-status
 logging event trunk-status
 ip dhcp snooping trust
 load-interval 30
 no shutdown
```

The Cisco Catalyst 3750 Series Switch requires the **switchport trunk encapsulation dot1q** command.

Step 3: Configure the new IP settings for each subinterface.

This design uses an IP addressing convention with the default gateway router assigned an IP address and IP mask combination of **N.N.N.1 255.255.255.0** where *N.N.N* is the IP network and *1* is the IP host.

When you are using a centralized DHCP server, your routers with LAN interfaces connected to a LAN using DHCP for end-station IP addressing must use an IP helper.

Example: RS11-2911

```
interface GigabitEthernet0/2.521
 description IoT-VRF-101 Data
 encapsulation dot1Q 521
 vrf forwarding IoT-VRF-101
 ip address 10.22.2.1 255.255.255.0
 ip helper-address global 10.4.48.10
 ip pim sparse-mode

interface GigabitEthernet0/2.522
 description CONT-VRF-102 Data
 encapsulation dot1Q 522
 vrf forwarding CONT-VRF-102
 ip address 10.26.2.1 255.255.255.0
```

```
 ip helper-address global 10.4.48.10
 ip pim sparse-mode

interface GigabitEthernet0/2.531
 description IoT-VRF-101 Voice
 encapsulation dot1Q 531
 vrf forwarding IoT-VRF-101
 ip address 10.22.3.1 255.255.255.0
 ip helper-address global 10.4.48.10
 ip pim sparse-mode

interface GigabitEthernet0/2.532
 description CONT-VRF-102 Voice
 encapsulation dot1Q 532
 vrf forwarding CONT-VRF-102
 ip address 10.26.3.1 255.255.255.0
 ip helper-address global 10.4.48.10
 ip pim sparse-mode
```

Procedure 3 Configure IKEv2 and IPsec profiles

To complete the IKEv2 and IPsec configuration for this router, follow the steps in "Configuring IKEv2 and IPsec for a remote site router" in Appendix B.

Procedure 4 Configure the mGRE tunnel

In this procedure, you configure mGRE tunnels for DMVPN in each VRF. This type of tunnel requires a source interface only. Use the same source interface that you use to connect to the MPLS or Internet.

In a multi-VRF deployment, all tunnels with the same tunnel source interface must use the same IPsec profile and must have the **tunnel protection shared** command configured. To differentiate tunnels after decryption, a different **tunnel key** is used per VRF.

Table 61 DMVPN tunnel information for remote-site border router

Transport name	IPSEC profile	Bandwidth	FVRF	Tunnel source
MPLS1	DMVPN-IPSEC-PRO-FILE-MPLS1	20000	IWAN-TRANSPORT-1	Gig 0/0
INET1	DMVPN-IPSEC-PRO-FILE-INET1	50000	IWAN-TRANSPORT-2	Gig 0/1

Table 62 Tunnel information for border router RS11-2921 (MPLS1)

VRF name	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	100	10.6.34.11/23	1100
IoT-VRF-101	101	10.21.34.11/23	1101
CONT-VRF-102	102	10.25.34.11/23	1102

Table 63 Tunnel information for border router RS11-2921 (INET1)

VRF name	Tunnel ID	IP address	NHRP network-ID/tunnel-key
Default VRF	200	10.6.36.11/23	1200
IoT-VRF-101	201	10.21.36.11/23	1201
CONT-VRF-102	202	10.25.36.11/23	1202

Example: RS11-2911

```
interface Tunnel101
 description IoT-VRF-101 tunnel via MPLS1
 bandwidth 20000
 vrf forwarding IoT-VRF-101
 ip address 10.21.34.11 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 if-state nhrp
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 1101
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-MPLS1 shared
```

```
interface Tunnel102
 description CONT-VRF-102 tunnel via MPLS1
 bandwidth 20000
 vrf forwarding CONT-VRF-102
 ip address 10.25.34.11 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 if-state nhrp
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 1102
 tunnel vrf IWAN-TRANSPORT-1
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-MPLS1 shared

interface Tunnel201
 description IoT-VRF-101 tunnel via INET1
 bandwidth 50000
 vrf forwarding IoT-VRF-101
 ip address 10.21.36.11 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 1201
 tunnel vrf IWAN-TRANSPORT-2
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-INET1 shared

interface Tunnel202
 description CONT-VRF-102 tunnel via INET1
```

```
bandwidth 50000
vrf forwarding CONT-VRF-102
ip address 10.25.36.11 255.255.254.0
no ip redirects
ip mtu 1400
ip pim dr-priority 0
ip pim sparse-mode
ip tcp adjust-mss 1360
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
tunnel key 1202
tunnel vrf IWAN-TRANSPORT-2
tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-INET1 shared
```

Step 1: Configure NHRP on the tunnel interface.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires several additional configuration statements in order to define the NHRP server and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. Spoke routers require the NHRP static multicast mapping.

When hub BRs are added for horizontal scaling or a second DC is added as a transit site, spoke routers require additional NHS statements for each BR in their environment. The configuration details are covered in subsequent sections of this guide.

The value used for the NHS is the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA 5500 appliance. This design uses the values shown in the following tables.

Table 64 DMVPN tunnel NHRP parameters for border router RS11-2921 (MPLS1)

Parameter	Default VRF	IoT-VRF-101	CONT-VRF-102
DMVPN Tunnel ID	100	101	102
DMVPN hub-site BR public address (actual)	192.168.6.1	192.168.6.1	192.168.6.1
DMVPN transit-site BR public address (actual)	192.168.6.41	192.168.6.41	192.168.6.41
DMVPN hub-site BR public address (externally routable after NAT)	n/a (MPLS1)	n/a (MPLS1)	n/a (MPLS1)
DMVPN transit-site BR public address (externally routable after NAT)	n/a (MPLS1)	n/a (MPLS1)	n/a (MPLS1)
DMVPN hub-site BR tunnel IP address (NHS)	10.6.34.1	10.21.34.1	10.25.34.1
DMVPN transit-site BR tunnel IP address (NHS)	10.6.34.2	10.21.34.2	10.25.34.2
NHRP network ID	1100	1101	1102

Table 65 DMVPN tunnel NHRP parameters for border router RS11-2921 (INET1)

Parameter	Default VRF	IoT-VRF-101	CONT-VRF-102
DMVPN Tunnel ID	200	201	202
DMVPN hub-site BR public address (actual)	192.168.146.10	192.168.146.10	192.168.146.10
DMVPN transit-site BR public address (actual)	192.168.146.13	192.168.146.13	192.168.146.13
DMVPN hub-site BR public address (externally routable after NAT)	172.16.140.1	172.16.140.1	172.16.140.1
DMVPN transit-site BR public address (externally routable after NAT)	172.16.140.2	172.16.140.2	172.16.140.2
DMVPN hub-site BR tunnel IP address (NHS)	10.6.36.1	10.21.36.1	10.25.36.1
DMVPN transit-site BR tunnel IP address (NHS)	10.6.36.2	10.21.36.2	10.25.36.2
NHRP network ID	1200	1201	1202

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, it may appear as a duplicate to an entry already in the cache and be rejected. The **registration no-unique** option allows you to overwrite existing cache entries. This feature is only required on NHRP clients (DMVPN spoke routers). **The if-state nhrp** option ties the tunnel line-protocol state to the reachability of the NHRP NHS, and if the NHS is unreachable, the tunnel line-protocol state changes to down. This feature is used in conjunction with EOT.

Example: RS11-2921

```
interface Tunnel101
 ip nhrp authentication cisco123
 ip nhrp network-id 1101
 ip nhrp holdtime 600
 ip nhrp nhs 10.21.34.1 nbma 192.168.6.1 multicast
 ip nhrp nhs 10.21.34.2 nbma 192.168.6.41 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp

interface Tunnel102
 ip nhrp authentication cisco123
 ip nhrp network-id 1102
 ip nhrp holdtime 600
 ip nhrp nhs 10.25.34.1 nbma 192.168.6.1 multicast
 ip nhrp nhs 10.25.34.2 nbma 192.168.6.41 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp

interface Tunnel201
 ip nhrp authentication cisco123
 ip nhrp network-id 1201
 ip nhrp holdtime 600
 ip nhrp nhs 10.21.36.1 nbma 172.16.140.1 multicast
 ip nhrp nhs 10.21.36.2 nbma 172.16.140.2 multicast
 ip nhrp registration no-unique
```

```
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp

interface Tunnel202
 ip nhrp authentication cisco123
 ip nhrp network-id 1202
 ip nhrp holdtime 600
 ip nhrp nhs 10.25.36.1 nbma 172.16.140.1 multicast
 ip nhrp nhs 10.25.36.2 nbma 172.16.140.2 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp
```

Procedure 5 Configure the routing protocol for OSPF

Table 66 OSPF information for remote-site border router RS11-2921

OSPF process-ID	VRF name	Router-ID	LAN interface	LAN IP network/ Subnet mask
100	Default VRF	10.255.241.11	Gig 0/2.64 Gig 0/2.69	10.7.0.0/21 10.255.241.11/32
101	IoT-VRF-101	10.201.241.11	Gig 0/2.521 Gig 0/2.531	10.22.0.0/21 10.201.241.11/32
102	CONT-VRF-102	10.202.241.11	Gig 0/2.522 Gig 0/2.532	10.26.0.0/21 10.202.241.11/32

Step 1: Configure an OSPF routing protocol on the spoke router for the new VRFs.

Example: RS11-2921

```
router ospf 101 vrf IoT-VRF-101
 router-id 10.201.241.11
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF
 passive-interface default
 no passive-interface GigabitEthernet0/2.521
 no passive-interface GigabitEthernet0/2.531
```

```
 network 10.22.0.0 0.0.7.255 area 0
 network 10.201.241.11 0.0.0.0 area 0
 default-information originate

router ospf 102 vrf CONT-VRF-102
 router-id 10.202.241.11
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF
 passive-interface default
 no passive-interface GigabitEthernet0/2.522
 no passive-interface GigabitEthernet0/2.532
 network 10.26.0.0 0.0.7.255 area 0
 network 10.202.241.11 0.0.0.0 area 0
 default-information originate
```

Procedure 6 Configure the routing protocol for BGP

Table 67 BGP routing information for remote-site border router RS11-2921

VRF name	Router ID	Aggregate-subnet	Peer-group	Hub tunnel address	Tunnel ID
Default VRF	10.255.241.11	10.7.0.0/21	MPLS1-HUB	10.6.34.1 10.6.34.2	100
			INET1-HUB	10.6.36.1 10.6.36.2	200
IoT-VRF-101	10.201.241.11	10.22.0.0/21	MPLS1-HUB-VRF101	10.21.34.1 10.21.34.2	101
			INET1-HUB-VRF101	10.21.36.1 10.21.36.2	201
CONT-VRF-102	10.202.241.11	10.26.0.0/21	MPLS1-HUB-VRF102	10.25.34.1 10.25.34.2	102
			INET1-HUB-VRF102	10.25.36.1 10.25.36.2	202

Step 1: Using the parameters in the table above, configure BGP routing protocol for VRFs IoT-VRF-101 and CONT-VRF-102.

Example: IoT-VRF-101–RS11-2921

```
router bgp 65100
 address-family ipv4 vrf IoT-VRF-101
  bgp router-id 10.201.241.11
  aggregate-address 10.22.0.0 255.255.248.0 summary-only
  redistribute connected
  neighbor INET1-HUB-VRF101 peer-group
  neighbor INET1-HUB-VRF101 remote-as 65100
  neighbor INET1-HUB-VRF101 description To IWAN INET1 Hub Router
  neighbor INET1-HUB-VRF101 update-source Tunnel201
  neighbor INET1-HUB-VRF101 timers 20 60
  neighbor INET1-HUB-VRF101 send-community
  neighbor INET1-HUB-VRF101 next-hop-self all
  neighbor INET1-HUB-VRF101 weight 50000
  neighbor INET1-HUB-VRF101 soft-reconfiguration inbound
  neighbor MPLS1-HUB-VRF101 peer-group
  neighbor MPLS1-HUB-VRF101 remote-as 65100
  neighbor MPLS1-HUB-VRF101 description To IWAN MPLS1 Hub Router
  neighbor MPLS1-HUB-VRF101 update-source Tunnel101
  neighbor MPLS1-HUB-VRF101 timers 20 60
  neighbor MPLS1-HUB-VRF101 send-community
  neighbor MPLS1-HUB-VRF101 next-hop-self all
  neighbor MPLS1-HUB-VRF101 weight 50000
  neighbor MPLS1-HUB-VRF101 soft-reconfiguration inbound
  neighbor 10.21.34.1 peer-group MPLS1-HUB-VRF101
  neighbor 10.21.34.1 activate
  neighbor 10.21.34.2 peer-group MPLS1-HUB-VRF101
  neighbor 10.21.34.2 activate
  neighbor 10.21.36.1 peer-group INET1-HUB-VRF101
  neighbor 10.21.36.1 activate
  neighbor 10.21.36.2 peer-group INET1-HUB-VRF101
  neighbor 10.21.36.2 activate
  maximum-secondary-paths ibgp 3
  distance bgp 201 89 89
 exit-address-family
```

Example: CONT-VRF-102–RS11-2921

```
router bgp 65100
 address-family ipv4 vrf CONT-VRF-102
  bgp router-id 10.202.241.11
  aggregate-address 10.26.0.0 255.255.248.0 summary-only
  redistribute connected
  neighbor INET1-HUB-VRF102 peer-group
  neighbor INET1-HUB-VRF102 remote-as 65100
  neighbor INET1-HUB-VRF102 description To IWAN INET1 Hub Router
  neighbor INET1-HUB-VRF102 update-source Tunnel202
  neighbor INET1-HUB-VRF102 timers 20 60
  neighbor INET1-HUB-VRF102 send-community
  neighbor INET1-HUB-VRF102 next-hop-self all
  neighbor INET1-HUB-VRF102 weight 50000
  neighbor INET1-HUB-VRF102 soft-reconfiguration inbound
  neighbor MPLS1-HUB-VRF102 peer-group
  neighbor MPLS1-HUB-VRF102 remote-as 65100
  neighbor MPLS1-HUB-VRF102 description To IWAN MPLS1 Hub Router
  neighbor MPLS1-HUB-VRF102 update-source Tunnel102
  neighbor MPLS1-HUB-VRF102 timers 20 60
  neighbor MPLS1-HUB-VRF102 send-community
  neighbor MPLS1-HUB-VRF102 next-hop-self all
  neighbor MPLS1-HUB-VRF102 weight 50000
  neighbor MPLS1-HUB-VRF102 soft-reconfiguration inbound
  neighbor 10.25.34.1 peer-group MPLS1-HUB-VRF102
  neighbor 10.25.34.1 activate
  neighbor 10.25.34.2 peer-group MPLS1-HUB-VRF102
  neighbor 10.25.34.2 activate
  neighbor 10.25.36.1 peer-group INET1-HUB-VRF102
  neighbor 10.25.36.1 activate
  neighbor 10.25.36.2 peer-group INET1-HUB-VRF102
  neighbor 10.25.36.2 activate
  maximum-secondary-paths ibgp 3
  distance bgp 201 89 89
 exit-address-family
```

Procedure 7 Configure the prefix-lists for OSPF and BGP

Step 1: Create the local loopback prefix-list for each VRF on remote-site border router.

Table 68 Local loopback prefix-list for remote-site border router RS11-2921

VRF name	Prefix-list	IP-subnet
Default VRF	LOCAL-LOOPBACKS	10.255.241.11/32
IoT-VRF-101	LOCAL-LOOPBACKS-101	10.201.241.11/32
CONT-VRF-102	LOCAL-LOOPBACKS-102	10.202.241.11/32

Table 69 Local subnet prefix-list for remote-site border router RS11-2921

VRF name	Prefix-list	IP-subnet
Default VRF	LOCAL-SUBNETS	10.7.0.0/21
IoT-VRF-101	LOCAL-SUBNETS-101	10.22.0.0/21
CONT-VRF-102	LOCAL-SUBNETS-102	10.26.0.0/21

Example: RS11-2921

```
ip prefix-list LOCAL-LOOPBACKS-101 seq 10 permit 10.201.241.11/32
ip prefix-list LOCAL-LOOPBACKS-102 seq 10 permit 10.202.241.11/32
ip prefix-list LOCAL-SUBNETS-101 seq 10 permit 10.22.0.0/21
ip prefix-list LOCAL-SUBNETS-102 seq 10 permit 10.26.0.0/21
```

Procedure 8 Create and apply the prefix route maps for OSPF and BGP

Step 1: Create the prefix route-map SPOKE-OUT for BGP on remote-site border router.

Table 70 Prefix route-map SPOKE-OUT for RS11-2921

VRF name	Community-value	Prefix-list
Default VRF	65100:20	LOCAL-LOOPBACKS LOCAL-SUBNETS
IoT-VRF-101	65100:20	LOCAL-LOOPBACKS-101 LOCAL-SUBNETS-101
CONT-VRF-102	65100:20	LOCAL-LOOPBACKS-102 LOCAL-SUBNETS-102

```
route-map SPOKE-OUT-VRF101 permit 10
 description Prefer POP2 with community 65100:20
 match ip address prefix-list LOCAL-LOOPBACKS-101 LOCAL-SUBNETS-101
 set community 65100:20

route-map SPOKE-OUT-VRF102 permit 10
 description Prefer POP2 with community 65100:20
 match ip address prefix-list LOCAL-LOOPBACKS-102 LOCAL-SUBNETS-102
 set community 65100:20
```

Step 2: Apply both the prefix route-maps on remote-site border router.

```
router bgp 65100

 address-family ipv4 vrf IoT-VRF-101
  neighbor INET1-HUB-VRF101 route-map POP-SELECT in
  neighbor INET1-HUB-VRF101 route-map SPOKE-OUT-VRF101 out
  neighbor MPLS1-HUB-VRF101 route-map POP-SELECT in
  neighbor MPLS1-HUB-VRF101 route-map SPOKE-OUT-VRF101 out
exit-address-family

 address-family ipv4 vrf CONT-VRF-102
  neighbor INET1-HUB-VRF102 route-map POP-SELECT in
  neighbor INET1-HUB-VRF102 route-map SPOKE-OUT-VRF102 out
  neighbor MPLS1-HUB-VRF102 route-map POP-SELECT in
  neighbor MPLS1-HUB-VRF102 route-map SPOKE-OUT-VRF102 out
exit-address-family
```

Step 3: Apply both the prefix route-maps on remote-site border router.

```
router ospf 101 vrf IoT-VRF-101
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF

router ospf 102 vrf CONT-VRF-102
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF
```

Procedure 9 Create the static null routes for non-default VRFs

Step 1: Configure the static null route for VRF IoT-VRF-101.

```
ip route vrf IoT-VRF-101 10.22.0.0 255.255.248.0 Null0
```

Step 2: Configure the static null route for VRF CONT-VRF-102.

```
ip route vrf CONT-VRF-102 10.26.0.0 255.255.248.0 Null0
```

PROCESS

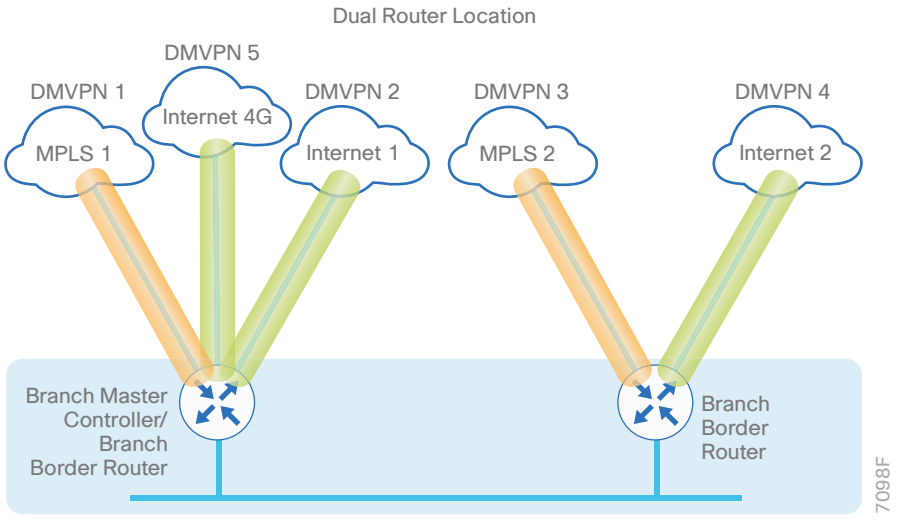
Modifying the First Router for Dual Router Design

1. Configure the access layer HSRP
2. Configure the OSPF routing protocol on the transit network
3. Enable EOT

Use the following process to configure dual-router remote site. In this section, the design assumes that you have moved to a separate site that has a configured single-router and now need to configure the second router to make it a dual-router site. The single-router example used in the previous section is assumed to be left as is.

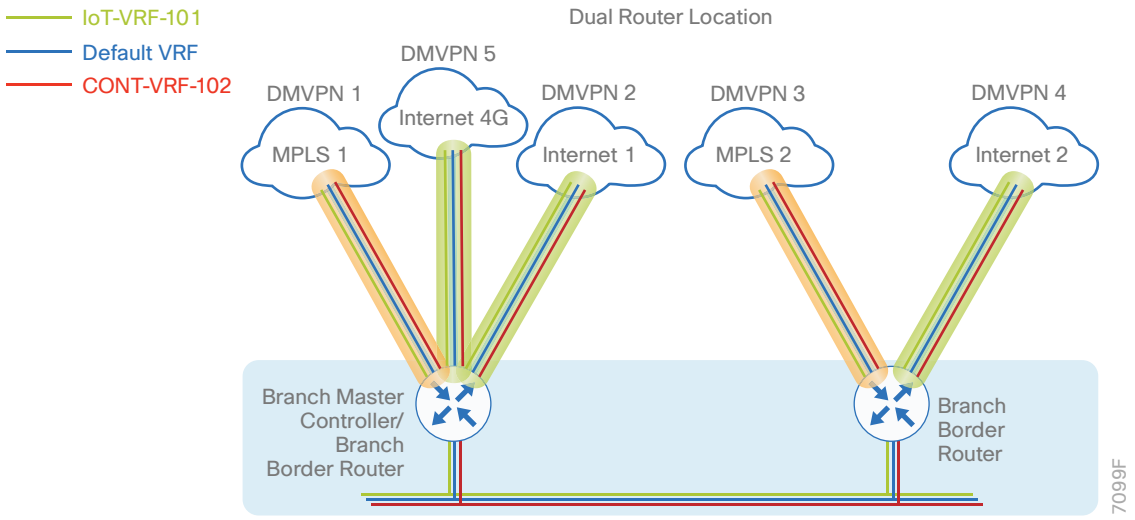
The following diagram shows the physical connections between both remote-site border routers and up to five transports. The IWAN dual hybrid model supports up to five WAN transports at a dual-router remote site.

Figure 10 *Physical view of dual router at remote-site location*



The following diagram shows the logical view of the multi-VRF traffic between both of the remote-site border routers and up to five transports.

Figure 11 *Multi VRF view of dual router at remote-site location*



Procedure 1 Configure the access layer HSRP

You need to configure HSRP to enable the use of a virtual IP (VIP) as a default gateway that is shared between two routers. The HSRP active router is the router connected to the primary WAN link and the HSRP standby router is the router connected to the secondary WAN link

In this procedure, you configure the router with connectivity to the access layer switch. In the access layer design, the remote sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The following table shows the relevant HSRP parameters for the router configuration.

Table 71 *WAN remote-site HSRP parameters (dual router)*

Router	HSRP role	VIP	Real IP address	HSRP priority	PIM DR priority
Primary	Active	.1	.2	110	110
Secondary	Standby	.1	.3	105	105

Step 1: Using the parameters in the table above, create the subinterfaces for all data or voice traffic.

```
interface GigabitEthernet0/0/2.521
 ip address 10.22.146.2 255.255.255.0
 ip pim dr-priority 110
 standby version 2
 standby 1 ip 10.22.146.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123

interface GigabitEthernet0/0/2.522
 ip address 10.26.146.2 255.255.255.0
 ip pim dr-priority 110
 standby version 2
 standby 1 ip 10.26.146.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123

interface GigabitEthernet0/0/2.531
 ip address 10.22.147.2 255.255.255.0
 ip pim dr-priority 110
 standby version 2
 standby 1 ip 10.22.147.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123

interface GigabitEthernet0/0/2.532
 ip address 10.26.147.2 255.255.255.0
 ip pim dr-priority 110
 standby version 2
 standby 1 ip 10.26.147.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Step 2: Configure transit network between two routers.

```
interface GigabitEthernet0/0/2.511
 description IoT-VRF-101 Transit Net
 encapsulation dot1Q 511
 vrf forwarding IoT-VRF-101
 ip address 10.22.144.9 255.255.255.252
 ip pim sparse-mode

interface GigabitEthernet0/0/2.512
 description CONT-VRF-102 Transit Net
 encapsulation dot1Q 512
 vrf forwarding CONT-VRF-102
 ip address 10.26.144.9 255.255.255.252
 ip pim sparse-mode
```

Step 3: Add transit network VLANs to the access layer switch.

If the VLAN does not already exist on the access layer switch, configure it now.

```
vlan 511
 name VRF-101_TransitNet
vlan 512
 name VRF-102_TransitNet
```

Step 4: Add transit network VLANs to the existing access layer switch trunk.

```
interface GigabitEthernet0/2
 switchport trunk allowed vlan add 511,512
```

Procedure 2 Configure the OSPF routing protocol on the transit network

Step 1: Turn off passive-interface for the transit network LAN interfaces.

```
router ospf 101 vrf IoT-VRF-101
 no passive-interface GigabitEthernet0/2.511

router ospf 102 vrf CONT-VRF-102
 no passive-interface GigabitEthernet0/2.512
```

Procedure 3 Enable EOT

The HSRP active router remains the active router unless the router is reloaded or fails. Having the HSRP router remain as the active router can lead to undesired behavior. If the primary WAN transport were to fail, the HSRP active router would learn an alternate path through the transit network to the HSRP standby router and begin to forward traffic across the alternate path. This is sub-optimal routing, and you can address it by using EOT.

The HSRP active router can track the state of its DMVPN tunnel interface. If the tunnel line-protocol state changes to down, this implies that the path to the primary site is no longer viable. This is a benefit of using the **if-state nhrp** feature with a DMVPN tunnel configuration.

This procedure is valid only on the router connected to the primary transport.

Step 1: Configure EOT.

A tracked object is created based on tunnel line-protocol state. If the tunnel is up, the tracked object status is Up; if the tunnel is down, the tracked object status is Down. A short delay is added after the tunnel interface comes back up in order to ensure that routing has converged properly before changing the HSRP active router.

```
track 100 interface Tunnel100 line-protocol
track 200 interface Tunnel200 line-protocol
track 500 interface Tunnel500 line-protocol

track 50 list boolean or
 object 100
 object 200
 object 500
 delay up 20
```

Step 2: Link HSRP with the tracked object. All data or voice subinterfaces should enable HSRP tracking. HSRP can monitor the tracked object status. If the status is down, the HSRP priority is decremented by the configured priority. If the decrease is large enough, the HSRP standby router preempts.

```
interface GigabitEthernet0/0/2.521
 standby 1 track 50 decrement 10

interface GigabitEthernet0/0/2.522
 standby 1 track 50 decrement 10

interface GigabitEthernet0/0/2.531
 standby 1 track 50 decrement 10

interface GigabitEthernet0/0/2.532
 standby 1 track 50 decrement 10
```

PROCESS

Configuring Second DMVPN Router at Remote Site

1. Configure the IVRF definitions and loopbacks
2. Configure the connections to the access switch
3. Configure the access layer HSRP
4. Configure IKEv2 and IPsec profiles
5. Configure the mGRE tunnel
6. Configure the routing protocol for OSPF
7. Configure the routing protocol for BGP
8. Configure the prefix-lists for OSPF and BGP
9. Create and apply the prefix route maps for OSPF and BGP
10. Create the static null routes

Use these procedures when configuring the second router of a dual-router design. This set of procedures includes the additional steps necessary to configure a second router as a DMVPN spoke router when the first router has already been configured with the process "Configuring Remote-Site DMVPN Spoke Router."

If you have not done so already, the previous process, "Modifying the First Router for Dual Router Design," must be completed. The parameters in the tables below are used in the following procedures.

Table 72 VRFs and loopback interfaces for remote-site router (RS32-4451x-2)

VRF name	Loopback interface	IP address	OSPF process-id
Default VRF	Loopback 0	10.255.243.32/32	100
IoT-VRF-101	Loopback 101	10.201.243.32/32	101
CONT-VRF-102	Loopback 102	10.202.243.32/32	102

Reader Tip

Whenever IWAN is designed with WAAS leveraging AppNav/WCCP, please ensure that the Loopback IP address that is being used for PfR is not also used as the AppNav Service Controller address or WCCP router ID. This is applicable for any Branch IWAN router that is part of an AppNav/WCCP Cluster.

Procedure 1 Configure the IVRF definitions and loopbacks

In this procedure, you configure the IVRF definitions and their associated loopbacks for the remote-site border router.

Step 1: Configure the two Inside IVRF definitions.

```
vrf definition IoT-VRF-101
 rd 101:1

 address-family ipv4
 exit-address-family

vrf definition CONT-VRF-102
 rd 102:1

 address-family ipv4
 exit-address-family
```

Step 2: Create the loopback interfaces.

Example: RS32-4451x-2

```
interface Loopback101
 description IoT-VRF-101
 vrf forwarding IoT-VRF-101
 ip address 10.201.243.32 255.255.255.255
 ip pim sparse-mode
 hold-queue 1024 in
 hold-queue 1024 out

interface Loopback102
 description CONT-VRF-102
 vrf forwarding CONT-VRF-102
 ip address 10.202.243.32 255.255.255.255
 hold-queue 1024 in
 hold-queue 1024 out
```

Procedure 2 Configure the connections to the access switch

In this procedure, you configure the router with connectivity to the access layer switch. In the access layer design, the remote sites use collapsed routing, with 802.1Q trunk interfaces to the LAN access layer.

Step 1: Configure IP settings for each subinterface.

This design uses an IP addressing convention with the default gateway router assigned an IP address and IP mask combination of **N.N.N.1 255.255.255.0** where *N.N.N* is the IP network and *1* is the IP host.

When you are using a centralized DHCP server, your routers with LAN interfaces connected to a LAN using DHCP for end-station IP addressing must use an IP helper.

This remote-site DMVPN spoke router is the second router of a dual-router design and HSRP is configured at the access layer. The actual interface IP assignments are configured in the following procedure.

```
interface GigabitEthernet0/0/2.521
 encapsulation dot1Q 521
 vrf forwarding IoT-VRF-101
 ip helper-address global 10.4.48.10
 ip pim sparse-mode

interface GigabitEthernet0/0/2.522
 encapsulation dot1Q 522
 vrf forwarding CONT-VRF-102
 ip helper-address global 10.4.48.10
 ip pim sparse-mode

interface GigabitEthernet0/0/2.531
 encapsulation dot1Q 531
 vrf forwarding IoT-VRF-101
 ip helper-address global 10.4.48.10
 ip pim sparse-mode

interface GigabitEthernet0/0/2.532
 encapsulation dot1Q 532
 vrf forwarding CONT-VRF-102
 ip helper-address global 10.4.48.10
 ip pim sparse-mode
```

Procedure 3 Configure the access layer HSRP

You configure HSRP to enable a VIP that you use as a default gateway that is shared between two routers. The HSRP active router is the router connected to the primary carrier and the HSRP standby router is the router connected to the secondary carrier or backup link.

Step 1: Configure the HSRP standby router with a standby priority that is lower than the HSRP active router.

The router with the higher standby priority value is elected as the HSRP active router. The preempt option allows a router with a higher priority to become the HSRP active, without waiting for a scenario where there is no router in the HSRP active state. The relevant HSRP parameters for the router configuration are shown in the following table.

Table 73 WAN remote-site HSRP parameters (dual router)

Router	HSRP role	VIP	Real IP address	HSRP priority	PIM DR priority
Primary	Active	.1	.2	110	110
Secondary	Standby	.1	.3	105	105

Step 2: Create the subinterfaces for both data and voice VLANs for each VRF.

```
interface GigabitEthernet0/0/2.521
 description IoT-VRF-101 Data
 ip address 10.22.146.3 255.255.255.0
 ip pim dr-priority 105
 standby version 2
 standby 1 ip 10.22.146.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123

interface GigabitEthernet0/0/2.522
 description CONT-VRF-102 Data
 ip address 10.26.146.3 255.255.255.0
 ip pim dr-priority 105
 standby version 2
 standby 1 ip 10.26.146.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

```
interface GigabitEthernet0/0/2.531
 description IoT-VRF-101 Voice
 ip address 10.22.147.3 255.255.255.0
 ip pim dr-priority 105
 standby version 2
 standby 1 ip 10.22.147.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123

interface GigabitEthernet0/0/2.532
 description CONT-VRF-102 Voice
 ip address 10.26.147.3 255.255.255.0
 ip pim dr-priority 105
 standby version 2
 standby 1 ip 10.26.147.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string c1sco123
```

Step 3: Configure transit network between two routers.

```
interface GigabitEthernet0/0/2.511
 description IoT-VRF-101 Transit Net
 encapsulation dot1Q 511
 vrf forwarding IoT-VRF-101
 ip address 10.22.144.10 255.255.255.252
 ip pim sparse-mode

interface GigabitEthernet0/0/2.512
 description CONT-VRF-102 Transit Net
 encapsulation dot1Q 512
 vrf forwarding CONT-VRF-102
 ip address 10.26.144.10 255.255.255.252
 ip pim sparse-mode
```

Procedure 4 Configure IKEv2 and IPsec profiles

To complete the IKEv2 and IPsec configuration for this router, follow the steps in "Configuring IKEv2 and IPsec for a remote site router" in Appendix B.

Procedure 5 Configure the mGRE tunnel

In this procedure, you configure mGRE tunnels for DMVPN in each VRF. This type of tunnel requires a source interface only. Use the same source interface that you use to connect to the MPLS or Internet.

In a multi-VRF deployment, all tunnels with the same tunnel source interface must use the same IPsec profile and must have the **tunnel protection shared** command configured. To differentiate tunnels after decryption, a different **tunnel key** is used per VRF.

Table 74 DMVPN tunnel information for remote-site border router

Transport name	IPSEC profile	Bandwidth	FVRF	Tunnel source
MPLS2	DMVPN-IPSEC-PROFILE-MPLS2	50000	IWAN-TRANSPORT-3	Gig 0/0/0
INET2	DMVPN-IPSEC-PROFILE-INET2	300000	IWAN-TRANSPORT-4	Gig 0/0/1

Table 75 Tunnel information for border router RS32-4451x-2 (MPLS2)

VRF name	Tunnel ID	IP address	NHRP network-ID/ tunnel-key
Default VRF	300	10.6.38.32/23	1300
IoT-VRF-101	301	10.21.38.32/23	1301
CONT-VRF-102	302	10.25.38.32/23	1302

Table 76 Tunnel information for border router RS32-4451x-2 (INET2)

VRF name	Tunnel ID	IP address	NHRP network-ID/ tunnel-key
Default VRF	400	10.6.40.32/23	1400
IoT-VRF-101	401	10.21.40.32/23	1401
CONT-VRF-102	402	10.25.40.32/23	1402

Step 1: Using the parameters in the tables above, configure the tunnel interfaces for each tunnel ID.

Example: RS32-4451x-2

```
interface Tunnel301
 description IoT-VRF-101 tunnel via MPLS2
 bandwidth 50000
 vrf forwarding IoT-VRF-101
 ip address 10.21.38.32 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 if-state nhrp
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 1301
 tunnel vrf IWAN-TRANSPORT-3
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-MPLS2 shared

interface Tunnel302
 description CONT-VRF-102 tunnel via MPLS2
 bandwidth 50000
 vrf forwarding CONT-VRF-102
 ip address 10.25.38.32 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 if-state nhrp
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 1302
 tunnel vrf IWAN-TRANSPORT-3
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-MPLS2 shared
```

```
interface Tunnel401
 description IoT-VRF-101 tunnel via INET2
 bandwidth 300000
 vrf forwarding IoT-VRF-101
 ip address 10.21.40.32 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel key 1401
 tunnel vrf IWAN-TRANSPORT-4
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-INET2 shared

interface Tunnel402
 description CONT-VRF-102 tunnel via INET2
 bandwidth 300000
 vrf forwarding CONT-VRF-102
 ip address 10.25.40.32 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim dr-priority 0
 ip pim sparse-mode
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre multipoint
 tunnel key 1402
 tunnel vrf IWAN-TRANSPORT-4
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE-INET2 shared
```

Step 2: Configure NHRP on tunnel interface.

The DMVPN hub router is the NHRP server for all of the spokes. NHRP is used by remote routers to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires several additional configuration statements in order to define the NHRP server and NHRP map statements for the DMVPN hub router mGRE tunnel IP address. Spoke routers require the NHRP static multicast mapping.

When hub BRs are added for horizontal scaling or a second DC is added as a transit site, spoke routers require additional NHS statements for each BR in their environment. The configuration details are covered in subsequent sections of this guide.

The value used for the NHS is the mGRE tunnel address for the DMVPN hub router. The map entries must be set to the outside NAT value of the DMVPN hub, as configured on the Cisco ASA 5500. This design uses the values shown in the following tables.

Table 77 DMVPN tunnel NHRP parameters for border router RS32-4451x-2 (MPLS2)

Parameter	Default VRF	IoT-VRF-101	CONT-VRF-102
DMVPN Tunnel ID	300	301	302
DMVPN hub-site BR public address (actual)	192.168.7.1	192.168.7.1	192.168.7.1
DMVPN transit-site BR public address (actual)	192.168.7.41	192.168.7.41	192.168.7.41
DMVPN hub-site BR public address (externally routable after NAT)	n/a (MPLS1)	n/a (MPLS1)	n/a (MPLS1)
DMVPN transit-site BR public address (externally routable after NAT)	n/a (MPLS1)	n/a (MPLS1)	n/a (MPLS1)
DMVPN hub-site BR tunnel IP address (NHS)	10.6.38.1	10.21.38.1	10.25.38.1
DMVPN transit-site BR tunnel IP address (NHS)	10.6.38.2	10.21.38.2	10.25.38.2
NHRP network ID	1300	1301	1302

Table 78 DMVPN tunnel NHRP parameters for border router RS32-4451x-2 (INET2)

Parameter	Default VRF	IoT-VRF-101	CONT-VRF-102
DMVPN Tunnel ID	400	401	402
DMVPN hub-site BR public address (actual)	192.168.146.11	192.168.146.11	192.168.146.11
DMVPN transit-site BR public address (actual)	192.168.146.14	192.168.146.14	192.168.146.14
DMVPN hub-site BR public address (externally routable after NAT)	172.17.140.1	172.17.140.1	172.17.140.1
DMVPN transit-site BR public address (externally routable after NAT)	172.17.140.2	172.17.140.2	172.17.140.2
DMVPN hub-site BR tunnel IP address (NHS)	10.6.40.1	10.21.40.1	10.25.40.1
DMVPN transit-site BR tunnel IP address (NHS)	10.6.40.2	10.21.40.2	10.25.40.2
NHRP network ID	1400	1401	1402

NHRP requires all devices within a DMVPN cloud to use the same network ID and authentication key. The NHRP cache holdtime should be configured to 600 seconds.

This design supports DMVPN spoke routers that receive their external IP addresses through DHCP. It is possible for these routers to acquire different IP addresses after a reload. When the router attempts to register with the NHRP server, the router may appear as a duplicate to an entry already in the cache and be rejected. The **registration no-unique** option allows you to overwrite existing cache entries. This feature is only required on NHRP clients (DMVPN spoke routers). **The if-state nhrp** option ties the tunnel line-protocol state to the reachability of the NHRP NHS, and if the NHS is unreachable, the tunnel line-protocol state changes to down. This feature is used in conjunction with EOT.

Example: RS32-4451x-2

```
interface Tunnel301
 ip nhrp authentication cisco123
 ip nhrp network-id 1301
 ip nhrp holdtime 600
 ip nhrp nhs 10.21.38.1 nbma 192.168.7.1 multicast
 ip nhrp nhs 10.21.38.2 nbma 192.168.7.41 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp

interface Tunnel302
```

```
 ip nhrp authentication cisco123
 ip nhrp network-id 1302
 ip nhrp holdtime 600
 ip nhrp nhs 10.25.38.1 nbma 192.168.7.1 multicast
 ip nhrp nhs 10.25.38.2 nbma 192.168.7.41 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp

interface Tunnel401
 ip nhrp authentication cisco123
 ip nhrp network-id 1401
 ip nhrp holdtime 600
 ip nhrp nhs 10.21.40.1 nbma 172.17.140.1 multicast
 ip nhrp nhs 10.21.40.2 nbma 172.17.140.2 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp

interface Tunnel402
 ip nhrp authentication cisco123
 ip nhrp network-id 1402
 ip nhrp holdtime 600
 ip nhrp nhs 10.25.40.1 nbma 172.17.140.1 multicast
 ip nhrp nhs 10.25.40.2 nbma 172.17.140.2 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 no nhrp route-watch
 if-state nhrp
```

Procedure 6 Configure the routing protocol for OSPF

Table 79 OSPF information for remote-site border router RS32-4451x-2

OSPF process-ID	VRF name	Router-ID	LAN interface	LAN IP network/ subnet mask
100	Default VRF	10.255.243.32	Gig 0/0/2.64 Gig 0/0/2.69 Gig 0/0/2.99	10.7.144.0/21 10.255.243.32/32
101	IoT-VRF-101	10.201.243.32	Gig 0/0/2.521 Gig 0/0/2.531 Gig 0/0/2.511	10.22.144.0/21 10.201.243.32/32
102	CONT-VRF-102	10.202.243.32	Gig 0/0/2.522 Gig 0/0/2.532 Gig 0/0/2.512	10.26.144.0/21 10.202.243.32/32

Step 1: Configure an OSPF routing protocol on the spoke router.

Example: RS32-4451x-2

```
router ospf 101 vrf IoT-VRF-101
 router-id 10.201.243.32
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF
 passive-interface default
 no passive-interface GigabitEthernet0/0/2.521
 no passive-interface GigabitEthernet0/0/2.531
 no passive-interface GigabitEthernet0/0/2.511
 network 10.22.144.0 0.0.7.255 area 0
 network 10.201.243.32 0.0.0.0 area 0
 default-information originate

router ospf 102 vrf CONT-VRF-102
 router-id 10.202.243.32
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF
 passive-interface default
 no passive-interface GigabitEthernet0/0/2.522
 no passive-interface GigabitEthernet0/0/2.532
```

```
no passive-interface GigabitEthernet0/0/2.512
network 10.26.144.0 0.0.7.255 area 0
network 10.202.243.32 0.0.0.0 area 0
default-information originate
```

Procedure 7 Configure the routing protocol for BGP

Table 80 BGP routing information for remote-site border router RS32-4451x-2

VRF name	Router ID	Aggregate-subnet	Peer-group	Hub tunnel address	Tunnel ID
Default VRF	10.255.243.32	10.7.144.0/21	MPLS2-HUB	10.6.38.1 10.6.38.2	300
			INET2-HUB	10.6.40.1 10.6.40.2	400
IoT-VRF-101	10.201.243.32	10.22.144.0/21	MPLS2-HUB-VRF101	10.21.38.1 10.21.38.2	301
			INET2-HUB-VRF101	10.21.40.1 10.21.40.2	401
CONT-VRF-102	10.202.243.32	10.26.144.0/21	MPLS2-HUB-VRF102	10.25.38.1 10.25.38.2	302
			INET2-HUB-VRF102	10.25.40.1 10.25.40.2	402

Step 1: Configure BGP routing protocol for VRFs IoT-VRF-101 and CONT-VRF-102.

Example: IoT-VRF-101–RS32-4451x-2

```
router bgp 65100
 address-family ipv4 vrf IoT-VRF-101
  bgp router-id 10.201.243.32
  aggregate-address 10.22.144.0 255.255.248.0 summary-only
  redistribute connected
  neighbor INET2-HUB-VRF101 peer-group
  neighbor INET2-HUB-VRF101 remote-as 65100
  neighbor INET2-HUB-VRF101 description To IWAN INET2 Hub Router
  neighbor INET2-HUB-VRF101 update-source Tunnel401
  neighbor INET2-HUB-VRF101 timers 20 60
```

```
 neighbor INET2-HUB-VRF101 send-community
 neighbor INET2-HUB-VRF101 next-hop-self all
 neighbor INET2-HUB-VRF101 weight 50000
 neighbor INET2-HUB-VRF101 soft-reconfiguration inbound
 neighbor MPLS2-HUB-VRF101 peer-group
 neighbor MPLS2-HUB-VRF101 remote-as 65100
 neighbor MPLS2-HUB-VRF101 description To IWAN MPLS2 Hub Router
 neighbor MPLS2-HUB-VRF101 update-source Tunnel301
 neighbor MPLS2-HUB-VRF101 timers 20 60
 neighbor MPLS2-HUB-VRF101 send-community
 neighbor MPLS2-HUB-VRF101 next-hop-self all
 neighbor MPLS2-HUB-VRF101 weight 50000
 neighbor MPLS2-HUB-VRF101 soft-reconfiguration inbound
 neighbor 10.21.38.1 peer-group MPLS2-HUB-VRF101
 neighbor 10.21.38.1 activate
 neighbor 10.21.38.2 peer-group MPLS2-HUB-VRF101
 neighbor 10.21.38.2 activate
 neighbor 10.21.40.1 peer-group INET2-HUB-VRF101
 neighbor 10.21.40.1 activate
 neighbor 10.21.40.2 peer-group INET2-HUB-VRF101
 neighbor 10.21.40.2 activate
 maximum-secondary-paths ibgp 3
 distance bgp 201 89 89
exit-address-family
```

Example: CONT-VRF-102–RS32-4451x-2

```
router bgp 65100
 address-family ipv4 vrf IoT-VRF-101
  bgp router-id 10.202.243.32
  aggregate-address 10.26.144.0 255.255.248.0 summary-only
  redistribute connected
  neighbor INET2-HUB-VRF102 peer-group
  neighbor INET2-HUB-VRF102 remote-as 65100
  neighbor INET2-HUB-VRF102 description To IWAN INET2 Hub Router
  neighbor INET2-HUB-VRF102 update-source Tunnel402
  neighbor INET2-HUB-VRF102 timers 20 60
```

```
 neighbor INET2-HUB-VRF102 send-community
 neighbor INET2-HUB-VRF102 next-hop-self all
 neighbor INET2-HUB-VRF102 weight 50000
 neighbor INET2-HUB-VRF102 soft-reconfiguration inbound
 neighbor MPLS2-HUB-VRF102 peer-group
 neighbor MPLS2-HUB-VRF102 remote-as 65100
 neighbor MPLS2-HUB-VRF102 description To IWAN MPLS2 Hub Router
 neighbor MPLS2-HUB-VRF102 update-source Tunnel302
 neighbor MPLS2-HUB-VRF102 timers 20 60
 neighbor MPLS2-HUB-VRF102 send-community
 neighbor MPLS2-HUB-VRF102 next-hop-self all
 neighbor MPLS2-HUB-VRF102 weight 50000
 neighbor MPLS2-HUB-VRF102 soft-reconfiguration inbound
 neighbor 10.25.38.1 peer-group MPLS2-HUB-VRF102
 neighbor 10.25.38.1 activate
 neighbor 10.25.38.2 peer-group MPLS2-HUB-VRF102
 neighbor 10.25.38.2 activate
 neighbor 10.25.40.1 peer-group INET2-HUB-VRF102
 neighbor 10.25.40.1 activate
 neighbor 10.25.40.2 peer-group INET2-HUB-VRF102
 neighbor 10.25.40.2 activate
 maximum-secondary-paths ibgp 3
 distance bgp 201 89 89
exit-address-family
```

Procedure 8 Configure the prefix-lists for OSPF and BGP

Step 1: Create the local loopback prefix-list for each VRF on remote-site border router.

Table 81 Local loopback prefix-list for remote-site border router RS32-4451x-2

VRF name	Prefix-list	IP-subnet
Default VRF	LOCAL-LOOPBACKS	10.255.241.32/32 10.255.243.32/32
IoT-VRF-101	LOCAL-LOOPBACKS-101	10.201.241.32/32 10.201.243.32/32
CONT-VRF-102	LOCAL-LOOPBACKS-102	10.202.241.32/32 10.202.243.32/32

Example: RS32-4451x-2

```
ip prefix-list LOCAL-LOOPBACKS-101 seq 10 permit 10.201.241.32/32
ip prefix-list LOCAL-LOOPBACKS-101 seq 20 permit 10.201.243.32/32

ip prefix-list LOCAL-LOOPBACKS-102 seq 10 permit 10.202.241.32/32
ip prefix-list LOCAL-LOOPBACKS-102 seq 20 permit 10.202.243.32/32
```

Step 2: Create the local subnet prefix-list for each VRF on remote-site border router.

Table 82 Local subnet prefix-list for remote-site border router RS32-4451x-2

VRF name	Prefix-list	IP-subnet
Default VRF	LOCAL-SUBNETS	10.7.144.0/21
IoT-VRF-101	LOCAL-SUBNETS-101	10.22.144.0/21
CONT-VRF-102	LOCAL-SUBNETS-102	10.26.144.0/21

Example: RS32-4451x-2

```
ip prefix-list LOCAL-SUBNETS-101 seq 10 permit 10.22.144.0/21
ip prefix-list LOCAL-SUBNETS-102 seq 10 permit 10.26.144.0/21
```

Procedure 9 Create and apply the prefix route maps for OSPF and BGP

Step 1: Create the prefix route-map SPOKE-OUT for BGP on remote-site border router.

The parameters in the table below are used in this step.

Table 83 Prefix route-map SPOKE-OUT information for remote-site border router RS32-4451x-2

VRF name	Community-value	Prefix-list
Default VRF	65100:10	LOCAL-LOOPBACKS LOCAL-SUBNETS
IoT-VRF-101	65100:10	LOCAL-LOOPBACKS-101 LOCAL-SUBNETS-101
CONT-VRF-102	65100:10	LOCAL-LOOPBACKS-102 LOCAL-SUBNETS-102

```
route-map SPOKE-OUT-VRF101 permit 10
 description Prefer POP1 with community 65100:10
 match ip address prefix-list LOCAL-LOOPBACKS-101 LOCAL-SUBNETS-101
 set community 65100:10

route-map SPOKE-OUT-VRF102 permit 10
 description Prefer POP1 with community 65100:10
 match ip address prefix-list LOCAL-LOOPBACKS-102 LOCAL-SUBNETS-102
 set community 65100:10
```

Step 2: Apply both the prefix route-maps on remote-site border router.

```
router bgp 65100

 address-family ipv4 vrf IoT-VRF-101
  neighbor INET2-HUB-VRF101 route-map POP-SELECT in
  neighbor INET2-HUB-VRF101 route-map SPOKE-OUT-VRF101 out
  neighbor MPLS2-HUB-VRF101 route-map POP-SELECT in
  neighbor MPLS2-HUB-VRF101 route-map SPOKE-OUT-VRF101 out
exit-address-family

 address-family ipv4 vrf CONT-VRF-102
  neighbor INET2-HUB-VRF102 route-map POP-SELECT in
  neighbor INET2-HUB-VRF102 route-map SPOKE-OUT-VRF102 out
  neighbor MPLS2-HUB-VRF102 route-map POP-SELECT in
  neighbor MPLS2-HUB-VRF102 route-map SPOKE-OUT-VRF102 out
exit-address-family
```

Step 3: Create the route-map REDIST-BGP-TO-OSPF for OSPF on remote-site border router.

```
route-map REDIST-BGP-TO-OSPF permit 10
 description Set a route tag to identify routes redistributed from BGP
 set tag 1

route-map REDIST-OSPF-TO-BGP deny 10
 description Block all routes redistributed from BGP
 match tag 1

route-map REDIST-OSPF-TO-BGP permit 20
```

```
 description Redistribute all other routes
 match route-type internal
 match route-type external type-1
 match route-type external type-2
```

Step 4: Apply both the prefix route-maps on remote-site border router.

```
router ospf 101 vrf IoT-VRF-101
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF

router ospf 102 vrf CONT-VRF-102
 redistribute bgp 65100 subnets route-map REDIST-BGP-TO-OSPF
```

Procedure 10 Create the static null routes

Step 1: Configure the static null route for VRF IoT-VRF-101.

```
ip route vrf IoT-VRF-101 10.22.144.0 255.255.248.0 Null0
```

Step 2: Configure the static null route for VRF CONT-VRF-102.

```
ip route vrf CONT-VRF-102 10.26.144.0 255.255.248.0 Null0
```

Deploying Firewall for Inter-VRF Route Leaking

In a multi-VRF IWAN network, there is full isolation of routing information from each other. A user on one VRF is isolated and unable to communicate with the users on other VRFs. The route leaking node (firewall) is responsible for extending routes between the GRT and VRF tables. As an example, this design accomplishes the route leaking using a Cisco Firewall (ASA 5525). However, customers may use another vendor's hardware to implement business requirements to allow/deny different types of traffic.

PROCESS

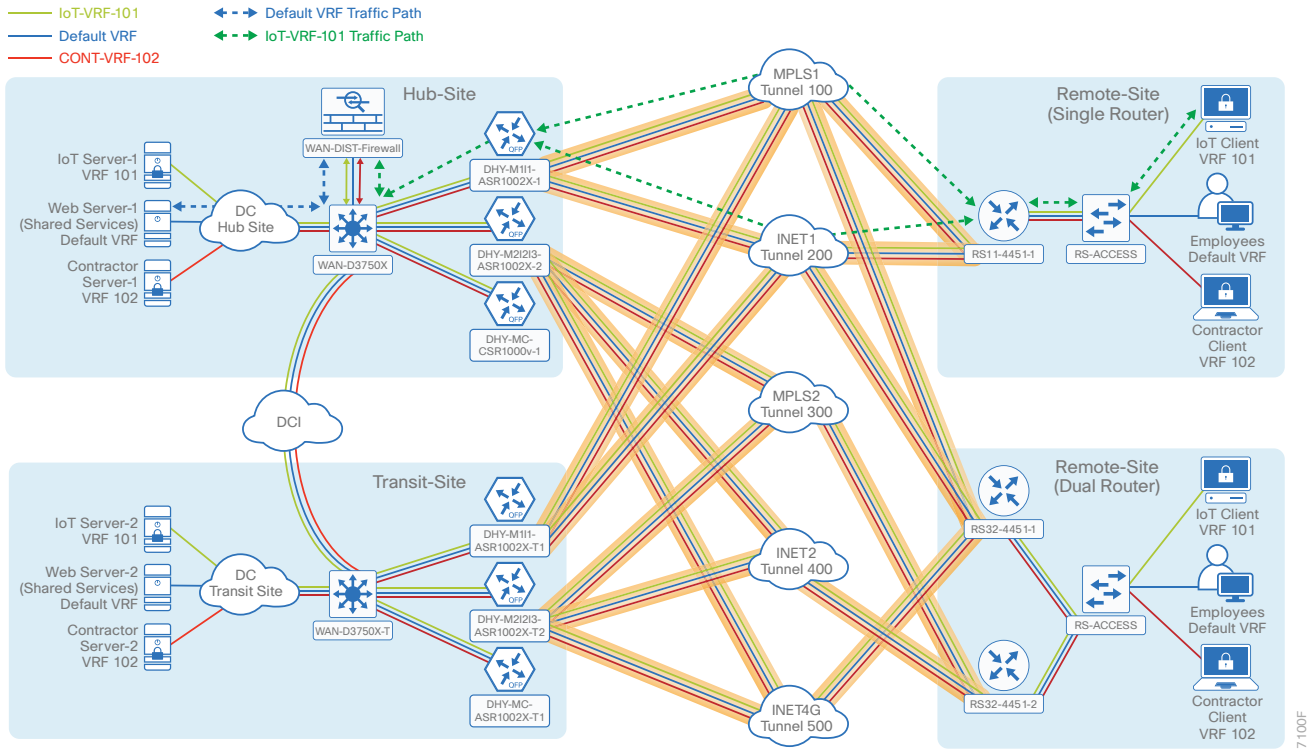
Configuring a Firewall at Hub-Site

1. Configure the network interfaces
2. Define the static routes for Inter-VRF route leaking
3. Define and apply the access lists

The following diagram uses dotted lines to show the end-to-end traffic flow from remote sites to the hub-site. The dotted-line color indicates how the firewall directs the traffic flow on two sides:

- The blue dotted line shows the firewall directing the example IoT VRF traffic to the shared services in the global network.
- The green dotted line shows the traffic from the example IoT client to/from the WAN distribution switch, routed to the firewall.

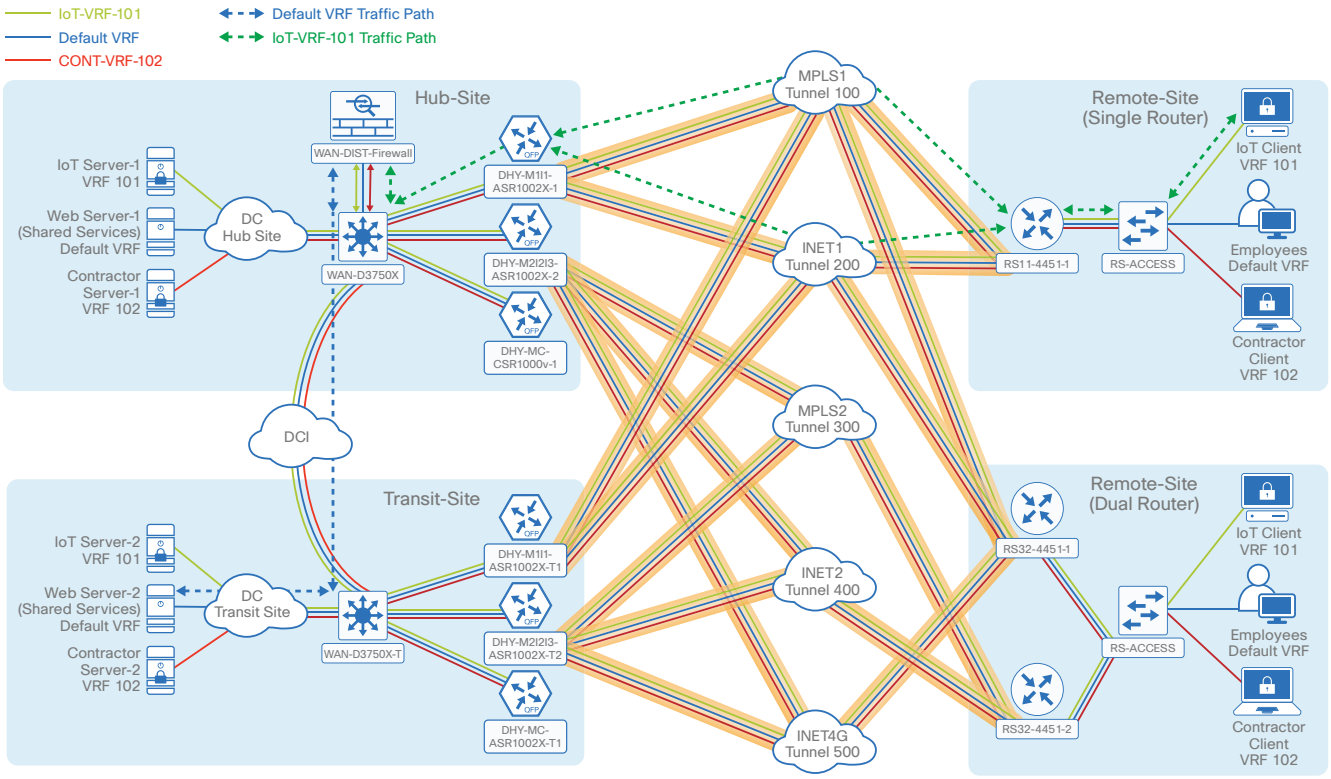
Figure 12 *Firewall managing the traffic flow between the hub and remote sites*



The following diagram uses dotted lines to show the end-to-end traffic flow from remote sites to the transit-site. The dotted-line color indicates how the firewall directs the traffic flow on two sides:

- The blue dotted line shows the firewall directing the example IoT VRF traffic to the shared services in the global network in the transit-site.
- The green dotted line shows the traffic from the example IoT client to/from the WAN distribution switch, routed to the firewall.

Figure 13 *Firewall at the hub-site managing the traffic flow between the transit and remote sites*



Procedure 1 Configure the network interfaces

In this procedure, you configure the connection between the Cisco ASA firewall and the hub-site distribution switch.

Step 1: Configure the physical interface.

```
interface GigabitEthernet0/0
description WAN-D3750X (gig 1/0/23)
 channel-group 20 mode on
 no nameif
 no security-level
 no ip address
 no shutdown

interface GigabitEthernet0/1
 description WAN-D3750X (gig 2/0/23)
 channel-group 20 mode on
 no nameif
 no security-level
 no ip address
 no shutdown
```

Step 2: Configure the port-channel.

```
interface Port-channel20
 description WAN-D3750X
 lacp max-bundle 8
 no nameif
 no security-level
 no ip address
 no shutdown
```

Step 3: Configure the sub port-channel for default VRF.

```
interface Port-channel20.20
 vlan 20
 nameif DC-INSIDE
 security-level 100
 ip address 10.6.32.26 255.255.255.248
```

Step 4: Configure the sub port-channel for VRF IoT-VRF-101.

```
interface Port-channel20.21
 vlan 21
 nameif VRF101-OUTSIDE
 security-level 100
 ip address 10.21.32.26 255.255.255.248
```

Step 5: Configure the sub port-channel for VRF CONT-VRF-102.

```
interface Port-channel20.22
 vlan 22
 nameif VRF102-OUTSIDE
 security-level 100
 ip address 10.25.32.26 255.255.255.248
```

Procedure 2 Define the static routes for Inter-VRF route leaking

In this procedure, you define the next-hop IP address for global and both VRFs.

Step 1: Define next-hop IP address for multi VRF routes from GRT.

```
route DC-INSIDE 0.0.0.0 0.0.0.0 10.6.32.25 1
```

Step 2: Define next-hop IP address for GRT from IoT-VRF-101.

```
route VRF101-OUTSIDE 10.20.0.0 255.252.0.0 10.21.32.25 1
route VRF101-OUTSIDE 10.201.240.0 255.255.252.0 10.21.32.25 1
```

Step 3: Define next-hop IP address for GRT from CONT-VRF-102.

```
route VRF102-OUTSIDE 10.202.240.0 255.255.252.0 10.25.32.25 1
route VRF102-OUTSIDE 10.24.0.0 255.252.0.0 10.25.32.25 1
```

Procedure 3 Define and apply the access lists

In this procedure, you configure the access lists in order to enable the IP network security between global and both VRFs.

Step 1: Define the global implicit rules.

```
access-list GLOBAL-ACCESS extended permit icmp any any echo
access-list GLOBAL-ACCESS extended permit icmp any any echo-reply
access-list GLOBAL-ACCESS extended permit ip any any
```

Step 2: Apply the rules to global access-group.

```
access-group GLOBAL-ACCESS global
```

Deploying IWAN Performance Routing

Performance Routing Version 3 (PfRv3) consists of two major Cisco IOS components, a master controller (MC) and a border router (BR). The MC defines the policies and applies them to various traffic classes that traverse the BR systems. The MC can be configured to learn and control traffic classes on the network.

The remote site typically manages fewer active traffic classes, which are made up of prefixes and applications. In most remote site deployments, it is possible to co-locate the MC and BR on the same hardware platform. CPU and memory utilization should be monitored on MC platforms, and if utilization is high, the network manager should consider an MC platform with a higher capacity CPU and memory. The MC communicates with the BRs over an authenticated TCP socket but has no requirement for populating its own IP routing table with anything more than a route to reach the BRs.

PROCESS

Configuring the Hub-site Master Controller

1. Configure the IVRF definitions and loopbacks
2. Configure the connections to the hub-site WAN distribution switch
3. Configure the routing protocol on the LAN

This section describes configuring the performance routing (PfR) hub-site MC.

Procedure 1 Configure the IVRF definitions and loopbacks

In this procedure, you configure the definitions for two VRFs and their associated loopback interfaces.

Step 1: Configure the VRFs.

```
vrf definition IoT-VRF-101
 rd 101:1

 address-family ipv4
 exit-address-family

vrf definition CONT-VRF-102
 rd 102:1

 address-family ipv4
 exit-address-family
```

Step 2: Configure the loopback interfaces.

```
interface Loopback101
 description IoT-VRF-101
 vrf forwarding IoT-VRF-101
 ip address 10.21.32.251 255.255.255.255
 hold-queue 1024 in
 hold-queue 1024 out

interface Loopback102
 description CONT-VRF-102
 vrf forwarding CONT-VRF-102
 ip address 10.25.32.251 255.255.255.255
 hold-queue 1024 in
 hold-queue 1024 out
```

Procedure 2 Configure the connections to the hub-site WAN distribution switch

Step 1: Add the port-channel sub-interfaces.

```
interface Port-channel21.1100
 description IW-WAN-D3750X
 encapsulation dot1Q 1100
 ip address 10.6.32.151 255.255.255.224

interface Port-channel21.1101
 description IW-WAN-D3750X IoT-VRF-101
 encapsulation dot1Q 1101
 vrf forwarding IoT-VRF-101
 ip address 10.21.32.151 255.255.255.224

interface Port-channel21.1102
 description IW-WAN-D3750X CONT-VRF-102
 encapsulation dot1Q 1102
 vrf forwarding CONT-VRF-102
 ip address 10.25.32.151 255.255.255.224
```

Procedure 3 Configure the routing protocol on the LAN

Step 1: Configure OSPF for IoT-VRF-101 VRF.

```
router ospf 101 vrf IoT-VRF-101
 router-id 10.21.32.251
 capability vrf-lite
 passive-interface default
 no passive-interface Port-channel21.1101
 network 10.21.32.128 0.0.0.63 area 0
 network 10.21.32.251 0.0.0.0 area 0
```

Step 2: Configure OSPF for CONT-VRF-102 VRF.

```
router ospf 102 vrf CONT-VRF-102
 router-id 10.25.32.251
 capability vrf-lite
 passive-interface default
 no passive-interface Port-channel21.1102
 network 10.25.32.128 0.0.0.63 area 0
 network 10.25.32.251 0.0.0.0 area 0
```

PROCESS

Configuring PfR for the Hub-site Location

1. Verify IP connectivity to remote-site loopback interfaces
2. Configure prefixes for the enterprise and DC
3. Configure PfR domain in the hub-site MC
4. Configure PfR domain in the hub-site BR
5. Verify PfR domain is operational on the hub-site MC

All sites belong to a PfR domain where the remote site MCs are peered together. Peering has been greatly enhanced in PfRv3, which allows site information exchange and single touch provisioning.

PfRv3 has simplified policies with pre-existing templates. The policy configuration for the PfR domain is done in the hub MC and the information is distributed to all sites via MC peering. This not only simplifies provisioning substantially but also makes the policy consistent across the entire IWAN network.

PfRv3 uses Unified Monitor (also called Performance Monitor) to monitor traffic going into WAN links and traffic coming from the WAN links. It monitors performance metrics per differentiated service code point (DSCP) rather than monitoring on per-flow or per-prefix basis. When application-based policies are used, the MC uses a mapping table between the application name and the DSCP discovered. This reduces the number of records significantly. PfRv3 relies on performance data measured on the existing data traffic on all paths whenever it can, thereby reducing the need of synthetic traffic. Furthermore, the measurement data is not exported unless there is a violation, which further reduces control traffic and processing of those records.

PfRv3 is also VRF-aware, and instances of the MC work under a VRF.

Procedure 1 Verify IP connectivity to remote-site loopback interfaces

It is mandatory to use loopback interfaces for the peering traffic between the BR and MC routers. For this design, you put the loopback addresses into a specific subnet range, so they are easily identified in the routing table. The loopback address ranges for the remote sites are as follows:

Table 84 Loopback IP address ranges for remote-site border routers

IWAN design model	VRF name	Loopback 0 address range
Primary router	Default VRF	10.255.241.0/24
Primary router	IoT-VRF-101	10.201.241.0/24
Primary router	CONT-VRF-102	10.202.241.0/24
Secondary router	Default VRF	10.255.243.0/24
Secondary router	IoT-VRF-101	10.201.243.0/24
Secondary router	CONT-VRF-102	10.202.243.0/24

Step 1: Verify that the loopback 0 interfaces on each of your remote sites are reachable from the hub MC by using the **show ip route** command.

This example shows a loopback address range of 10.255.241.0/24 for six remote site primary routers.

```
DHY-MC-CSR1000v-1#show ip route | include 10.255.241
O E1     10.255.241.11/32
O E1     10.255.241.12/32
O E1     10.255.241.32/32
O E1     10.255.241.41/32
O E1     10.255.241.42/32
O E1     10.255.241.51/32
```

Procedure 2 Configure prefixes for the enterprise and DC

Before the configuration of PfRv3 on the hub MC, you must create a prefix list for the enterprise and DC. The enterprise-prefix list covers the range of IP addresses to be controlled and optimized within this IWAN domain. Prefixes outside of the enterprise-prefix list are not be controlled by application policies, but they are load-balanced.

The site-prefix range includes the prefixes at this specific site, which is normally a WAN aggregation or DC site. Site-prefixes are typically statically defined at WAN aggregation and DC sites and discovered automatically at remote sites.

Tech Tip

PfR does not support the ip prefix-list options **ge** and **le**.

Step 1: Create the enterprise prefix list for each new VRF.

```
ip prefix-list ENTERPRISE-PREFIXES-101 seq 10 permit 10.4.0.0/14
ip prefix-list ENTERPRISE-PREFIXES-101 seq 20 permit 10.21.0.0/16

ip prefix-list ENTERPRISE-PREFIXES-102 seq 10 permit 10.4.0.0/14
ip prefix-list ENTERPRISE-PREFIXES-102 seq 20 permit 10.25.0.0/16
```

Step 2: Create the primary site prefix list for each new VRF.

```
ip prefix-list DC1-PREFIXES-101 seq 10 permit 10.4.0.0/16
ip prefix-list DC1-PREFIXES-101 seq 20 permit 10.21.0.0/16

ip prefix-list DC1-PREFIXES-102 seq 10 permit 10.4.0.0/16
ip prefix-list DC1-PREFIXES-102 seq 20 permit 10.25.0.0/16
```

Procedure 3 Configure PfR domain in the hub-site MC

Domain policies are configured on the hub MC. These policies are distributed to branch MCs by using the peering infrastructure. All sites that are in the same domain share the same set of PfR policies. Policies can be based on DSCP or on application names.

Policies are created using preexisting templates, or they can be customized with manually defined thresholds for delay, loss, and jitter.

PfR policies support the following traffic measurements:

- **Transmission Control Protocol (TCP)**—Latency and loss
- **User Datagram Protocol (UDP)**—No measurements or loss
- **Real-time Transport Protocol (RTP)**—Jitter, latency and loss

Tech Tip

Loss is not calculated for UDP traffic that is not RTP. Traffic loss for RTP voice and video packets is calculated using the sequence numbers in the RTP header.

Table 85 PfR domain pre-defined policy templates

Pre-defined template	Priority	Threshold definition
Voice	1	One-way-delay threshold 150 msec
	2	Loss threshold 1.0 percent
	3	Jitter threshold 30000 usec
Real-time-video	1	Loss threshold 1.0 percent
	2	One-way-delay threshold 150 msec
	3	Jitter threshold 20000 usec
Low-latency-data	1	One-way-delay threshold 100 msec
	2	Loss threshold 5.0 percent
Bulk-data	1	One-way-delay threshold 300 msec
	2	Loss threshold 10.0 percent
Best-effort	1	One-way-delay threshold 500 msec
	2	Loss threshold 5.0 percent
Scavenger	1	One-way-delay threshold 500 msec
	2	Loss threshold 50.0 percent

To avoid unwanted channel unreachable messages, it is recommended that you change the value of the **channel-unreachable-timer** command from its default setting of 1 second. The command is under the **advanced** setting and the value is specified in seconds.

The NMS collector IP address and port number are defined in the hub MC. The information is automatically propagated to devices in the IWAN domain. If you do not want to use a single collector for your entire network, you can specify a different IP address and port number in the IWAN domain for each device.

Step 1: Create the hub-site MC domain for each new VRF.

```
domain iwan
 vrf IoT-VRF-101
  master hub
   source-interface Loopback101
   site-prefixes prefix-list DC1-PREFIXES-101
   password c1sco123
   enterprise-prefix prefix-list ENTERPRISE-PREFIXES-101
   collector 10.4.48.36 port 9991
 vrf CONT-VRF-102
```

```
 master hub
  source-interface Loopback102
  site-prefixes prefix-list DC1-PREFIXES-102
  password c1sco123
  enterprise-prefix prefix-list ENTERPRISE-PREFIXES-102
  collector 10.4.48.36 port 9991
```

Step 2: Create the hub-site MC policy for each new VRF.

The policies use the PfR predefined templates. The path preference for voice, real time video, and low latency data is to use MPLS1 and MPLS2 unless the delay, jitter, and loss values on the path fall outside the values specified in the templates. The bulk data and default classes use INET1 and INET2 with fallback to MPLS1 and MPLS2, and the scavenger class uses INET1 and INET2 with fallback to blackhole. The rest of the traffic is load-balanced between the two paths.

Tech Tip

With this recommended policy, PfR does not manage Internetwork Control (DSCP CS6) traffic. CS6 traffic should always follow the normal routing path.

```
domain iwan
 vrf IoT-VRF-101
  master hub
   load-balance advanced
    path-preference INET1 INET2 fallback routing
   class VOICE sequence 10
    match dscp ef policy voice
    path-preference MPLS1 MPLS2 fallback INET1 INET2
    path-last-resort INET4G
   class REAL_TIME_VIDEO sequence 20
    match dscp cs4 policy real-time-video
    match dscp af41 policy real-time-video
    match dscp af42 policy real-time-video
    match dscp af43 policy real-time-video
    path-preference MPLS1 MPLS2 fallback INET1 INET2
   class LOW_LATENCY_DATA sequence 30
    match dscp cs2 policy low-latency-data
    match dscp cs3 policy low-latency-data
    match dscp af21 policy low-latency-data
    match dscp af22 policy low-latency-data
```

```
    match dscp af23 policy low-latency-data
    path-preference MPLS1 MPLS2 fallback INET1 next-fallback INET2
    path-last-resort INET4G
   class BULK_DATA sequence 40
    match dscp af11 policy bulk-data
    match dscp af12 policy bulk-data
    match dscp af13 policy bulk-data
    path-preference INET1 INET2 fallback MPLS1 MPLS2
   class SCAVENGER sequence 50
    match dscp cs1 policy scavenger
    path-preference INET1 INET2 fallback blackhole
   class DEFAULT sequence 60
    match dscp default policy best-effort
    path-preference INET1 INET2 fallback MPLS1 MPLS2
vrf CONT-VRF-102
  master hub
   load-balance advanced
    path-preference INET1 INET2 fallback routing
   class VOICE sequence 10
    match dscp ef policy voice
    path-preference MPLS1 MPLS2 fallback INET1 INET2
    path-last-resort INET4G
   class REAL_TIME_VIDEO sequence 20
    match dscp cs4 policy real-time-video
    match dscp af41 policy real-time-video
    match dscp af42 policy real-time-video
    match dscp af43 policy real-time-video
    path-preference MPLS1 MPLS2 fallback INET1 INET2
   class LOW_LATENCY_DATA sequence 30
    match dscp cs2 policy low-latency-data
    match dscp cs3 policy low-latency-data
    match dscp af21 policy low-latency-data
    match dscp af22 policy low-latency-data
    match dscp af23 policy low-latency-data
    path-preference MPLS1 MPLS2 fallback INET1 next-fallback INET2
    path-last-resort INET4G
```

```
class BULK_DATA sequence 40
 match dscp af11 policy bulk-data
 match dscp af12 policy bulk-data
 match dscp af13 policy bulk-data
 path-preference INET1 INET2 fallback MPLS1 MPLS2
class SCAVENGER sequence 50
 match dscp cs1 policy scavenger
 path-preference INET1 INET2 fallback blackhole
class DEFAULT sequence 60
 match dscp default policy best-effort
 path-preference INET1 INET2 fallback MPLS1 MPLS2
```

Procedure 4 Configure PfR domain in the hub-site BR

The hub-site BRs are also the DMVPN hub WAN aggregation routers for the network. The PfRv3 configurations for standalone BRs are much simpler because they dynamically learn their policy information from the hub-site MC. The hub-site BR routers are also used to advertise the path names and path-ids specified in the hub-site MC configuration.

Table 86 Hub-site BR path and IP addresses

Host name	VRF name	Tunnel ID	Path	Path ID	Local MC loopback IP address
DHY-M1I1-ASR1002X-1	Default VRF	100	MPLS1	1	10.6.32.251
	IoT-VRF-101	101			10.21.32.251
	CONT-VRF-102	102			10.25.32.251
	Default VRF	200	INET1	2	10.6.32.251
	IoT-VRF-101	201			10.21.32.251
	CONT-VRF-102	202			10.25.32.251
DHY-M1I1-ASR1002X-2	Default VRF	300	MPLS2	3	10.6.32.251
	IoT-VRF-101	301			10.21.32.251
	CONT-VRF-102	302			10.25.32.251
	Default VRF	400	INET2	4	10.6.32.251
	IoT-VRF-101	401			10.21.32.251
	CONT-VRF-102	402			10.25.32.251
	Default VRF	500	INET4G	5	10.6.32.251
	IoT-VRF-101	501			10.21.32.251
	CONT-VRF-102	502			10.25.32.251

Reader Tip

Whenever IWAN is designed with WAAS leveraging AppNav, please ensure that the Loopback IP address that is being used for PfR is not also used as the AppNav Service Controller address. This is applicable for any Hub IWAN router that is part of an AppNav Cluster.

Step 1: Create the hub-site BR domain for each new VRF. When using multiple VRFs, the border router monitor cache is shared across the VRFs and requires additional configuration. If you do not change the values, a warning message is displayed on the console. The recommended value for three VRFs is 33%, which is 100 divided by 3, but the value can be adjusted if the number of flows or amount of traffic is not equal between the VRFs. This example is the primary hub-site BR.

```
domain iwan
 vrf default
  border
   advanced
    monitor-cache-percent 33
vrf IoT-VRF-101
  border
   source-interface Loopback101
   master 10.21.32.251
   password c1sco123
   advanced
    monitor-cache-percent 33
 vrf CONT-VRF-102
  border
   source-interface Loopback102
   master 10.25.32.251
   password c1sco123
   advanced
    monitor-cache-percent 33
```

Step 2: Add the path names and path-ids to the tunnel interfaces of the hub-site BR.

This example is the primary hub-site BR using tunnels with MPLS as the provider for each VRF.

```
interface Tunnel101
 domain iwan path MPLS1 path-id 1
interface Tunnel102
 domain iwan path MPLS1 path-id 1
```

This example is the primary hub-site BR using tunnels with INET as the provider for each VRF.

```
interface Tunnel201
 domain iwan path INET1 path-id 2
interface Tunnel202
 domain iwan path INET1 path-id 2
```

Step 3: Verify the border is operational for VRFs IoT-VRF-101 and CONT-VRF-102 by using the **show domain [name] vrf [VRF name] border status** command.

```
DHY-M1I1-ASR1002X-1#show domain iwan vrf IoT-VRF-101 border status
DHY-M1I1-ASR1002X-1#show domain iwan vrf CONT-VRF-102 border status
```

Step 4: Repeat this procedure for each hub BR by using the appropriate path name and path-id.

Procedure 5 Verify PfR domain is operational on the hub-site MC

The PfR path names and path-ids are automatically discovered at the remote site routers from the configuration entered into the tunnel interfaces at the hub site. The hub-site MC uses the path names and path-ids to determine where traffic should be sent according to its policies.

Step 1: Verify the domain is operational from the hub-site MC using the **show domain [name] master status** command for VRFs IoT-VRF-101 and CONT-VRF-102.

```
DHY-MC-CSR1000v-1#show domain iwan vrf IoT-VRF-101 master status
DHY-MC-CSR1000v-1#show domain iwan vrf CONT-VRF-102 master status
```

PROCESS

Configuring the Transit-site Master Controller

1. Configure the IVRF definitions and loopbacks
2. Configure the connections to the transit-site WAN distribution switch
3. Configure the routing protocol on the LAN

This section describes configuring the PfR transit-site MC as a new router. Only the core relevant features are included.

Procedure 1 Configure the IVRF definitions and loopbacks

In this procedure, you configure the definitions for two VRFs and their associated loopbacks.

Step 1: Configure the VRFs.

```
vrf definition IoT-VRF-101
 rd 101:1

 address-family ipv4
 exit-address-family
```

```
vrf definition CONT-VRF-102
 rd 102:1

 address-family ipv4
 exit-address-family
```

Step 2: Configure the loopbacks.

```
interface Loopback101
 description IoT-VRF-101
 vrf forwarding IoT-VRF-101
 ip address 10.23.32.251 255.255.255.255
 hold-queue 1024 in
 hold-queue 1024 out

interface Loopback102
 description CONT-VRF-102
 vrf forwarding CONT-VRF-102
 ip address 10.27.32.251 255.255.255.255
 hold-queue 1024 in
 hold-queue 1024 out
```

Procedure 2 Configure the connections to the transit-site WAN distribution switch

In this procedure, you add the new port-channel sub-interfaces.

Step 1: Add the port-channel sub-interfaces.

```
interface Port-channel21.1100
 description IW-WAN-D3750X-T
 encapsulation dot1Q 1100
 ip address 10.8.32.151 255.255.255.224

interface Port-channel21.1101
 description IW-WAN-D3750X-T IoT-VRF-101
 description IoT-VRF-101
 encapsulation dot1Q 1101
 vrf forwarding IoT-VRF-101
```

```
 ip address 10.23.32.151 255.255.255.224

interface Port-channel21.1102
 description IW-WAN-D3750X-T CONT-VRF-102
 encapsulation dot1Q 1102
 vrf forwarding CONT-VRF-102
 ip address 10.27.32.151 255.255.255.224
```

Procedure 3 Configure the routing protocol on the LAN

Step 1: Configure OSPF for IoT-VRF-101 VRF.

```
router ospf 101 vrf IoT-VRF-101
 router-id 10.23.32.251
 capability vrf-lite
 passive-interface default
 no passive-interface Port-channel21.1101
 network 10.23.32.128 0.0.0.63 area 0
 network 10.23.32.251 0.0.0.0 area 0
```

Step 2: Configure OSPF for CONT-VRF-102 VRF.

```
router ospf 102 vrf CONT-VRF-102
 router-id 10.27.32.251
 capability vrf-lite
 passive-interface default
 no passive-interface Port-channel21.1102
 network 10.27.32.128 0.0.0.63 area 0
 network 10.27.32.251 0.0.0.0 area 0
```

PROCESS

Configuring PfR for Transit-site Location

1. Verify IP connectivity to remote site loopback interfaces
2. Configure prefixes for the enterprise and DC
3. Configure PfR domain in the transit-site MC
4. Configure PfR domain in the transit-site BR
5. Verify the PfR domain is operational on the transit-site MC

These procedures are similar to previously configured PfR for the hub-site location.

Procedure 1 Verify IP connectivity to remote site loopback interfaces

To verify the remote-site loopback interfaces reachabilities on the transit-site MC, in the previous process "Configuring PfR for the Hub-site Location," follow Procedure 1, "Verify IP connectivity to remote-site loopback interfaces."

Procedure 2 Configure prefixes for the enterprise and DC

Before the configuration of PfRv3 on the transit MC, you must create prefix lists for the DC. The enterprise-prefix list is only configured on the hub MC and you do not configure one on the transit MC.

The site-prefix range for the transit site includes the prefixes at this specific site, which is normally a WAN aggregation or DC site. Site-prefixes are typically statically defined at WAN aggregation and DC sites and discovered automatically at remote sites.

Tech Tip

PfR does not support the ip prefix-list options **ge** and **le**.

Step 1: Create the transit-site prefix list for each VRF.

```
ip prefix-list DC2-PREFIXES-101 seq 10 permit 10.4.0.0/16
ip prefix-list DC2-PREFIXES-101 seq 20 permit 10.8.0.0/16
ip prefix-list DC2-PREFIXES-101 seq 30 permit 10.23.0.0/16

ip prefix-list DC2-PREFIXES-102 seq 10 permit 10.4.0.0/16
ip prefix-list DC2-PREFIXES-102 seq 20 permit 10.8.0.0/16
ip prefix-list DC2-PREFIXES-102 seq 30 permit 10.27.0.0/16
```

Procedure 3 Configure PfR domain in the transit-site MC

Domain policies are configured on the hub MC. These policies are distributed to branch MCs and the transit MC by using the peering infrastructure. All sites that are in the same domain share the same set of PfR policies. The transit MC must peer to the hub MC to get the policy information.

Step 1: Update the transit-site MC domain for the new VRFs.

Example

```
domain iwan
 vrf IoT-VRF-101
  master transit 1
   source-interface Loopback101
   site-prefixes prefix-list DC2-PREFIXES-101
   password c1sco123
   hub 10.21.32.251
 vrf CONT-VRF-102
  master transit 1
   source-interface Loopback102
   site-prefixes prefix-list DC2-PREFIXES-102
   password c1sco123
   hub 10.25.32.251
```

Step 2: Verify the hub-site MC policy configuration is available by using the **show domain [name] master policy** command.

The output from this command should look the same as the output on the hub-site MC.

Procedure 4 Configure PfR domain in the transit-site BR

The transit-site BRs are also the DMVPN hub WAN aggregation routers for the transit-site network. The PfRv3 configurations for standalone BRs are much simpler because they dynamically learn their policy information from the transit-site MC. The transit-site BR routers are also used to advertise the path names and path-ids specified in the hub-site MC configuration.

Table 87 Transit-site BR path and IP addresses

Host name	VRF name	Tunnel ID	Path	Path ID	Local MC loopback IP address
DHY-M1I1-ASR1002X-T1	Default VRF	100	MPLS1	1	10.8.32.251
	IoT-VRF-101	101			10.23.32.251
	CONT-VRF-102	102			10.27.32.251
	Default VRF	200	INET1	2	10.8.32.251
	IoT-VRF-101	201			10.23.32.251
	CONT-VRF-102	202			10.27.32.251
DHY-M1I1-ASR1002X-T2	Default VRF	300	MPLS2	3	10.8.32.251
	IoT-VRF-101	301			10.23.32.251
	CONT-VRF-102	302			10.27.32.251
	Default VRF	400	INET2	4	10.8.32.251
	IoT-VRF-101	401			10.23.32.251
	CONT-VRF-102	402			10.27.32.251
	Default VRF	500	INET4G	5	10.8.32.251
	IoT-VRF-101	501			10.23.32.251
	CONT-VRF-102	502			10.27.32.251

Reader Tip

Whenever IWAN is designed with WAAS leveraging AppNav, please ensure that the Loopback IP address that is being used for PfR is not also used as the AppNav Service Controller address. This is applicable for any Hub IWAN router that is part of an AppNav Cluster.

Step 1: Update the transit-site BR domain for the new VRFs.

When using multiple VRFs, the border router monitor cache is shared across the VRFs and requires additional configuration. If you do not change the values, a warning message is displayed on the console. The recommended value for three VRFs is 33%, which is 100 divided by 3, but the value can be adjusted if the number of flows or amount of traffic is not equal between the VRFs.

This example is the primary transit-site BR.

```
domain iwan
 vrf default
  border
   advanced
    monitor-cache-percent 33
 vrf IoT-VRF-101
  border
   source-interface Loopback101
   master 10.23.32.251
   password c1sco123
   advanced
    monitor-cache-percent 33
 vrf CONT-VRF-102
  border
   source-interface Loopback102
   master 10.27.32.251
   password c1sco123
   advanced
    monitor-cache-percent 33
```

Step 2: Add the path names and path-ids to the tunnel interfaces of the transit-site BR.

This example is the primary transit-site BR using tunnels with MPLS as the provider for each VRF.

```
interface Tunnel101
 domain iwan path MPLS1 path-id 1
interface Tunnel102
 domain iwan path MPLS1 path-id 1
```

This example is the primary transit-site BR using tunnels with INET as the provider for each VRF.

```
interface Tunnel201
 domain iwan path INET1 path-id 2
interface Tunnel202
 domain iwan path INET1 path-id 2
```

Step 3: Verify the border is operational for VRFs IoT-VRF-101 and CONT-VRF-102 by using the **show domain [name] vrf [VRF name] border status** command.

```
DHY-M1I1-ASR1002X-T1#show domain iwan vrf IoT-VRF-101 border status
DHY-M1I1-ASR1002X-T1#show domain iwan vrf CONT-VRF-102 border status
```

Step 4: Repeat this procedure for each transit BR by using the appropriate path name and path-id.

Procedure 5 Verify the PfR domain is operational on the transit-site MC

The PfR path names and path-ids are automatically discovered at the remote site routers from the configuration entered into the tunnel interfaces at the hub and transit sites. The hub-site MC uses the path names and path-ids to determine where traffic should be sent according to its policies.

Step 1: Verify the domain is operational from the transit-site MC by using the **show domain [name] master status** command for VRFs IoT-VRF-101 and CONT-VRF-102.

```
DHY-MC-ASR1002X-T1#show domain iwan vrf IoT-VRF-101 master status
DHY-MC-ASR1002X-T1#show domain iwan vrf CONT-VRF-102 master status
```

PROCESS

Configuring PfR for Remote Site Locations

1. Verify IP connectivity to hub MC loopback interface
2. Configure PfR in the primary remote site router
3. Configure PfR in the secondary remote site router
4. Verify PfR traffic classes are controlled

Remote sites are discovered using peering. Each remote site MC peers with the hub MC. The remote site MC advertises local site information and learns information about every other site. Prefixes specific to sites are advertised along with the site-id. The site-prefix to site-id mapping is used in monitoring and optimization. This mapping is also used for creating reports for specific sites.

WAN interfaces at each site are discovered using a special probing mechanism referred to as smart probes. This further reduces provisioning on the remote sites. The WAN interface discovery also creates mapping of the interface to a particular service provider. The mapping is used in monitoring and optimization.

Procedure 1 Verify IP connectivity to hub MC loopback interface

PfRv3 requires loopback interfaces for the peering traffic between the BR and MC routers. For this design, you put the hub MC loop back interface into the subnet range of the hub location. The following table shows the loopback addresses for the hub MC.

Table 88 Hub MC loopback IP addresses

VRF name	Loopback interface	Loopback IP address
Default VRF	Loopback 0	10.6.32.251
IoT-VRF-101	Loopback 101	10.21.32.251
CONT-VRF-102	Loopback 102	10.25.32.251

Each remote site must have a route to the hub over each exit path. You can have more than two paths. You can also have two routes and Equal Cost Multiple Paths.

Step 1: Verify that there are at least two available paths to the loopback 0 interface on the hub MC from each remote site router by using the **show ip bgp [Hub MC Loopback address]** command.

```
RS32-4451X-1#show ip bgp 10.6.32.251
BGP routing table entry for 10.6.32.251/32, version 340
Paths: (6 available, best #5, table default)
  Not advertised to any peer
  Refresh Epoch 2
  Local
    10.6.44.1 from 10.6.44.1 (10.6.32.242)
      Origin IGP, metric 3, localpref 760, weight 50000, valid, internal
      Community: 65100:500
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 2
  Local, (received-only)
    10.6.44.1 from 10.6.44.1 (10.6.32.242)
      Origin IGP, metric 3, localpref 760, valid, internal
      Community: 65100:500
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 2
  Local
    10.6.36.1 from 10.6.36.1 (10.6.32.241)
      Origin IGP, metric 3, localpref 780, weight 50000, valid, internal
      Community: 65100:200
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 2
  Local, (received-only)
    10.6.36.1 from 10.6.36.1 (10.6.32.241)
      Origin IGP, metric 3, localpref 780, valid, internal
      Community: 65100:200
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 2
  Local
    10.6.34.1 from 10.6.34.1 (10.6.32.241)
      Origin IGP, metric 3, localpref 800, weight 50000, valid, internal, best
```

```
      Community: 65100:100
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 2
  Local, (received-only)
    10.6.34.1 from 10.6.34.1 (10.6.32.241)
      Origin IGP, metric 3, localpref 800, valid, internal
      Community: 65100:100
      rx pathid: 0, tx pathid: 0
```

Step 2: Repeat this procedure to verify the available path for each VRF.

Procedure 2 Configure PfR in the primary remote site router

Each remote site must have a branch MC and branch BR configured. At dual-router sites it is recommended that you configure the primary router as both an MC and BR and the secondary router as only a BR. The domain name, VRF, and password must match the hub MC configuration. Use the respective loopback interfaces as the source for each VRFs. Configure the hub MC IP address.

Reader Tip

Whenever IWAN is designed with WAAS leveraging AppNav/WCCP, please ensure that the Loopback IP address that is being used for PfR is not also used as the AppNav Service Controller address or WCCP router ID. This is applicable for any Branch IWAN router that is part of an AppNav/WCCP Cluster.

Step 1: If you are not on the router console port, turn on terminal monitoring with the **terminal monitor** command from the global command line interface.

```
terminal monitor
```

Step 2: Update the branch MC domain for the new VRFs. This example configures the branch MC and points to the IP address of the hub MC in the associated VRF of the IWAN dual hybrid design model.

```
domain iwan
 vrf IoT-VRF-101
  master branch
   source-interface Loopback101
   password c1sco123
   hub 10.21.32.251
 vrf CONT-VRF-102
  master branch
   source-interface Loopback102
   password c1sco123
   hub 10.25.32.251
```

Step 3: After approximately two minutes, the console displays an EIGRP SAF message similar to the one below, which indicates the branch MC has created an adjacency with the loopback interface of the hub MC.

```
Sep 16 14:16:00.389: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.6.32.251
(Loopback0) is up: new adjacency
```

```
Jun 16 11:37:15.811: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.6.32.251
(Loopback0) is up: new adjacency
Jun 16 11:37:15.954: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.21.32.251
(Loopback101) is up: new adjacency
Jun 16 11:37:16.101: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.25.32.251
(Loopback102) is up: new adjacency
```

Step 4: Verify the PfR policy from the hub MC has been propagated to the branch MC by using the **show domain [name]** master policy command.

```
RS32-4451X-1#show domain iwan vrf IoT-VRF-101 master policy
RS32-4451X-1#show domain iwan vrf CONT-VRF-102 master policy
```

The output from this command should look the same as the output on the hub MC.

Step 5: Enable the BR function.

When using multiple VRFs, the border router monitor cache is shared across the VRFs and requires additional configuration. If you do not change the values, a warning message is displayed on the console. The recommended value for three VRFs is 33%, which is 100 divided by 3, but the value can be adjusted if the number of flows or amount of traffic is not equal between the VRFs.

This example configures the branch BR and points it to the local branch MC, which is running on the same router platform.

```
domain iwan
 vrf default
  border
   advanced
    monitor-cache-percent 33
 vrf IoT-VRF-101
  border
   source-interface Loopback101
   master local
   password c1sco123
   advanced
    monitor-cache-percent 33
vrf CONT-VRF-102
  border
```

```
source-interface Loopback102
master local
password c1sco123
advanced
 monitor-cache-percent 33
```

Step 6: After approximately thirty seconds, the console displays a line protocol up/down message similar to the one below, which indicates the automatically generated tunnel interface has been created.

```
Jun 16 11:46:26.674: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
Jun 16 11:46:44.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1,
changed state to up
Jun 16 11:46:44.708: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2,
changed state to up
```

Step 7: Verify that the branch BR is operational by using the **show domain [name] vrf [VRF name] border status** command for non-default VRFs.

```
RS32-4451X-1#show domain iwan vrf IoT-VRF-101 border status
RS32-4451X-1#show domain iwan vrf IoT-VRF-101 border status
```

Step 8: Verify that the branch MC is operational by using **the show domain [name] vrf [VRF name] master status** command for non-default VRFs.

Procedure 3 Configure PfR in the secondary remote site router

Use this procedure only when there is a secondary remote site router. If you have a single router at a remote location, skip this procedure.

PfRv3 requires loopback interfaces for the peering traffic between the BR and MC routers. For this design, you put the hub MC loop back interface into the subnet range of the hub location. Each remote site must have a route to the hub MC in the BGP routing table over each exit path. You can have more than two paths. You can also have two routes and Equal Cost Multiple Paths.

Reader Tip

Whenever IWAN is designed with WAAS leveraging AppNav/WCCP, please ensure that the Loopback IP address that is being used for PfR is not also used as the AppNav Service Controller address or WCCP router ID. This is applicable for any Branch IWAN router that is part of an AppNav/WCCP Cluster

Step 1: Verify that there are at least two available paths to the loopback 0 interface on the hub MC from each remote site router by using the **show ip bgp [Hub MC Loopback address]** command.

```
RS32-4451X-2#show ip bgp 10.6.32.251
```

Step 2: Repeat the previous step to verify the available path for each VRF.

Step 3: Enable the BR function.

When using multiple VRFs, the border router monitor cache is shared across the VRFs and requires additional configuration. If you do not change the values, a warning message is displayed on the console. The recommended value for three VRFs is 33%, which is 100 divided by 3, but the value can be adjusted if the number of flows or amount of traffic is not equal between the VRFs.

```
domain iwan
 vrf default
  border
   advanced
    monitor-cache-percent 33
```

This example configures the branch BR and points it to the branch MC, which is running on the primary remote site router.

```
domain iwan
 vrf default
  border
   advanced
    monitor-cache-percent 33
 vrf IoT-VRF-101
  border
   source-interface Loopback101
   master 10.201.241.32
   password c1sco123
   advanced
    monitor-cache-percent 33
 vrf CONT-VRF-102
  border
   source-interface Loopback102
   master 10.202.241.32
   password c1sco123
   advanced
    monitor-cache-percent 33
```

Step 4: After approximately thirty seconds, the console displays several EIGRP messages and a line protocol up/down message similar to those shown below. These messages indicate the branch BR has neighbored with the branch MC and automatically generated the tunnel interface from the loopback of the branch BR to the loopback of the branch MC.

```
Jun 16 11:48:36.831: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.26.144.9
(GigabitEthernet0/0/2.512) is up: new adjacency

Jun 16 11:48:36.832: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.26.146.2
(GigabitEthernet0/0/2.522) is up: new adjacency

Jun 16 11:48:36.832: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.26.147.2
(GigabitEthernet0/0/2.532) is up: new adjacency

Jun 16 11:48:36.832: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.202.241.32
(Loopback102) is up: new adjacency

Jun 16 11:48:37.613: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up

Jun 16 11:48:43.344: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.22.144.9
(GigabitEthernet0/0/2.511) is up: new adjacency

Jun 16 11:48:43.344: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.22.146.2
(GigabitEthernet0/0/2.521) is up: new adjacency

Jun 16 11:48:43.344: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.22.147.2
(GigabitEthernet0/0/2.531) is up: new adjacency

Jun 16 11:48:43.344: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.201.241.32
(Loopback101) is up: new adjacency

Jun 16 11:48:44.126: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1,
changed state to up

Jun 16 11:48:58.540: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.7.146.2
(GigabitEthernet0/0/2.64) is up: new adjacency

Jun 16 11:48:58.540: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.7.147.2
(GigabitEthernet0/0/2.69) is up: new adjacency

Jun 16 11:48:58.540: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.6.38.2
(Tunnel300) is up: new adjacency

Jun 16 11:48:58.540: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.6.40.2
(Tunnel400) is up: new adjacency

Jun 16 11:48:58.541: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.7.144.9
(GigabitEthernet0/0/2.99) is up: new adjacency

Jun 16 11:48:58.541: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.255.241.32
(Loopback0) is up: new adjacency

Jun 16 11:48:59.324: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2,
changed state to up
```

Step 5: Verify that the branch BR is operational by using the **show domain [name] vrf [VRF name] border status** command for non-default VRFs.

Step 6: Repeat Procedure 1 through Procedure 3 for each remote site in your network.

Procedure 4 Verify PfR traffic classes are controlled

The final procedure is to verify that the configured and default traffic classes are controlled by the MC at the hub and branch locations.

For more information about verifying PfR traffic classes, see the main Intelligent WAN Deployment Guide.

Deploying IWAN Quality of Service

QoS has already proven itself as the enabling technology for the convergence of voice, video, and data networks. As business needs evolve, so do demands on QoS technologies. The need to protect voice, video and critical data with QoS mechanisms is extremely important on the WAN because access speeds are much lower than the LAN networks that feed them.

PROCESS

Applying DMVPN QoS Policy to DMVPN Hub Routers

1. Configure per-tunnel QoS policies for DMVPN hub router
2. Configure per-tunnel QoS NHRP policies on DMVPN hub router

For multi-VRF deployments, the QoS configuration has to take into account each tunnel sending traffic to the same remote site router at the same time. In a multi-VRF environment, the following rules are applied:

- Total bandwidth for VRFs should not exceed 200% of remote-site inbound service rate, because oversubscription traffic will be dropped in the SP cloud.
- Bandwidth does not have to be divided equally between VRFs.
- QoS policies do not have to be the same per VRF.
- Bandwidth for guest traffic is normally about half the value of employee traffic.
- Bandwidth for low volume VRFs such as IoT and PCI should use a much smaller percentage, closer to one-tenth the value of employee traffic.
- As the number of VRFs increases, the percentages need to come down accordingly based on the network administrators' knowledge of their traffic patterns.

This process applies only to DMVPN WAN aggregation routers.

Procedure 1 Configure per-tunnel QoS policies for DMVPN hub router

The QoS policy on a tunnel instance allows you to shape the tunnel traffic to individual spokes and to differentiate between traffic classes within the tunnel for appropriate treatment.

The QoS policy on the tunnel instance is defined and applied only to the DMVPN hub routers at the central site. The remote-site router signals the QoS group policy information to the hub router with a command in the NHRP configuration, which greatly reduces QoS configuration and complexity. The hub router applies the signaled policy in the egress direction for each remote site.

In the example below, configure the default VRF traffic at 80% of the remote site inbound service rate bandwidth, the IoT VRF at 10% of the bandwidth, and the contractor VRF at 80% of the bandwidth.

The **bandwidth remaining ratio** command is used to provide each site with their fair share of the remaining bandwidth when the outbound interface is experiencing congestion. If you do not use this command, the lower-bandwidth sites get all of their assigned bandwidth, while the higher bandwidth sites get less than their fair share.

In the example below, divide the shape average bandwidth by 1 Mbps to come up with the value for the ratio. If you have sites with less than 5 Mbps of shape average bandwidth, you should divide the shape average for all of your sites by 100 Kbps to ensure they all get a reasonable ratio greater than 1.

Tech Tip

With Per-Tunnel QoS for DMVPN, the queuing and shaping is performed at the outbound physical interface for the GRE/IPsec tunnel packets. This means that the GRE header, the IPsec header and the layer2 (for the physical interface) header are included in the packet-size calculations for shaping and bandwidth queuing of packets under QoS. The values in the table are examples; make sure to adjust these values for your specific needs and remote-site bandwidth provisioned with your ISP.

Table 89 Per-tunnel QoS policies with 80% employee, 10% IoT and 80% contractor

Policy name	Class	Bandwidth bps	Bandwidth remaining ratio
RS-GROUP-300MBPS-80-POLICY	Class-default	240000000	240
RS-GROUP-200MBPS-80-POLICY	Class-default	160000000	160
RS-GROUP-100MBPS-80-POLICY	Class-default	80000000	80
RS-GROUP-50MBPS-80-POLICY	Class-default	40000000	40
RS-GROUP-30MBPS-80-POLICY	Class-default	24000000	24
RS-GROUP-20MBPS-80-POLICY	Class-default	16000000	16
RS-GROUP-10MBPS-80-POLICY	Class-default	8000000	8
RS-GROUP-4G-80-POLICY	Class-default	6000000	6
RS-GROUP-300MBPS-10-POLICY-VRF101	Class-default	30000000	30
RS-GROUP-200MBPS-10-POLICY-VRF101	Class-default	20000000	20
RS-GROUP-100MBPS-10-POLICY-VRF101	Class-default	10000000	10
RS-GROUP-50MBPS-10-POLICY-VRF101	Class-default	5000000	5
RS-GROUP-30MBPS-10-POLICY-VRF101	Class-default	3000000	3
RS-GROUP-20MBPS-10-POLICY-VRF101	Class-default	2000000	2
RS-GROUP-10MBPS-10-POLICY-VRF101	Class-default	1000000	1
RS-GROUP-4G-10-POLICY-VRF101	Class-default	2000000	2
RS-GROUP-300MBPS-80-POLICY-VRF102	Class-default	240000000	240
RS-GROUP-200MBPS-80-POLICY-VRF102	Class-default	160000000	160
RS-GROUP-100MBPS-80-POLICY-VRF102	Class-default	80000000	80
RS-GROUP-50MBPS-80-POLICY-VRF102	Class-default	40000000	40
RS-GROUP-30MBPS-80-POLICY-VRF102	Class-default	24000000	24
RS-GROUP-20MBPS-80-POLICY-VRF102	Class-default	16000000	16
RS-GROUP-10MBPS-80-POLICY-VRF102	Class-default	8000000	8
RS-GROUP-4G-80-POLICY-VRF102	Class-default	6000000	6

Step 1: Create policy.

```
policy-map [policy-map-name]
```

Step 2: Define a shaper and bandwidth remaining ratio for the default-class and apply the **WAN** QoS queuing child service policy created in Procedure 2, "Create policy map with queuing policy."

The shape average value is entered in bits per second (bps). If all of your bandwidth values are greater than 5 Mbps, enter the bandwidth remaining ratio as shape average bandwidth/1 Mbps. If any of your bandwidth values are 5 Mbps or less, enter the bandwidth remaining ratio as shape average bandwidth/100 Kbps.

```
policy-map [policy-map-name]
 description [percentage] of inbound service rate
 class class-default
 shape average [bandwidth (bps)]
 bandwidth remaining ratio [shape average bandwidth/1 Mbps]
  service-policy [policy-map name]
```

Step 3: For each remote-site type, repeat steps 1 and 2.

Example: Hub border router

```
policy-map RS-GROUP-300MBPS-80-POLICY
 description 80% of inbound service rate
 class class-default
  shape average 240000000
  bandwidth remaining ratio 240
   service-policy WAN
policy-map RS-GROUP-200MBPS-80-POLICY
 description 80% of inbound service rate
 class class-default
  shape average 160000000
  bandwidth remaining ratio 160
   service-policy WAN
policy-map RS-GROUP-100MBPS-80-POLICY
 description 80% of inbound service rate
 class class-default
  shape average 80000000
  bandwidth remaining ratio 80
   service-policy WAN
policy-map RS-GROUP-50MBPS-80-POLICY
 description 80% of inbound service rate
```

```
 class class-default
  shape average 40000000
  bandwidth remaining ratio 40
   service-policy WAN
policy-map RS-GROUP-30MBPS-80-POLICY
 description 80% of inbound service rate
 class class-default
  shape average 24000000
  bandwidth remaining ratio 24
   service-policy WAN
policy-map RS-GROUP-20MBPS-80-POLICY
 description 80% of inbound service rate
 class class-default
  shape average 16000000
  bandwidth remaining ratio 16
   service-policy WAN
policy-map RS-GROUP-10MBPS-80-POLICY
 description 80% of inbound service rate
 class class-default
  shape average 8000000
  bandwidth remaining ratio 8
   service-policy WAN
policy-map RS-GROUP-4G-80-POLICY
 description 80% of inbound service rate
 class class-default
  shape average 6000000
  bandwidth remaining ratio 6
   service-policy WAN
policy-map RS-GROUP-300MBPS-10-POLICY-VRF101
 description 10% of inbound service rate
 class class-default
  shape average 30000000
  bandwidth remaining ratio 30
   service-policy WAN
policy-map RS-GROUP-200MBPS-10-POLICY-VRF101
 description 10% of inbound service rate
```

```
 class class-default
  shape average 20000000
  bandwidth remaining ratio 20
   service-policy WAN
policy-map RS-GROUP-100MBPS-10-POLICY-VRF101
 description 10% of inbound service rate
 class class-default
  shape average 10000000
  bandwidth remaining ratio 10
   service-policy WAN
policy-map RS-GROUP-50MBPS-10-POLICY-VRF101
 description 10% of inbound service rate
 class class-default
  shape average 5000000
  bandwidth remaining ratio 5
   service-policy WAN
policy-map RS-GROUP-30MBPS-10-POLICY-VRF101
 description 10% of inbound service rate
 class class-default
  shape average 3000000
  bandwidth remaining ratio 3
   service-policy WAN
policy-map RS-GROUP-20MBPS-10-POLICY-VRF101
 description 10% of inbound service rate
 class class-default
  shape average 2000000
  bandwidth remaining ratio 2
   service-policy WAN
policy-map RS-GROUP-10MBPS-10-POLICY-VRF101
 description 10% of inbound service rate
 class class-default
  shape average 1000000
  bandwidth remaining ratio 1
   service-policy WAN
policy-map RS-GROUP-4G-10-POLICY-VRF101
 description 10% of inbound service rate
```

```
 class class-default
  shape average 2000000
  bandwidth remaining ratio 2
   service-policy WAN
policy-map RS-GROUP-300MBPS-80-POLICY-VRF102
 description 80% of inbound service rate
 class class-default
  shape average 240000000
  bandwidth remaining ratio 240
   service-policy WAN
policy-map RS-GROUP-200MBPS-80-POLICY-VRF102
 description 80% of inbound service rate
 class class-default
  shape average 160000000
  bandwidth remaining ratio 160
   service-policy WAN
policy-map RS-GROUP-100MBPS-80-POLICY-VRF102
 description 80% of inbound service rate
 class class-default
  shape average 80000000
  bandwidth remaining ratio 80
   service-policy WAN
policy-map RS-GROUP-50MBPS-80-POLICY-VRF102
 description 80% of inbound service rate
 class class-default
  shape average 40000000
  bandwidth remaining ratio 40
   service-policy WAN
policy-map RS-GROUP-30MBPS-80-POLICY-VRF102
 description 80% of inbound service rate
 class class-default
  shape average 24000000
  bandwidth remaining ratio 24
   service-policy WAN
policy-map RS-GROUP-20MBPS-80-POLICY-VRF102
 description 80% of inbound service rate
```

```
 class class-default
  shape average 16000000
  bandwidth remaining ratio 16
   service-policy WAN
policy-map RS-GROUP-10MBPS-80-POLICY-VRF102
 description 80% of inbound service rate
 class class-default
  shape average 8000000
  bandwidth remaining ratio 8
   service-policy WAN
policy-map RS-GROUP-4G-80-POLICY-VRF102
 description 80% of inbound service rate
 class class-default
  shape average 6000000
  bandwidth remaining ratio 6
   service-policy WAN
```

Procedure 2 Configure per-tunnel QoS NHRP policies on DMVPN hub router

The QoS policy that the hub uses for a particular endpoint or spoke is selected by the NHRP group in which the spoke is configured.

Prerequisites and important caveats:

- DMVPN must be fully configured and operational before you can configure an NHRP group on a spoke or map the NHRP group to a QoS policy on a hub.
- Although you may configure multiple spokes as part of the same NHRP group, the tunnel traffic for each spoke is measured individually for shaping and policing.
- Only output NHRP policies are supported. These apply to per-site traffic egressing the router towards the WAN.

Step 1: Create NHRP group policy name mapping and apply the policies configured in the previous procedure to the DMVPN tunnel interface on the hub router.

```
interface tunnel[number]
 ip nhrp map group [NHRP GROUP Policy Name] service-policy output [policy-map
name]
```

Example: Hub border router

```
interface Tunnel100
 ip nhrp map group RS-GROUP-300MBPS-80 service-policy output RS-GROUP-300MBPS-80-POLICY
 ip nhrp map group RS-GROUP-200MBPS-80 service-policy output RS-GROUP-200MBPS-80-POLICY
 ip nhrp map group RS-GROUP-100MBPS-80 service-policy output RS-GROUP-100MBPS-80-POLICY
 ip nhrp map group RS-GROUP-50MBPS-80 service-policy output RS-GROUP-50MBPS-80-POLICY
 ip nhrp map group RS-GROUP-30MBPS-80 service-policy output RS-GROUP-30MBPS-80-POLICY
 ip nhrp map group RS-GROUP-20MBPS-80 service-policy output RS-GROUP-20MBPS-80-POLICY
 ip nhrp map group RS-GROUP-10MBPS-80 service-policy output RS-GROUP-10MBPS-80-POLICY
 ip nhrp map group RS-GROUP-4G-80 service-policy output RS-GROUP-4G-80-POLICY

interface Tunnel101
 ip nhrp map group RS-GROUP-300MBPS-10-VRF101 service-policy output RS-GROUP-300MBPS-10-POLICY-VRF101
 ip nhrp map group RS-GROUP-200MBPS-10-VRF101 service-policy output RS-GROUP-200MBPS-10-POLICY-VRF101
 ip nhrp map group RS-GROUP-100MBPS-10-VRF101 service-policy output RS-GROUP-100MBPS-10-POLICY-VRF101
 ip nhrp map group RS-GROUP-50MBPS-10-VRF101 service-policy output RS-GROUP-50MBPS-10-POLICY-VRF101
 ip nhrp map group RS-GROUP-30MBPS-10-VRF101 service-policy output RS-GROUP-30MBPS-10-POLICY-VRF101
 ip nhrp map group RS-GROUP-20MBPS-10-VRF101 service-policy output RS-GROUP-20MBPS-10-POLICY-VRF101
 ip nhrp map group RS-GROUP-10MBPS-10-VRF101 service-policy output RS-GROUP-10MBPS-10-POLICY-VRF101
 ip nhrp map group RS-GROUP-4G-10-VRF101 service-policy output RS-GROUP-4G-10-POLICY-VRF101

interface Tunnel102
 ip nhrp map group RS-GROUP-300MBPS-80-VRF102 service-policy output RS-GROUP-300MBPS-80-POLICY-VRF102
 ip nhrp map group RS-GROUP-200MBPS-80-VRF102 service-policy output RS-GROUP-200MBPS-80-POLICY-VRF102
```

```
ip nhrp map group RS-GROUP-100MBPS-80-VRF102 service-policy output RS-GROUP-100MBPS-80-POLICY-VRF102

ip nhrp map group RS-GROUP-50MBPS-80-VRF102 service-policy output RS-GROUP-50MBPS-80-POLICY-VRF102

ip nhrp map group RS-GROUP-30MBPS-80-VRF102 service-policy output RS-GROUP-30MBPS-80-POLICY-VRF102

ip nhrp map group RS-GROUP-20MBPS-80-VRF102 service-policy output RS-GROUP-20MBPS-80-POLICY-VRF102

ip nhrp map group RS-GROUP-10MBPS-80-VRF102 service-policy output RS-GROUP-10MBPS-80-POLICY-VRF102

ip nhrp map group RS-GROUP-4G-80-VRF101 service-policy output RS-GROUP-4G-80-POLICY-VRF101
```

PROCESS

Applying QoS Configurations to Remote Site Routers

1. Configure per-tunnel QoS NHRP policy on remote-site routers
2. Verify QoS policy on physical interfaces of remote site router
3. Verify DMVPN per-tunnel QoS from hub routers

This process completes the remote-site QoS configuration and applies to all DMVPN spoke routers.

Procedure 1 Configure per-tunnel QoS NHRP policy on remote-site routers

This procedure configures the remote-site router to reference the QoS policy configured on the hub site routers.

Step 1: Apply the NHRP group policy to the DMVPN tunnel interface on the corresponding remote-site router. Use the NHRP group name as defined on the hub router in Procedure 2, "Configure per tunnel QoS policies for DMVPN hub router," above.

Configure the bandwidth statement on the interface to match the outbound service rate. Even though we are shaping from the hub site to a lower percentage of bandwidth, configure the bandwidth receive statement on the interface to match the inbound service rate and the NHRP group policy chosen. The bandwidth value is entered in kilobits per second (Kbps).

```
interface Tunnel[value]
 bandwidth [outbound service rate value in Kbps]
 bandwidth receive [inbound service rate value in Kbps]
 ip nhrp group [NHRP GROUP Policy Name]
```

Example: Remote site router with dual-link for hybrid

This example shows a remote-site using a 16 Mbps policy and a 40 Mbps policy on default VRF and IoT-VRF-102. A 2 Mbps policy and a 5 Mbps policy are being used on CONT-VRF-101.

```
interface Tunnel100
 bandwidth 20000
 bandwidth receive 20000
 ip nhrp group RS-GROUP-20MBPS-80
interface Tunnel101
 bandwidth 20000
 bandwidth receive 20000
 ip nhrp group RS-GROUP-20MBPS-10-VRF101
interface Tunnel102
 bandwidth 20000
 bandwidth receive 20000
 ip nhrp group RS-GROUP-20MBPS-80-VRF102
interface Tunnel200
 bandwidth 50000
 bandwidth receive 50000
 ip nhrp group RS-GROUP-50MBPS-80
interface Tunnel201
 bandwidth 50000
 bandwidth receive 50000
 ip nhrp group RS-GROUP-50MBPS-10-VRF101
interface Tunnel202
 bandwidth 50000
 bandwidth receive 50000
 ip nhrp group RS-GROUP-50MBPS-80-VRF102
```

Procedure 2 Verify QoS policy on physical interfaces of remote site router

After all of the physical interfaces on a router are configured, you can verify each one before moving to the next remote site.

Step 1: Verify the QoS output policy on each interface is correct by using the **show policy-map interface** command.

Step 2: Repeat the previous step for each interface configured with QoS.

Tech Tip

If you experience tail-drops in your class class-default, a potential work-around is to increase the size of the queue-limit.

On an interface with bandwidth of less than 15 Mbps, the default queue-limit is 64 packets. Increasing this value adds latency to the traffic in the default-class but also reduces the number of tail-drops.

```
policy-map WAN
 class class-default
  queue-limit 512 packets
```

Procedure 3 Verify DMVPN per-tunnel QoS from hub routers

After the all of the DMVPN routers are configured for Per-Tunnel QoS, you can verify the configurations from the hub router.

Step 1: Verify the Per-Tunnel QoS output policy to each remote-site is correct by using the **show dmvpn detail** command.

Step 2: Repeat the previous step for each DMVPN hub router.

Appendix A: Product List

To view the full list of IWAN-supported routers for this version of the CVD, see Supported Cisco Platforms and Software Releases. All master controllers and border router devices at a common site must use the same version of software.

This guide was validated using the software detailed in this appendix. When deploying, you should always use the Cisco IOS Software Checker tool to see if there are software vulnerabilities applicable for your environment. This tool is available at the following location:

https://tools.cisco.com/security/center/selectIOSVersion.x

Appendix B: Crypto Configurations

These steps in this appendix are common for different router types. Please confirm each section matches the router type you are deploying before proceeding.

CONFIGURING IKEV2 AND IPSEC FOR A DMVPN BORDER ROUTER

This section is for DMVPN border routers only.

In multi-VRF deployment, all tunnels with the same tunnel source interface must use the same IPsec profile and must have the **tunnel protection shared** command configured. For example, if tunnels 100 through 102 uses GigabitEthernet0/0 as their tunnel source and tunnels 200 through 202 uses GigabitEthernet0/1, then define the profile DMVPN-IPSEC-PROFILE-MPLS1 for tunnels 100 through 102 and DMVPN-IPSEC-PROFILE-INET1 for tunnels 200 through 202.

The crypto configurations have been simplified in this version of the guide in order to minimize the variations from previous guides.

Table 90 Crypto parameters

Parameter	Pre-Shared Keys
crypto ikev2 keyring	DMVPN-KEYRING
crypto ikev2 profile	DMVPN-IKEv2-PROFILE
crypto ipsec profile	DMVPN-IPSEC-PROFILE-[transport name]

IPsec uses a key exchange between the routers in order to encrypt/decrypt the traffic. These keys are exchanged using pre-shared keys.

Configuring IKEv2 and IPsec with pre-shared keys

Step 1: Configure the crypto keyring for pre-shared keys.

The crypto keyring defines a pre-shared key (or password) valid for IP sources that are reachable within a particular VRF. This key is a wildcard pre-shared key if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 as the network/mask combination.

```
crypto ikev2 keyring [keyring name]
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key [password]
```

Example

```
crypto ikev2 keyring DMVPN-KEYRING
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key c1sco123
```

Step 2: Configure the IKEv2 proposal.

The user-defined IKEv2 proposal includes only the following:

- Encryption with AES cipher and a 256-bit key
- Pseudo-random function with SHA and a 512-bit digest
- Diffie-Hellman group: 19

```
crypto ikev2 proposal [proposal name]
 encryption [encryption algorithm]
 prf [pseudo-random function algorithm]
 group [Diffie-Hellman group]
```

Example

```
crypto ikev2 proposal AES/GCM/256
 encryption aes-gcm-256
 prf sha512
 group 19
```

The default IKEv2 proposal is also used.

A **show crypto ikev2 proposal** displays the details of the two proposals.

```
show crypto ikev2 proposal
 IKEv2 proposal: AES/GCM/256
      Encryption : AES-GCM-256
      Integrity  : none
      PRF        : SHA512
      DH Group   : DH_GROUP_256_ECP/Group 19
 IKEv2 proposal: default
      Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
      Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
      PRF        : SHA512 SHA384 SHA256 SHA1 MD5
      DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Step 3: Configure the IKEv2 policy.

The crypto policy includes the proposal you created in the previous step. This policy matches any FVRF defined on the router.

```
crypto ikev2 policy [policy name]
 match fvrf any
 proposal [proposal name]
```

Example

```
crypto ikev2 policy AES/GCM/256
 match fvrf any
 proposal AES/GCM/256
```

The default IKEv2 policy is also used.

A **show crypto ikev2 policy** displays the details of the two policies.

```
show crypto ikev2 policy
 IKEv2 policy : AES/GCM/256
      Match fvrf : any
      Match address local : any
      Proposal    : AES/GCM/256

 IKEv2 policy : default
      Match fvrf : any
      Match address local : any
      Proposal    : default
```

Step 4: Configure the IKEv2 profile.

The IKEv2 profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0. The **identity local address** must match the loopback address of this router.

Tech Tip

Identity local address is needed for customers who use Carrier Grade NAT (CGN) which requires a unique identity per remote site router even if the same pre-NAT IP address is used for other locations. The command does not affect customers who are not using CGN, so it is a recommended best practice to use the command all of the time.

The profile also defines what method of key sharing are used on this router with **authentication local** and what methods are accepted from remote locations with **authentication remote**. The **pre-share** keyword is used with the keyring defined above.

```
crypto ikev2 profile [profile name]
 description [profile description]
 match fvrf [vrf name]
 match identity remote address [IP address]
 identity local address [Loopback IP address of this router]
 authentication remote pre-share
 authentication local pre-share
 keyring local [keyring name]
```

Example: MPLS1 hub border router–HY-MPLS1-ASR1002X-1

```
crypto ikev2 profile DMVPN-IKEv2-PROFILE
 description PSK Profile
 match fvrf any
 match identity remote address 0.0.0.0
 identity local address 10.6.32.241
 authentication local pre-share
 authentication remote pre-share
 keyring local DMVPN-KEYRING
```

Step 5: Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit GCM encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set [transform set] esp-gcm 256
 mode transport
```

Example

```
crypto ipsec transform-set AES256/GCM/TRANSPORT esp-gcm 256
 mode transport
```

Step 6: Configure the IPsec profile.

The IPsec profile creates an association between an IKEv2 profile and an IPsec transform-set.

```
crypto ipsec profile [profile name]
 set transform-set [transform set]
 set ikev2-profile [ikev2 profile name]
```

Repeat this step for each WAN transport desired for DMVPN tunnels.

Example

IPSec profile for WAN transport MPLS1.

```
crypto ipsec profile DMVPN-IPSEC-PROFILE-MPLS1
 set transform-set AES256/GCM/TRANSFORM
 set ikev2-profile DMVPN-IKEv2-PROFILE
```

IPSec profile for WAN transport INET1.

```
crypto ipsec profile DMVPN-IPSEC-PROFILE-INET1
 set transform-set AES256/GCM/TRANSFORM
 set ikev2-profile DMVPN-IKEv2-PROFILE
```

Step 7: Increase the IPsec anti-replay window size.

```
crypto ipsec security-association replay window-size [value]
```

Example

```
crypto ipsec security-association replay window-size 1024
```

Tech Tip

QoS queuing delays can cause anti-replay packet drops, so it is important to extend the window size in order to prevent the drops from occurring.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the maximum window size in order to minimize future anti-replay problems. On the ASR1K, ISR4K and ISRG2 router platforms, the maximum replay window size is 1024.

If you do not increase the window size, the router may drop packets and you may see the following error messages on the router CLI and in the log:

%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed

A **show crypto ipsec sa** displays the transform and anti-replay window size.

```
show crypto ipsec sa

interface: Tunnel102
    Crypto map tag: DMVPN-IPSEC-PROFILE-MPLS1-head-1, local addr 192.168.6.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.6.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.6.33/255.255.255.255/47/0)
```

```
   current_peer 192.168.6.33 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 97284, #pkts encrypt: 97284, #pkts digest: 97284
    #pkts decaps: 96016, #pkts decrypt: 96016, #pkts verify: 96016
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.6.1, remote crypto endpt.: 192.168.6.33
     plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEther-
net0/0/3
     current outbound spi: 0x7A893B64(2055813988)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x857AB276(2239410806)
        transform: esp-gcm 256 ,
        in use settings ={Transport, }
        conn id: 2374, flow_id: HW:374, sibling_flags FFFFFFFF80000008, crypto
map: DMVPN-IPSEC-PROFILE-MPLS1-head-1
        sa timing: remaining key lifetime (k/sec): (4607666/1797)
        IV size: 8 bytes
        replay detection support: Y  replay window size: 1024
        Status: ACTIVE(ACTIVE)
```

Step 8: Return to the previous place in the guide.

CONFIGURING IKEV2 AND IPSEC FOR A REMOTE SITE ROUTER

This section is for remote site routers only.

In multi-VRF deployment, all tunnels with the same tunnel source interface must use the same IPsec profile and must have the **tunnel protection shared** command configured. For example, if tunnels 100 through 102 uses GigabitEthernet0/0 as their tunnel source and tunnels 200 through 202 uses GigabitEthernet0/1, then define the profile DMVPN-IPSEC-PROFILE-MPLS1 for tunnels 100 through 102 and DMVPN-IPSEC-PROFILE-INET1 for tunnels 200 through 202.

The crypto configurations have been simplified in this version of the guide in order to minimize the variations from previous guides. Use the values in the table that represent the design you are configuring.

Table 91 Crypto parameters

Parameter	Pre-Shared Keys
crypto ikev2 keyring	DMVPN-KEYRING
crypto ikev2 profile	DMVPN-IKEv2-PROFILE
crypto ipsec profile	DMVPN-IPSEC-PROFILE-[transport name]

IPsec uses a key exchange between the routers in order to encrypt/decrypt the traffic. These keys are exchanged using pre-shared keys.

Configuring IKEv2 and IPsec with Pre-Shared Keys

Step 1: Configure the crypto keyring for pre-shared keys.

The crypto keyring defines a pre-shared key (or password) valid for IP sources that are reachable within a particular VRF. This key is a wildcard pre-shared key if it applies to any IP source. A wildcard key is configured using the 0.0.0.0 0.0.0.0 network/mask combination.

```
crypto ikev2 keyring [keyring name]
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key [password]
```

Example

```
crypto ikev2 keyring DMVPN-KEYRING
 peer ANY
  address 0.0.0.0 0.0.0.0
  pre-shared-key c1sco123
```

Step 2: Configure the IKEv2 proposal.

The user-defined IKEv2 proposal includes only the following:

- Encryption with AES cipher and a 256-bit key
- Pseudo-random function with SHA and a 512-bit digest
- Diffie-Hellman group: 19

```
crypto ikev2 proposal [proposal name]
 encryption [encryption algorithm]
 prf [pseudo-random function algorithm]
 group [Diffie-Hellman group]
```

Example

```
crypto ikev2 proposal AES/GCM/256
 encryption aes-gcm-256
 prf sha512
 group 19
```

The default IKEv2 proposal is also used.

A **show crypto ikev2 proposal** displays the details of the two proposals.

```
show crypto ikev2 proposal
 IKEv2 proposal: AES/GCM/256
      Encryption : AES-GCM-256
      Integrity  : none
      PRF        : SHA512
      DH Group   : DH_GROUP_256_ECP/Group 19
 IKEv2 proposal: default
      Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
      Integrity  : SHA512 SHA384 SHA256 SHA96 MD596
      PRF        : SHA512 SHA384 SHA256 SHA1 MD5
      DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Step 3: Configure the IKEv2 policy.

The crypto policy includes the proposal you created in the previous step. This policy matches any FVRF defined on the router.

```
crypto ikev2 policy [policy name]
 match fvrf any
 proposal [proposal name]
```

Example

```
crypto ikev2 policy AES/GCM/256
 match fvrf any
 proposal AES/GCM/256
```

The default IKEv2 policy is also used.

A **show crypto ikev2 policy** displays the details of the two policies.

```
show crypto ikev2 policy

IKEv2 policy : AES/GCM/256
     Match fvrf : any
     Match address local : any
     Proposal    : AES/GCM/256

IKEv2 policy : default
     Match fvrf : any
     Match address local : any
     Proposal    : default
```

Step 4: Configure the IKEv2 profile.

The IKEv2 profile creates an association between an identity address, a VRF, and a crypto keyring. A wildcard address within a VRF is referenced with 0.0.0.0. The **identity local address** must match the loopback address of this router.

Tech Tip

Identity local address is needed for customers who use CGN, which requires a unique identity per remote site router even if the same pre-NAT IP address is used for other locations. The command does not affect customers who are not using CGN, so it is a recommended best practice to use the command all of the time.

The profile also defines what method of key sharing are used on this router with **authentication local** and what methods are accepted from remote locations with **authentication remote**. The **pre-share** keyword is used with the keyring defined above.

DPD is essential in order to facilitate fast re-convergence and for spoke registration to function properly in case a DMVPN hub is restarted. The IWAN design recommends you set the remote site DPD timer to 40 seconds with a 5 second retry. Moving the DPD timer into the **crypto ikev2 profile** ensures the command is used immediately, rather than waiting for the first 24 hour refresh cycle if the command is entered in the global configuration.

```
crypto ikev2 profile [profile name]
 description [profile description]
 match fvrf [vrf name]
 match identity remote address [IP address]
 identity local address [Loopback IP address of this router]
 authentication remote pre-share
 authentication local pre-share
 keyring local [keyring name]
```

Example: Single-router remote site for hybrid–RS11-2921

```
crypto ikev2 profile DMVPN-IKEv2-PROFILE
 description PSK Profile
 match fvrf any
 match identity remote address 0.0.0.0
 identity local address 10.255.241.11
 authentication local pre-share
 authentication remote pre-share
 keyring local DMVPN-KEYRING
 dpd 40 5 on-demand
```

Step 5: Define the IPsec transform set.

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. Peers agree to use a particular transform set when protecting a particular data flow.

The IPsec transform set for DMVPN uses the following:

- ESP with the 256-bit GCM encryption algorithm
- ESP with the SHA (HMAC variant) authentication algorithm

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport mode.

```
crypto ipsec transform-set [transform set] esp-gcm 256
 mode transport
```

Example

```
crypto ipsec transform-set AES256/GCM/TRANSPORT esp-gcm 256
 mode transport
```

Step 6: Configure the IPsec profile.

The IPsec profile creates an association between an IKEv2 profile and an IPsec transform-set.

```
crypto ipsec profile [profile name]
 set transform-set [transform set]
 set ikev2-profile [ikev2 profile name]
```

Repeat this step for each WAN transport desired for DMVPN tunnels.

Example

IPSec profile for WAN transport MPLS1.

```
crypto ipsec profile DMVPN-IPSEC-PROFILE-MPLS1
 set transform-set AES256/GCM/TRANSFORM
 set ikev2-profile DMVPN-IKEv2-PROFILE
```

IPSec profile for WAN transport INET1.

```
crypto ipsec profile DMVPN-IPSEC-PROFILE-INET1
 set transform-set AES256/GCM/TRANSFORM
 set ikev2-profile DMVPN-IKEv2-PROFILE
```

Step 7: Increase the IPsec anti-replay window size.

```
crypto ipsec security-association replay window-size [value]
```

Example

```
crypto ipsec security-association replay window-size 1024
```

Tech Tip

QoS queuing delays can cause anti-replay packet drops, so it is important to extend the window size in order to prevent the drops from occurring.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed.

It is recommended that you use the maximum window size in order to minimize future anti-replay problems. On the ASR1K, ISR4K and ISRG2 router platforms, the maximum replay window size is 1024.

If you do not increase the window size, the router may drop packets and you may see the following error messages on the router CLI and in the log:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
```

Step 8: Return to the previous place in the guide.

Appendix C: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- Routing update:
  - Added maximum secondary paths to remote site routers

You can use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.