CISCO VALIDATED DESIGN

Intelligent WAN Multiple Transports Deployment Guide

April 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 (this guide)
- IWAN Multiple VRF Deployment 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.

DEPLOYMENT DETAILS

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
```

Deploying Multiple WAN Transports

Use this guide to scale your IWAN deployment beyond a single pair of WAN transports at a POP location.

This design enables the following capabilities:

- Up to nine WAN transports at each POP with one designated as a path of last resort
- Convergence across WAN transports when all channels in a given transport fail or reach their maximum bandwidth limits
- Up to three WAN transports at a single-router remote site
- Up to five WAN transports at a dual-router remote site

This design adds multiple WAN transports to any of the previous design models. The multiple transport design model is not limited to two MPLS, two Internet, and one PLR transport, but this specific design is used to discuss the underlying principles. The same concepts can be applied to other multiple transport designs.

You can add multiple WAN transports with new border routers or the Multiple Tunnel Termination (MTT) feature for each transport, depending on the scaling requirements.

PROCESS

Configuring New Border Routers for Multiple WAN Transports

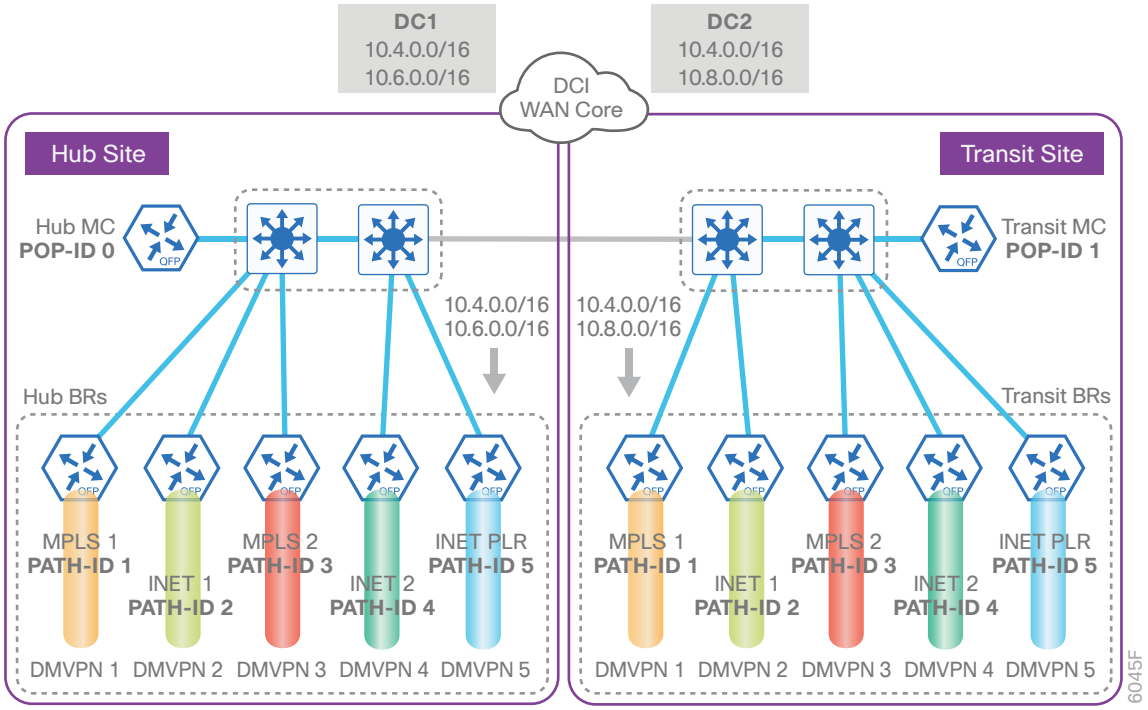
1. Copy the configuration from the existing router to the new router
2. Configure the BR platform
3. Configure connectivity to the LAN
4. Configure the routing protocol for the LAN
5. Connect to the MPLS WAN or Internet
6. Configure the mGRE tunnel
7. Configure the routing protocol for the WAN
8. Configure network address translation on the firewall

If you are planning to add the new transports with new border routers, follow the procedures in this process. If you are planning to add the new transports to existing border routers, follow the procedures in the next process, "Configuring MTT for Multiple WAN Transports."

For this process, you configure three new hub BRs and three new transit BRs with similar base configurations as your existing hub and transit BRs. You also have to make changes to the hub master controller and the remote site routers to take advantage of the new border routers.

The following diagram shows the IWAN dual hybrid with PLR design model using new hub border routers for each transport.

Figure 1 *IWAN dual hybrid with PLR design model using new border routers*



The new hub and transit site BRs have unique IP addresses and port-channel assignments, but the rest of the configuration items are the same as the existing border routers.

Follow the process "Configuring DMVPN Hub Router" in the Intelligent WAN Deployment Guide, using the base PfR information from the existing hub BRs. Make the required changes from the procedures below to add the new hub BRs and WAN transports to your IWAN domain.

The example below is for the MPLS2 hub BR. However, the process can be used for any of the BRs in this design. This model has five border routers at the hub site and five border routers at the transit site.

Procedure 1 Copy the configuration from the existing router to the new router

Optional

If you do not want to copy the configuration from an existing router, skip this procedure.

If the hardware for the corresponding new BR is identical to an existing BR, you can use this optional procedure to copy the configuration file from one router to the other as a starting point and then follow the procedures below. If you are creating a new MPLS BR, start with an existing MPLS BR, and if you are creating a new INET BR, start with an existing INET BR.

Step 1: Copy the running configuration from an existing router to your FTP server.

```
DHY-MPLS1-ASR1002X-1# copy running-config ftp://cisco:cisco@10.4.48.27
Address or name of remote host [10.4.48.27]?
Destination filename [dhy-mpls1-asr1002x-1-confg]?
Writing dhy-mpls1-asr1002x-1-confg !
15884 bytes copied in 0.800 secs (12707 bytes/sec)
```

Step 2: From the console of the new BR, copy and paste the configuration into the router before making the changes below.

You can also make the changes below in a text editor before pasting the configuration into the router.

Procedure 2 Configure the BR platform

In this procedure, you configure system settings that are unique to the new BR.

Table 1 Path, loopback IP addresses and F-VRF for hub BRs

Host name	Path	Path ID	Loopback IP address	WAN Transport F-VRF
DHY-MPLS1-ASR1002X-1	MPLS1	1	10.6.32.241/32	IWAN-Transport-1
DHY-INET1-ASR1002X-2	INET1	2	10.6.32.242/32	IWAN-Transport-2
DHY-MPLS2-ASR1002X-3	MPLS 2	3	10.6.32.243/32	IWAN-Transport-3
DHY-INET2-ASR1002X-4	INET 2	4	10.6.32.244/32	IWAN-Transport-4
DHY-INET4G-ASR1002X-5	PLR	5	10.6.32.245/32	IWAN-Transport-5

Table 2 Path, loopback IP addresses and F-VRF for transit BRs

Host name	Path	Path ID	Loopback IP address	WAN Transport F-VRF
DHY-MPLS1-ASR1002X-T1	MPLS1	1	10.8.32.241/32	IWAN-Transport-1
DHY-INET1-ASR1002X-T2	INET1	2	10.8.32.242/32	IWAN-Transport-2
DHY-MPLS2-ASR1002X-T3	MPLS 2	3	10.8.32.243/32	IWAN-Transport-3
DHY-INET2-ASR1002X-T4	INET 2	4	10.8.32.244/32	IWAN-Transport-4
DHY-INET4G-ASR1002X-T5	PLR	5	10.8.32.245/32	IWAN-Transport-5

Step 1: Configure the device host name to make it easy to identify the device.

```
hostname DHY-MPLS2-ASR1002X-3
```

Step 2: Configure an in-band management interface.

The loopback interface is a logical interface that is always reachable as long as the device is powered on and any IP interface is reachable to the network.

The loopback address is commonly a host address with a 32-bit address mask.

```
interface Loopback 0
  ip address 10.6.32.243 255.255.255.255
```

Procedure 3 Configure connectivity to the LAN

Any links to adjacent distribution layers should be Layer 3 links or Layer 3 EtherChannels. Choose a unique port-channel interface from the LAN switch perspective.

Table 3 Port channels and outside interface IP address for hub BRs

Host name	Port-channel numbers	Port-channel IP address	MPLS / Internet DMZ IP address
DHY-MPLS1-ASR1002X-1	1	10.6.32.2/30	192.168.6.1/24
DHY-INET1-ASR1002X-2	2	10.6.32.6/30	192.168.146.10/24
DHY-MPLS2-ASR1002X-3	3	10.6.32.10/30	192.168.7.1/24
DHY-INET2-ASR1002X-4	4	10.6.32.14/30	192.168.146.11/24
DHY-INET4G-ASR1002X-5	5	10.6.32.18/30	192.168.146.12/24

Table 4 Port channels and outside interface IP address for transit BRs

Host name	Port-channel numbers	Port-channel IP address	MPLS / Internet DMZ IP address
DHY-MPLS1-ASR1002X-T1	1	10.8.32.2/30	192.168.6.41/24
DHY-INET1-ASR1002X-T2	2	10.8.32.6/30	192.168.146.13/24
DHY-MPLS2-ASR1002X-T3	3	10.8.32.10/30	192.168.7.41/24
DHY-INET2-ASR1002X-T4	4	10.8.32.14/30	192.168.146.14/24
DHY-INET4G-ASR1002X-T5	5	10.8.32.18/30	192.168.146.15/24

Step 1: Configure a Layer 3 interface.

```
interface Port-channel3
  description IWAN-D3750X
  ip address 10.6.32.10 255.255.255.252
  ip pim sparse-mode
  no shutdown
```

Step 2: Configure EtherChannel member interfaces.

Configure the physical interfaces to tie to the logical port-channel by using the **channel-group** command. The number for the port-channel and channel-group must match. Not all router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet0/0/0
 description IWAN-D3750X Gig1/0/3

interface GigabitEthernet0/0/1
 description IWAN-D3750X Gig2/0/3

interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
  no ip address
  cdp enable
  channel-group 3
  no shutdown
```

Procedure 4 Configure the routing protocol for the LAN

If you are planning to use EIGRP, choose option 1. If you are planning to use BGP on the WAN and OSPF on the LAN, choose option 2.

Option 1: EIGRP on the LAN

The following table shows the EIGRP LAN delay in use.

Table 5 EIGRP LAN delay for IWAN hub and transit routers

LAN Interface	EIGRP LAN Delay (10 usec)
All LAN	50000

Step 1: Configure IP unicast routing using EIGRP named mode.

In this design, the tunnel, port-channel, and loopback must be EIGRP interfaces. The loopback may remain a passive interface. The network range must include all interface IP addresses, either in a single network statement or in multiple network statements.

This design uses a best practice of assigning the router ID to a loopback address.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  network 10.6.0.0 0.1.255.255
  eigrp router-id 10.6.32.243
 exit-address-family
```

Step 2: Configure the EIGRP interface.

Allow EIGRP to form neighbor relationships across the interface to establish peering adjacencies and exchange route tables. In this step, you configure EIGRP authentication by using the authentication key specified in the previous procedure.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  af-interface Port-channel3
   no passive-interface
   authentication mode md5
   authentication key-chain LAN-KEY
  exit-af-interface
 exit-address-family
```

Step 3: Configure the throughput delay on the LAN interface.

At the hub location where there are multiple border routers, the interface throughput delay setting should be set to influence the EIGRP routing protocol path preference.

Tech Tip

If you are using Port-channel interfaces with two Gigabit Ethernet members as recommended in this guide, you will have to double the LAN path delay to 500000 microseconds (usec), instead of the standard IWAN setting of 250000.

Set the internal LAN path to 500000 microseconds (usec). The delay command is entered in 10 usec units.

```
interface Port-channel3
  delay 50000
```

Option 2: OSPF on the LAN

Step 1: Configure OSPF Area 0 by using the loopback interface IP address as the router-id.

```
router ospf 100
 router-id 10.6.32.243
```

Step 2: Remove passive interface for the LAN interface.

```
router ospf 100
 no passive-interface Port-channel3
```

Procedure 5 Connect to the MPLS WAN or Internet

Each IWAN DMVPN hub requires a connection to the WAN transport, which for the dual hybrid model is either MPLS or Internet.

If you are using MPLS in this design, the DMVPN hub is connected to the service provider's MPLS PE router. The IP addressing used between IWAN CE and MPLS PE routers must be negotiated with your MPLS carrier.

If you are using the Internet in this design, the DMVPN hub is connected through a Cisco ASA 5500 using a DMZ interface specifically created and configured for a VPN termination router.

The IP address that you use for the Internet-facing interface of the DMVPN hub router must be an Internet-routable address. There are two possible methods for accomplishing this task:

- Assign a routable IP address directly to the router.
- Assign a non-routable RFC-1918 address directly to the router and use a static NAT on the Cisco ASA 5500 to translate the router IP address to a routable IP address.

This design assumes that the Cisco ASA 5500 is configured for static NAT for the DMVPN hub router.

Option 1: MPLS WAN physical WAN interface

The DMVPN design is using FVRF, so you must place the WAN interface into the VRF from the table above.

Step 1: Enable the interface, select the VRF, and assign the IP address.

```
interface GigabitEthernet0/0/3
 vrf forwarding IWAN-TRANSPORT-3
 ip address 192.168.7.1 255.255.255.252
 no shutdown
```

Step 2: Configure the VRF-specific default routing.

The VRF created for FVRF must have its own default route to the MPLS. This default route points to the MPLS PE router's IP address and is used by DMVPN for tunnel establishment.

```
ip route vrf IWAN-TRANSPORT-3 0.0.0.0 0.0.0.0 192.168.7.2
```

Option 2: Internet WAN physical WAN interface

The DMVPN design is using FVRF, so you must place the WAN interface into the VRF from the table above.

Step 1: Enable the interface, select the VRF, and assign the IP address.

```
interface GigabitEthernet0/0/3
 vrf forwarding IWAN-TRANSPORT-4
 ip address 192.168.146.11 255.255.255.0
 no shutdown
```

Step 2: Configure the VRF-specific default routing.

The VRF created for FVRF must have its own default route to the Internet. This default route points to the Cisco ASA 5500's DMZ interface IP address.

```
ip route vrf IWAN-TRANSPORT-4 0.0.0.0 0.0.0.0 192.168.146.1
```

Procedure 6 Configure the mGRE tunnel

The parameters in the table below are used in this procedure. Choose the row that represents the BR that you are configuring. This procedure applies to the MPLS2 hub BR in the IWAN dual hybrid with PLR design model.

Table 6 DMVPN tunnel parameters for hub BR

Hostname	Tunnel type	Tunnel number	Tunnel IP address
DHY-MPLS1-ASR1002X-1	MPLS1	10	10.6.34.1/23
DHY-INET1-ASR1002X-2	INET1	11	10.6.36.1/23
DHY-MPLS2-ASR1002X-3	MPLS2	12	10.6.38.1/23
DHY-INET2-ASR1002X-4	INET2	13	10.6.40.1/23
DHY-INET4G-ASR1002X-5	PLR	14	10.6.44.1/23

Table 7 DMVPN tunnel parameters for transit BR

Hostname	Tunnel type	Tunnel number	Tunnel IP address
DHY-MPLS1-ASR1002X-T1	MPLS1	10	10.6.34.2/23
DHY-INET1-ASR1002X-T2	INET1	11	10.6.36.2/23
DHY-MPLS2-ASR1002X-T3	MPLS2	12	10.6.38.2/23
DHY-INET2-ASR1002X-T4	INET2	13	10.6.40.2/23
DHY-INET4G-ASR1002X-T5	PLR	14	10.6.44.2/23

Step 1: Configure the basic interface settings.

The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

```
interface Tunnel12
 ip address 10.6.38.1 255.255.254.0
```

Step 2: (Optional) If this is a PLR tunnel interface, configure the domain path with the path of last resort feature.

The **path-last-resort** keyword activates the PLR feature on the tunnel interface. The following PLR modes are supported:

- **Standby mode**–No traffic classes are currently routed over the path of last resort service provider.
- **Active mode**–Traffic classes are currently routed over the path of last resort service provider.
- **Disabled mode**–The path of last resort is not enabled.

Tech Tip

The channels of the PLR are inactive when it is in standby mode. Once the PLR is active, smart probes are sent only on DSCP 0 (Zero SLA) to conserve bandwidth. In addition, smart probe frequency is reduced to 1 packet every 10 seconds from 20 packets per seconds and unreachable detection is extended to 60 seconds.

```
interface Tunnel14
 domain iwan path INET4G path-id 5 path-last-resort
```

Procedure 7 Configure the routing protocol for the WAN

If you are planning to use EIGRP, choose option 1. If you are planning to use BGP on the WAN and OSPF on the LAN, choose option 2.

Option 1: EIGRP on the WAN

The following table shows the DMVPN tunnel names and EIGRP WAN delay in use.

Table 8 EIGRP WAN delay for IWAN hybrid hub and transit routers

DMVPN tunnel	EIGRP WAN delay (10 usec)
Tunnel10	1000 (MPLS1)
Tunnel11	2000 (INET1)
Tunnel12	1100 (MPLS2)
Tunnel13	2100 (INET2)
Tunnel14	2200 (PLR)

Step 1: Configure EIGRP network summarization.

The IP assignments for the entire network were designed so they can be summarized within a few aggregate routes. As configured below, the **summary-address** command suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the remote sites, which offers a measure of resiliency. If the various networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  af-interface Tunnel12
   summary-address 10.6.0.0 255.255.0.0
   summary-address 10.7.0.0 255.255.0.0
   summary-address 10.8.0.0 255.255.0.0
   summary-address 10.255.240.0 255.255.248.0
  exit-af-interface
```

Step 2: Configure EIGRP summary metrics.

Step 3: If there are many component routes to be summarized and the component routes are frequently updated, the metrics are also updated frequently, which may cause a spike in the CPU usage. The **summary-metric** command explicitly sets the metric for the summary regardless of the component route metric, which reduces the computational load on a router.

The first value is the bandwidth metric in Kbits per second. The second value is the delay metric in 10 usecs. The third value is the reliability metric where 255 is 100% reliable. The fourth value is the effective bandwidth metric (loading) where 255 is 100% loaded. The fifth value is the MTU of the path.

Tech Tip

EIGRP uses the path's minimum bandwidth as part of the metric calculation. The path's minimum bandwidth is defined in a route advertisement in the minimum bandwidth path attribute. Setting the summary metric bandwidth (first value) to 10 Mbps essentially removes the ability to differentiate between a 10 Mbps tunnel (MPLS1) and a 100 Mbps circuit (INET1) because both paths have a minimum bandwidth of 10 Mbps. Setting the summary metric bandwidth to 10 Gbps as recommended in this guide allows the calculations on the branch router to differentiate tunnel bandwidth regardless of the size of each path.

Use the identical values for each summary address defined in the previous step.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  topology base
   summary-metric 10.6.0.0/16 10000000 10000 255 1 1500
   summary-metric 10.7.0.0/16 10000000 10000 255 1 1500
   summary-metric 10.8.0.0/16 10000000 10000 255 1 1500
   summary-metric 10.255.240.0/21 10000000 10000 255 1 1500
  exit-af-topology
```

Step 4: Configure the throughput delay on the tunnel interface.

The tunnel interface throughput delay setting should be set to influence the EIGRP routing protocol path preference. Set the WAN path delay using the values from the table at the top of this procedure. The delay command is entered in 10 usec units.

```
interface Tunnel12
  delay 1100
```

Step 5: Tag the routes for data center (POP) affinity.

In this design, there are different IP subnets for each DMVPN network, and the EIGRP tags are clearly defined to help with readability and troubleshooting. When a design uses more than one POP site, tags are required in order to identify the different DMVPN hub router locations, which allows a remote site to prefer one POP over the other.

Outbound distribute-lists are used to set tags on the DMVPN hub routers towards the WAN. The remote-site routers use **eigrp stub-site** in order to protect against becoming transit sites.

The following tables show specific route tags in use.

Table 9 *Route tag information for hub BRs at POP1*

DMVPN hub	DMVPN tunnel	DMVPN tunnel key	Tag tunnel
DHY-MPLS1-ASR1002X-1	Tunnel10	101 (MPLS1)	101 (All routes)
DHY-INET1-ASR1002X-2	Tunnel11	102 (INET1)	102 (All routes)
DHY-MPLS2-ASR1002X-3	Tunnel12	103 (MPLS2)	103 (All routes)
DHY-INET2-ASR1002X-4	Tunnel13	104 (INET2)	104 (All routes)
DHY-INET4G-ASR1002X-5	Tunnel14	105 (PLR)	105 (All routes)

Table 10 *Route tag information for transit BRs at POP2*

DMVPN hub	DMVPN tunnel	DMVPN tunnel key	Tag tunnel
DHY-MPLS1-ASR1002X-T1	Tunnel10	106 (MPLS1)	106 (All routes)
DHY-INET1-ASR1002X-T2	Tunnel11	107 (INET1)	107 (All routes)
DHY-MPLS2-ASR1002X-T3	Tunnel12	108 (MPLS2)	108 (All routes)
DHY-INET2-ASR1002X-T4	Tunnel13	109 (INET2)	109 (All routes)
DHY-INET4G-ASR1002X-T5	Tunnel14	110 (PLR)	110 (All routes)

The following example shows the MPLS2 hub border router in the IWAN dual hybrid design model.

Example: POP1 MPLS2 hub border router—DHY-MPLS2-ASR1002X-3

```
route-map SET-TAG-ALL permit 10
 description Tag all routes advertised through the tunnel
 set tag 103

router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
   topology base
    distribute-list route-map SET-TAG-ALL out Tunnel12
   exit-af-topology
```

Example: POP1 INET2 hub border router— DHY-INET2-ASR1002X-4

```
route-map SET-TAG-ALL permit 10
 description Tag all routes advertised through the tunnel
 set tag 104

router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
   topology base
    distribute-list route-map SET-TAG-ALL out Tunnel13
   exit-af-topology
```

Option 2: BGP on the WAN

The following tables show the tunnel DMVPN IP subnets, local preferences, community strings, and metrics in use.

Table 11 *Tunnel IPs, local preferences, community strings, and metrics for hub BRs*

DMVPN hub router	DMVPN tunnel IP subnet	BGP local preference	BGP community string	OSPF metric preferred POP	OSPF metric secondary POP
DHY-MPLS1-ASR1002X-1	10.6.34.0/23 (Tunnel10)	800 (MPLS1)	65100:100	1000	2000
DHY-INET1-ASR1002X-2	10.6.36.0/23 (Tunnel11)	780 (INET1)	65100:200	1200	2200
DHY-MPLS2-ASR1002X-3	10.6.38.0/23 (Tunnel12)	790 (MPLS2)	65100:300	1100	2100
DHY-INET2-ASR1002X-4	10.6.40.0/23 (Tunnel13)	770 (INET2)	65100:400	1300	2300
DHY-INET4G-ASR1002X-5	10.6.44.0/23 (Tunnel14)	760 (PLR)	65100:500	1400	2400

Table 12 *Tunnel IPs, local preferences, community strings, and metrics for transit BRs*

DMVPN hub router	DMVPN tunnel IP subnet	BGP local preference	BGP community string	OSPF metric preferred POP	OSPF metric secondary POP
DHY-MPLS1-ASR1002X-T1	10.6.34.0/23 (Tunnel10)	600 (MPLS1)	65100:101	1000	2000
DHY-INET1-ASR1002X-T2	10.6.36.0/23 (Tunnel11)	580 (INET1)	65100:201	1200	2200
DHY-MPLS2-ASR1002X-T3	10.6.38.0/23 (Tunnel12)	590 (MPLS2)	65100:301	1100	2100
DHY-INET2-ASR1002X-T4	10.6.40.0/23 (Tunnel13)	570 (INET2)	65100:401	1300	2300
DHY-INET4G-ASR1002X-T5	10.6.44.0/23 (Tunnel14)	560 (PLR)	65100:501	1400	2400

Step 1: Configure BGP values for the tunnel interface.

Use a private AS number for the BGP process. Assign this router's loopback address as the BGP router-id. Log the neighbor changes. Create a listen range that includes the subnet range of the tunnel interface. For internal BPG, use the same AS number for the remote sites. Create the route reflector and use the tunnel as the update source interface. Adjust the BGP hello and hold timers to 20 seconds and 60 seconds, respectively.

```
router bgp 65100
 bgp router-id 10.6.32.243
 bgp log-neighbor-changes
 bgp listen range 10.6.38.0/23 peer-group MPLS2-SPOKES
 neighbor MPLS2-SPOKES peer-group
 neighbor MPLS2-SPOKES remote-as 65100
 neighbor MPLS2-SPOKES description MPLS2 Spoke Route Reflector
 neighbor MPLS2-SPOKES update-source Tunnel12
 neighbor MPLS2-SPOKES timers 20 60
```

Step 2: Create the static null routes for the enterprise summary prefix and the site-specific prefixes.

```
ip route 10.4.0.0 255.252.0.0 Null0 254
ip route 10.6.0.0 255.255.0.0 Null0 254
ip route 10.4.0.0 255.255.0.0 Null0 254
```

Step 3: Configure the BGP address family.

Define the network statements for the default network, the enterprise summary prefix, the site-specific prefixes and the local MC loopback IP address the router will advertise to the remote sites. Configure BGP dynamic neighbors for the remote sites. Set the BGP distance and redistribute the internal networks.

```
router bgp 65100
 address-family ipv4
  bgp redistribute-internal
  network 0.0.0.0
  network 10.4.0.0 mask 255.252.0.0
  network 10.4.0.0 mask 255.255.0.0
  network 10.6.0.0 mask 255.255.0.0
  network 10.6.32.251 mask 255.255.255.255
  neighbor MPLS2-SPOKES activate
  neighbor MPLS2-SPOKES send-community
  neighbor MPLS2-SPOKES route-reflector-client
  neighbor MPLS2-SPOKES next-hop-self all
  neighbor MPLS2-SPOKES weight 50000
  neighbor MPLS2-SPOKES soft-reconfiguration inbound
  distance bgp 201 19 200
 exit-address-family
```

Step 4: Create the prefix lists for BGP.

Define the prefix-lists for the default network, the enterprise summary prefix, the site-specific prefixes, the local MC loopback IP address, and the subnet ranges for the DMVPN tunnels.

```
ip prefix-list DEFAULT-ROUTE seq 10 permit 0.0.0.0/0
ip prefix-list ENTERPRISE-PREFIX seq 10 permit 10.4.0.0/14
ip prefix-list LOCALDC-PREFIX seq 10 permit 10.4.0.0/16
ip prefix-list LOCALDC-PREFIX seq 20 permit 10.6.0.0/16
ip prefix-list LOCALMCLOOPBACK seq 10 permit 10.6.32.251/32
ip prefix-list TUNNEL-DMVPN seq 10 permit 10.6.38.0/23
```

Step 5: Create and apply the prefix route maps for BGP.

Define the route map to block prefixes inbound on the tunnel interface. Define the route map to allow prefixes to go out on the tunnel interface. Set the local preference and the community string for this DMVPN hub router. Apply the route maps to the BGP address family. Configure BGP to display communities in the format AA:NN.

Example: MPLS2 hub border router—DHY-MPLS2-ASR1002X-3

```
ip bgp-community new-format


route-map MPLS2-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LOCALMCLOOPBACK TUNNEL-DMVPN


route-map MPLS2-IN permit 1000
 description Allow Everything Else


route-map MPLS2-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LOCALMCLOOPBACK
 set local-preference 790
 set community 65100:300


router bgp 65100
 address-family ipv4
  neighbor MPLS2-SPOKES route-map MPLS2-IN in
  neighbor MPLS2-SPOKES route-map MPLS2-OUT out
exit-address-family
```

Example: INET2 hub border router– DHY-INET2-ASR1002X-4

```
ip bgp-community new-format


route-map INET2-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LO-
CALMCLOOPBACK TUNNEL-DMVPN


route-map INET2-IN permit 1000
 description Allow Everything Else


route-map INWT2-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LO-
CALMCLOOPBACK
 set local-preference 770
 set community 65100:400


router bgp 65100
 address-family ipv4
  neighbor INET2-SPOKES route-map INET2-IN in
  neighbor INET2-SPOKES route-map INET2-OUT out
exit-address-family
```

Step 6: Create and apply the BGP to OSPF redistribution route map for OSPF.

When there are two or more POP sites, there might be certain remote sites that want to prefer one POP over the other. This preference choice is done using a community string value that is sent by the remote site router to indicate which POP they prefer.

This example uses a community string in the form of AS:NN with AS being the BGP autonomous system number and NN being the value that selects the preferred POP.

Example:

65100:10 to prefer POP 1 (hub site)

65100:20 to prefer POP 2 (transit site)

The hub and transit BRs use the community string value they receive from the remote site in order to determine the OSPF metric for each location. The hub location matches the POP2 community string to set the higher metric values.

Define the community list to classify the remote sites as preferring POP1 or POP 2. Define the route map to block null routes from being distributed into OSPF. Set the metric to the appropriate value for the POP chosen by the remote site community string value. Apply the route map to the OSPF process when redistributing BGP.

Example: MPLS2 hub border router—DHY-MPLS2-ASR1002X-3

```
ip community-list standard POP2-SPOKES permit 65100:20

route-map REDIST-BGP-TO-OSPF permit 10
 description Secondary POP2 with higher Metric
 match community POP2-SPOKES
 set metric 2100
 set metric-type type-1

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

route-map REDIST-BGP-TO-OSPF permit 1000
 description Prefer POP1 with lower Metric
 set metric 1100
 set metric-type type-1

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

Example: INET2 hub border router—DHY-INET2-ASR1002X-4

```
ip community-list standard POP2-SPOKES permit 65100:20

route-map REDIST-BGP-TO-OSPF permit 10
 description Secondary POP2 with higher Metric
 match community POP2-SPOKES
 set metric 2300
 set metric-type type-1

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

```
route-map REDIST-BGP-TO-OSPF permit 1000
 description Prefer POP1 with lower Metric
 set metric 1300
 set metric-type type-1

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

Procedure 8 Configure network address translation on the firewall

You have to add the new Internet BRs to your firewall configuration for network address translation.

The DMZ network uses private network (RFC 1918) addressing that is not Internet-routable, so the firewall must translate the DMZ address of the DMVPN hub router to an outside public address.

The example DMZ address to public IP address mapping is shown in the following tables.

Table 13 DMVPN NAT address mapping for hub BRs

Hostname	DMVPN hub router DMZ address	DMVPN hub router public address (externally routable after NAT)
DHY-INET2-ASR1002X-4	192.168.146.11	172.17.140.1 (ISP-B)
DHY-INET4G-ASR1002X-5	192.168.146.12	172.18.140.1 (ISP-C)

Table 14 DMVPN NAT address mapping for transit BRs

Hostname	DMVPN hub router DMZ address	DMVPN hub router public address (externally routable after NAT)
DHY-INET2-ASR1002X-T4	192.168.146.14	172.17.140.2 (ISP-B)
DHY-INET4G-ASR1002X-T5	192.168.146.15	172.18.140.2 (ISP-C)

First, to simplify the configuration of the security policy, you create the External DMZ network objects that are used in the firewall policies.

Table 15 External DMZ firewall network objects for hub BRs

Network object name	Object type	IP address	Description
outside-dmvpn-4-ISPb	Host	172.17.140.1	DMVPN hub router 4 on ISP B (outside)
outside-dmvpn-5-ISPc	Host	172.18.140.1	DMVPN hub router 5 on ISP C (outside)

Table 16 External DMZ firewall network objects for transit BRs

Network object name	Object type	IP address	Description
outside-dmvpn-T4-ISPb	Host	172.17.140.2	DMVPN hub router T4 on ISP B (outside)
outside-dmvpn-T5-ISPc	Host	172.18.140.2	DMVPN hub router T5 on ISP C (outside)

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 2: Click **Add > Network Object**.

The Add Network Object dialog box appears.

Step 3: In the **Name** box, enter the name. (Example: outside-dmvpn-4-ISPb)

Step 4: In the **Type** list, choose **Host** or **Network**. (Example: Host)

Step 5: In the **IP Address** box, enter the address. (Example: 172.17.140.1)

Step 6: In the **Description** box, enter a useful description, and then click **OK**. (Example: DMVPN hub router 4 on ISP B)

Step 7: Repeat Step 2 through Step 6 for each object listed in the above tables. If an object already exists, then skip to the next object listed in the table.

Step 8: After adding all of the objects listed, on the Network Objects/Groups pane, click **Apply**.

Next, you add a network object for the private DMZ address of the DMVPN hub router.

Table 17 Private DMZ firewall network objects for hub BRs

Network object name	Object type	IP address	Description
dmz-dmvpn-4	Host	192.168.146.11	DMVPN hub router 4 on vpn-dmz
dmz-dmvpn-5	Host	192.168.146.12	DMVPN hub router 5 on vpn-dmz

Table 18 Private DMZ firewall network objects for transit BRs

Network object name	Object type	IP address	Description
dmz-dmvpn-T4	Host	192.168.146.14	DMVPN hub router T4 on vpn-dmz
dmz-dmvpn-T5	Host	192.168.146.15	DMVPN hub router T5 on vpn-dmz

Step 9: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 10: Click **Add > Network Object**.

The Add Network Object dialog box appears.

Step 11: In the **Name** box, enter the name. (Example: dmz-dmvpn-4)

Step 12: In the **Type** list, choose **Host** or **Network**. (Example: Host)

Step 13: In the **IP Address** box, enter the address. (Example: 192.168.146.11)

Step 14: In the **Description** box, enter a useful description, and then click **OK**. (Example: DMVPN hub router 4 on vpn-dmz)

Step 15: Click the two down arrows. The NAT pane expands.

Step 16: Select **Add Automatic Address Translation Rules**.

Step 17: In the **Translated Address** list, choose the network object created previously. (Example: outside-dmvpn-4-ISPb)

Step 18: Select **Use one-to-one address translation**, and then click **OK**.

Step 19: Repeat Step 10 through Step 18 for each object listed in the table above. If an object already exists, then skip to the next object listed in the table.

Step 20: After adding all of the objects listed, on the Network Objects/Groups pane, click **Apply**.

Step 21: Repeat this process for each new border router you add to your IWAN domain.

Step 22: Proceed to "Configuring PfR for Multiple WAN Transports."

PROCESS

Configuring MTT for Multiple WAN Transports

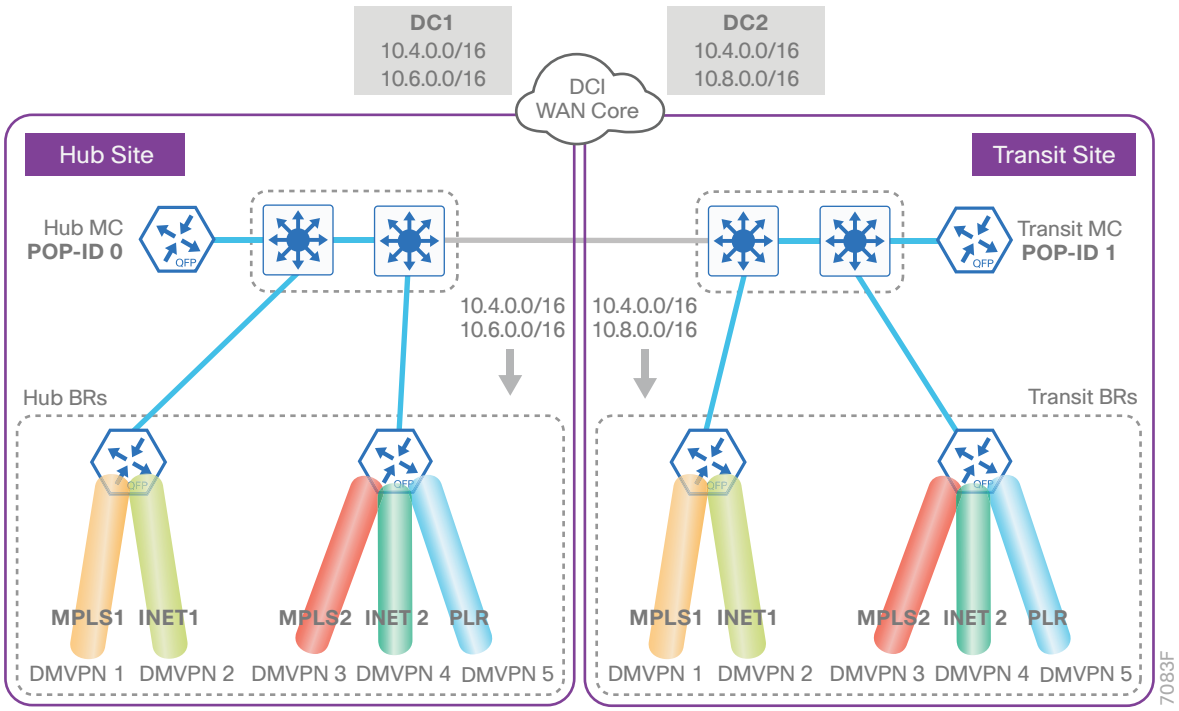
1. Connect to the MPLS WAN or Internet
2. Configure the mGRE tunnel
3. Configure the routing protocol for the WAN
4. Configure network address translation on the firewall

If you are planning to add the new transports to existing border routers, follow the procedures in this process. If you are planning to add the new transports with new border routers, follow the procedures in the previous process called "Configuring New Border Routers for Multiple WAN Transports".

For this process, you configure three new transports on the existing hub BRs and three new transports on the existing transit BRs. You also have to make changes to the hub master controller and the remote site routers to take advantage of the new transports.

The following diagram shows the IWAN dual hybrid with PLR design model using MTT for each transport.

Figure 2 *IWAN dual hybrid with PLR design model using MTT*



The process can be used for any of the new transports in this design. This model has two existing border routers at the hub site and two existing border routers at the transit site.

Procedure 1 Connect to the MPLS WAN or Internet

In this procedure, you configure system settings that are unique to the new transport.

Table 19 *Path, F-VRF and WAN IP addresses for hub BRs*

Host name	Physical interface	Path	Path ID	WAN transport F-VRF	MPLS/Internet DMZ IP address
DHY-M1I1-ASR1002X-1	Gig 0/0/3	MPLS1	1	IWAN-Transport-1	192.168.6.1/24
	Gig 0/0/4	INET1	2	IWAN-Transport-2	192.168.146.10/24
DHY-M2I2I3-ASR1002X-2	Gig 0/0/3	MPLS 2	3	IWAN-Transport-3	192.168.7.1/24
	Gig 0/0/4	INET 2	4	IWAN-Transport-4	192.168.146.11/24
	Gig 0/0/5	PLR	5	IWAN-Transport-5	192.168.146.12/24

Table 20 Path, F-VRF and WAN IP addresses for transit BRs

Host name	Physical interface	Path	Path ID	WAN transport F-VRF	MPLS/Internet DMZ IP address
DHY-M1I1-ASR1002X-T1	Gig 0/0/3	MPLS1	1	IWAN-Transport-1	192.168.6.41/24
	Gig 0/0/4	INET1	2	IWAN-Transport-2	192.168.146.13/24
DHY-M2I2I3-ASR1002X-T2	Gig 0/0/3	MPLS 2	3	IWAN-Transport-3	192.168.7.41/24
	Gig 0/0/4	INET 2	4	IWAN-Transport-4	192.168.146.14/24
	Gig 0/0/5	PLR	5	IWAN-Transport-5	192.168.146.15/24

Each IWAN DMVPN hub requires connections to their respective WAN transports, which for the dual hybrid model is either MPLS or Internet.

If you are using MPLS, the transport connects to the service provider's MPLS PE router. The IP addressing used between IWAN CE and MPLS PE routers must be negotiated with your MPLS carrier.

If you are using the Internet, the transport is connected through a Cisco ASA 5500 using a DMZ interface specifically created and configured for a VPN termination router.

The IP address that you use for the Internet-facing interface must be an Internet-routable address. There are two possible methods for accomplishing this task:

- Assign a routable IP address directly to the router.
- Assign a non-routable RFC-1918 address directly to the router and use a static NAT on the Cisco ASA 5500 to translate the router IP address to a routable IP address.

This design assumes that the Cisco ASA 5500 is configured for static NAT for the DMVPN hub router.

Option 1: MPLS WAN physical WAN interface

The DMVPN design is using FVRF, so you must place the WAN interface into the VRF from the table above.

Step 1: Enable the interface, select the VRF, and assign the IP address.

```
interface GigabitEthernet0/0/3
 description MPLS2
 vrf forwarding IWAN-TRANSPORT-3
 ip address 192.168.7.1 255.255.255.252
 no shutdown
```

Step 2: Configure the VRF-specific default routing.

The VRF created for FVRF must have its own default route to the MPLS. This default route points to the MPLS PE router's IP address and is used by DMVPN for tunnel establishment.

```
ip route vrf IWAN-TRANSPORT-3 0.0.0.0 0.0.0.0 192.168.7.2
```

Option 2: Internet WAN physical WAN interface

The DMVPN design is using FVRF, so you must place the WAN interface into the VRF from the table above.

Step 1: Enable the interface, select the VRF, and assign the IP address.

```
interface GigabitEthernet0/0/4
 description INET2
 vrf forwarding IWAN-TRANSPORT-4
 ip address 192.168.146.11 255.255.255.0
 no shutdown
```

Step 2: Configure the VRF-specific default routing.

The VRF created for FVRF must have its own default route to the Internet. This default route points to the Cisco ASA 5500's DMZ interface IP address.

```
ip route vrf IWAN-TRANSPORT-4 0.0.0.0 0.0.0.0 192.168.146.1
```

Procedure 2 Configure the mGRE tunnel

The parameters in the table below are used in this procedure. Choose the row that represents the transport that you are configuring. This procedure applies to the MPLS2 transport in the IWAN dual hybrid with PLR design model.

Table 21 DMVPN tunnel parameters for hub BR

Hostname	Tunnel type	Tunnel number	Tunnel IP address
DHY-M1I1-ASR1002X-1	MPLS1	10	10.6.34.1/23
	INET1	11	10.6.36.1/23
DHY-M2I2I3-ASR1002X-2	MPLS2	12	10.6.38.1/23
	INET2	13	10.6.40.1/23
	PLR	14	10.6.44.1/23

Table 22 DMVPN tunnel parameters for transit BR

Hostname	Tunnel type	Tunnel number	Tunnel IP address
DHY-M1I1-ASR1002X-T1	MPLS1	10	10.6.34.2/23
	INET1	11	10.6.36.2/23
DHY-M2I2I3-ASR1002X-T2	MPLS2	12	10.6.38.2/23
	INET2	13	10.6.40.2/23
	PLR	14	10.6.44.2/23

Step 1: Configure the basic interface settings.

The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

```
interface Tunnel12
 ip address 10.6.38.1 255.255.254.0
```

Step 2: (Optional) If this is a PLR tunnel interface, configure the domain path with the path of last resort feature.

The **path-last-resort** keyword activates the PLR feature on the tunnel interface. The following PLR modes are supported:

- **Standby mode**—No traffic classes are currently routed over the path of last resort service provider.
- **Active mode**—Traffic classes are currently routed over the path of last resort service provider.
- **Disabled mode**—The path of last resort is not enabled.

Tech Tip

The channels of the PLR are inactive when it is in standby mode. Once the PLR is active, smart probes are sent only on DSCP 0 (Zero SLA) to conserve bandwidth. In addition, smart probe frequency is reduced to 1 packet every 10 seconds from 20 packets per seconds and unreachable detection is extended to 60 seconds.

```
interface Tunnel14
 domain iwan path INET4G path-id 5 path-last-resort
```

Procedure 3 Configure the routing protocol for the WAN

If you are planning to use EIGRP, choose option 1. If you are planning to use BGP on the WAN and OSPF on the LAN, choose option 2.

Option 1: EIGRP on the WAN

The following table shows the DMVPN tunnel names and EIGRP WAN delay in use.

Table 23 EIGRP WAN delay for IWAN hybrid hub and transit routers

DMVPN tunnel	EIGRP WAN delay (10 usec)
Tunnel10	1000 (MPLS1)
Tunnel11	2000 (INET1)
Tunnel12	1100 (MPLS2)
Tunnel13	2100 (INET2)
Tunnel14	2200 (PLR)

Step 1: Configure EIGRP network summarization.

The IP assignments for the entire network are designed so they can be summarized within a few aggregate routes. As configured below, the **summary-address** command suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the remote sites, which offers a measure of resiliency. If the various networks cannot be summarized, then EIGRP continues to advertise the specific routes.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  af-interface Tunnel12
   summary-address 10.6.0.0 255.255.0.0
   summary-address 10.7.0.0 255.255.0.0
   summary-address 10.8.0.0 255.255.0.0
   summary-address 10.255.240.0 255.255.248.0
  exit-af-interface

  af-interface Tunnel13
   summary-address 10.6.0.0 255.255.0.0
   summary-address 10.7.0.0 255.255.0.0
   summary-address 10.8.0.0 255.255.0.0
   summary-address 10.255.240.0 255.255.248.0
  exit-af-interface

  af-interface Tunnel14
   summary-address 10.6.0.0 255.255.0.0
   summary-address 10.7.0.0 255.255.0.0
   summary-address 10.8.0.0 255.255.0.0
   summary-address 10.255.240.0 255.255.248.0
  exit-af-interface
```

Step 2: Configure EIGRP summary metrics.

If there are many component routes to be summarized and the component routes are frequently updated, the metrics are also updated frequently, which may cause a spike in the CPU usage. The **summary-metric** command explicitly sets the metric for the summary regardless of the component route metric, which reduces the computational load on a router.

The first value is the bandwidth metric in Kbits per second. The second value is the delay metric in 10 usecs. The third value is the reliability metric where 255 is 100% reliable. The fourth value is the effective bandwidth metric (loading) where 255 is 100% loaded. The fifth value is the MTU of the path.

Tech Tip

EIGRP uses the path's minimum bandwidth as part of the metric calculation. The path's minimum bandwidth is defined in a route advertisement in the minimum bandwidth path attribute. Setting the summary metric bandwidth (first value) to 10 Mbps essentially removes the ability to differentiate between a 10 Mbps tunnel (MPLS1) and a 100 Mbps circuit (INET1) because both paths have a minimum bandwidth of 10 Mbps. Setting the summary metric bandwidth to 10 Gbps as recommended in this guide allows the calculations on the branch router to differentiate tunnel bandwidth regardless of the size of each path.

Use the identical values for each summary address defined in the previous step.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  topology base
   summary-metric 10.6.0.0/16 10000000 10000 255 1 1500
   summary-metric 10.7.0.0/16 10000000 10000 255 1 1500
   summary-metric 10.8.0.0/16 10000000 10000 255 1 1500
   summary-metric 10.255.240.0/21 10000000 10000 255 1 1500
  exit-af-topology
```

Step 3: Configure the MTT maximum secondary paths.

The MTT feature adds support for secondary paths in the RIB of the supported routing protocols. The routing protocols are configured with one primary path and one or more secondary paths for a network. PfR is used for the primary, as well the secondary paths, so they are all active-active.

Use the **maximum-secondary-paths** command to limit the number of additional entries in the RIB to the number of tunnels terminated on the hub BR. The path value is set to one minus the total number of tunnels on the router.

The example below is for a hub BR with a total of three tunnels terminated.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  topology base
   maximum-secondary-paths 2
  exit-af-topology
```

Step 4: Configure the throughput delay on the tunnel interfaces.

The tunnel interface throughput delay setting should be set to influence the EIGRP routing protocol path preference. Set the WAN path delay using the values from the table at the top of this procedure. The delay command is entered in 10 usec units.

```
interface Tunnel12
  delay 1100

interface Tunnel13
  delay 2100

interface Tunnel14
  delay 2200
```

Step 5: Tag the routes for data center (POP) affinity.

In this design, there are different IP subnets for each DMVPN network, and the EIGRP tags are clearly defined to help with readability and troubleshooting. When a design uses more than one POP site, tags are required in order to identify the different DMVPN hub router locations which allows a remote site to prefer one POP over the other.

Outbound distribute-lists are used to set tags on the DMVPN hub routers towards the WAN. The remote-site routers use **eigrp stub-site** in order to protect against becoming transit sites.

The following tables show specific route tags in use.

Table 24 Route tag information for hub BRs at POP1

DMVPN hub	DMVPN tunnel	DMVPN tunnel key	Tag tunnel
DHY-M1I1-ASR1002X-1	Tunnel10	101 (MPLS1)	101 (All routes)
	Tunnel11	102 (INET1)	102 (All routes)
DHY-M2I2I3-ASR1002X-2	Tunnel12	103 (MPLS2)	103 (All routes)
	Tunnel13	104 (INET2)	104 (All routes)
	Tunnel14	105 (PLR)	105 (All routes)

Table 25 *Route tag information for transit BRs*

DMVPN hub	DMVPN tunnel	DMVPN tunnel key	Tag tunnel
DHY-M1I1-ASR1002X-T1	Tunnel10	106 (MPLS1)	106 (All routes)
	Tunnel11	107 (INET1)	107 (All routes)
DHY-M2I2I3-ASR1002X-T2	Tunnel12	108 (MPLS2)	108 (All routes)
	Tunnel13	109 (INET2)	109 (All routes)
	Tunnel14	110 (PLR)	110 (All routes)

The following example shows the MPLS2, INET2 and PLR transports in the IWAN dual hybrid design model.

Example: MPLS2, INET2 and PLR transports—DHY-M2I2I3-ASR1002X-2

```
route-map SET-TAG-MPLS2 permit 10
 description Tag all routes advertised through the tunnel
 set tag 103

route-map SET-TAG-INET2 permit 10
 description Tag all routes advertised through the tunnel
 set tag 104

route-map SET-TAG-PLR permit 10
 description Tag all routes advertised through the tunnel
 set tag 105

router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
   topology base
    distribute-list route-map SET-TAG-MPLS2 out Tunnel12
    distribute-list route-map SET-TAG-INET2 out Tunnel13
    distribute-list route-map SET-TAG-PLR out Tunnel14
   exit-af-topology
```

Option 2: BGP on the WAN

The following tables show the tunnel DMVPN IP subnets, local preferences, community strings, and metrics in use.

Table 26 *Tunnel IPs, local preferences, community strings, and metrics for hub BRs*

DMVPN hub router	DMVPN tunnel IP subnet	BGP local preference	BGP community string	OSPF metric preferred POP	OSPF metric secondary POP
DHY-M1I1-ASR1002X-1	10.6.34.0/23 (Tunnel10)	800 (MPLS1)	65100:100	1000	2000
	10.6.36.0/23 (Tunnel11)	780 (INET1)	65100:200	1200	2200
DHY-M2I2I3-ASR1002X-2	10.6.38.0/23 (Tunnel12)	790 (MPLS2)	65100:300	1100	2100
	10.6.40.0/23 (Tunnel13)	770 (INET2)	65100:400	1300	2300
	10.6.44.0/23 (Tunnel14)	760 (PLR)	65100:500	1400	2400

Table 27 *Tunnel IPs, local preferences, community strings, and metrics for transit BRs*

DMVPN hub router	DMVPN tunnel IP subnet	BGP local preference	BGP community string	OSPF metric preferred POP	OSPF metric secondary POP
DHY-M1I1-ASR1002X-T1	10.6.34.0/23 (Tunnel10)	600 (MPLS1)	65100:101	1000	2000
	10.6.36.0/23 (Tunnel11)	580 (INET1)	65100:201	1200	2200
DHY-M2I2I3-ASR1002X-T2	10.6.38.0/23 (Tunnel12)	590 (MPLS2)	65100:301	1100	2100
	10.6.40.0/23 (Tunnel13)	570 (INET2)	65100:401	1300	2300
	10.6.44.0/23 (Tunnel14)	560 (PLR)	65100:501	1400	2400

Step 1: Configure BGP values for the tunnel interface.

Use a private AS number for the BGP process. Assign this router's loopback address as the BGP router-id. Log the neighbor changes. Create a listen range that includes the subnet range of the tunnel interface. For internal BPG, use the same AS number for the remote sites. Create the route reflector and use the tunnel as the update source interface. Adjust the BGP hello and hold timers to 20 seconds and 60 seconds, respectively.

```
router bgp 65100
 bgp router-id 10.6.32.242
 bgp log-neighbor-changes
 bgp listen range 10.6.44.0/23 peer-group INET4G-SPOKES
 bgp listen range 10.6.40.0/23 peer-group INET2-SPOKES
 bgp listen range 10.6.38.0/23 peer-group MPLS2-SPOKES
 neighbor MPLS2-SPOKES peer-group
 neighbor MPLS2-SPOKES remote-as 65100
 neighbor MPLS2-SPOKES description MPLS2 Spoke Route Reflector
 neighbor MPLS2-SPOKES update-source Tunnel12
 neighbor MPLS2-SPOKES timers 20 60
 neighbor INET2-SPOKES peer-group
 neighbor INET2-SPOKES remote-as 65100
 neighbor INET2-SPOKES description INET2 Spoke Route Reflector
 neighbor INET2-SPOKES update-source Tunnel13
 neighbor INET2-SPOKES timers 20 60
 neighbor INET4G-SPOKES peer-group
 neighbor INET4G-SPOKES remote-as 65100
 neighbor INET4G-SPOKES description INET4G Spoke Route Reflector
 neighbor INET4G-SPOKES update-source Tunnel14
 neighbor INET4G-SPOKES timers 20 60
```

Step 2: Create the static null routes for the enterprise summary prefix and the site-specific prefixes.

```
ip route 10.4.0.0 255.252.0.0 Null0 254
ip route 10.6.0.0 255.255.0.0 Null0 254
ip route 10.4.0.0 255.255.0.0 Null0 254
```

Step 3: Configure the BGP address family.

Define the network statements for the default network, the enterprise summary prefix, the site-specific prefixes and the local MC loopback IP address the router will advertise to the remote sites. Configure BGP dynamic neighbors for the remote sites. Set the BGP distance and redistribute the internal networks.

```
router bgp 65100
 address-family ipv4
  bgp redistribute-internal
  network 0.0.0.0
  network 10.4.0.0 mask 255.252.0.0
  network 10.4.0.0 mask 255.255.0.0
  network 10.6.0.0 mask 255.255.0.0
  network 10.6.32.251 mask 255.255.255.255
  neighbor MPLS2-SPOKES activate
  neighbor MPLS2-SPOKES send-community
  neighbor MPLS2-SPOKES route-reflector-client
  neighbor MPLS2-SPOKES next-hop-self all
  neighbor MPLS2-SPOKES weight 50000
  neighbor MPLS2-SPOKES soft-reconfiguration inbound
  neighbor INET2-SPOKES activate
  neighbor INET2-SPOKES send-community
  neighbor INET2-SPOKES route-reflector-client
  neighbor INET2-SPOKES next-hop-self all
  neighbor INET2-SPOKES weight 50000
  neighbor INET2-SPOKES soft-reconfiguration inbound
  neighbor INET4G-SPOKES activate
  neighbor INET4G-SPOKES send-community
  neighbor INET4G-SPOKES route-reflector-client
  neighbor INET4G-SPOKES next-hop-self all
  neighbor INET4G-SPOKES weight 50000
  neighbor INET4G-SPOKES soft-reconfiguration inbound
  distance bgp 201 19 200
 exit-address-family
```

Step 4: Configure the MTT maximum secondary paths.

The MTT feature adds support for secondary paths in the RIB of the supported routing protocols. The routing protocols are configured with one primary path and one or more secondary paths for a network. PfR is used for the primary, as well the secondary paths, so they are all active-active.

Use the **maximum-secondary-paths** command to limit the number of additional entries in the RIB to the number of tunnels terminated on the hub BR. The path value is set to one minus the total number of tunnels on the router and the **ibgp** keyword indicates the router is using Internal BGP peering between its neighbors.

The example below is for a hub BR running iBGP with a total of three tunnels terminated.

```
router bgp 65100
 address-family ipv4
  maximum-secondary-paths ibgp 2
 exit-address-family
```

Step 5: Create the prefix lists for BGP.

Define the prefix-lists for the default network, the enterprise summary prefix, the site-specific prefixes, the local MC loopback IP address, and the subnet ranges for the DMVPN tunnels.

```
ip prefix-list DEFAULT-ROUTE seq 10 permit 0.0.0.0/0
ip prefix-list ENTERPRISE-PREFIX seq 10 permit 10.4.0.0/14
ip prefix-list LOCALDC-PREFIX seq 10 permit 10.4.0.0/16
ip prefix-list LOCALDC-PREFIX seq 20 permit 10.6.0.0/16
ip prefix-list LOCALMCLOOPBACK seq 10 permit 10.6.32.251/32
ip prefix-list TUNNEL-DMVPN seq 10 permit 10.6.38.0/23
```

Step 6: Create and apply the prefix route maps for BGP.

Define the route map to block prefixes inbound on the tunnel interface. Define the route map to allow prefixes to go out on the tunnel interface. Set the local preference and the community string for this DMVPN hub router. Apply the route maps to the BGP address family. Configure BGP to display communities in the format AA:NN.

Example: MPLS2 transport– DHY-M2I2I3-ASR1002X-2

```
ip bgp-community new-format

route-map MPLS2-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LOCALMCLOOPBACK TUNNEL-DMVPN

route-map MPLS2-IN permit 1000
 description Allow Everything Else

route-map MPLS2-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LOCALMCLOOPBACK
 set local-preference 790
 set community 65100:300

router bgp 65100
 address-family ipv4
  neighbor MPLS2-SPOKES route-map MPLS2-IN in
  neighbor MPLS2-SPOKES route-map MPLS2-OUT out
exit-address-family
```

Example: INET2 transport– DHY-M2I2I3-ASR1002X-2

```
ip bgp-community new-format

route-map INET2-IN deny 10
 description All Blocked Prefixes to come IN on BGP
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LOCALMCLOOPBACK TUNNEL-DMVPN

route-map INET2-IN permit 1000
 description Allow Everything Else

route-map INET2-OUT permit 10
 description All Allowed Prefixes to Go OUT on BGP to Spokes
```

```
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX LO-
CALMCLOOPBACK
 set local-preference 770
 set community 65100:400

router bgp 65100
 address-family ipv4
  neighbor INET2-SPOKES route-map INET2-IN in
  neighbor INET2-SPOKES route-map INET2-OUT out
exit-address-family
```

Step 7: Create and apply the BGP to OSPF redistribution route map for OSPF.

When there are two or more POP sites, there might be certain remote sites that want to prefer one POP over the other. This preference choice is done using a community string value that is sent by the remote site router to indicate which POP they prefer.

This example uses a community string in the form of AS:NN with AS being the BGP autonomous system number and NN being the value that selects the preferred POP.

Example:

65100:10 to prefer POP 1 (hub site)

65100:20 to prefer POP 2 (transit site)

The hub and transit BRs use the community string value they receive from the remote site in order to determine the OSPF metric for each location. The hub location matches the POP2 community string to set the higher metric values.

Define the community list to classify the remote sites as preferring POP1 or POP 2. Define the route map to block null routes from being distributed into OSPF. Set the metric to the appropriate value for the POP chosen by the remote site community string value. Apply the route map to the OSPF process when redistributing BGP.

Example: MPLS2 transport– DHY-M2I2I3-ASR1002X-2

```
ip community-list standard POP2-SPOKES permit 65100:20

route-map REDIST-BGP-TO-OSPF permit 10
 description Secondary POP2 with higher Metric
 match community POP2-SPOKES
 set metric 2100
 set metric-type type-1

route-map REDIST-BGP-TO-OSPF deny 20
 description Block Null routes to be distributed from BGP to OSPF
```

```
 match ip address prefix-list DEFAULT-ROUTE ENTERPRISE-PREFIX LOCALDC-PREFIX

route-map REDIST-BGP-TO-OSPF permit 1000
 description Prefer POP1 with lower Metric
 set metric 1100
 set metric-type type-1

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

Example: INET2 transport– DHY-M2I2I3-ASR1002X-2

```
ip community-list standard POP2-SPOKES permit 65100:20

route-map REDIST-BGP-TO-OSPF permit 10
 description Secondary POP2 with higher Metric
 match community POP2-SPOKES
 set metric 2300
 set metric-type type-1

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

route-map REDIST-BGP-TO-OSPF permit 1000
 description Prefer POP1 with lower Metric
 set metric 1300
 set metric-type type-1

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

Procedure 4 Configure network address translation on the firewall

You have to add the new Internet transports to your firewall configuration for network address translation.

The DMZ network uses private network (RFC 1918) addressing that is not Internet-routable, so the firewall must translate the DMZ address of the DMVPN hub router to an outside public address.

The example DMZ address to public IP address mapping is shown in the following tables.

Table 28 DMVPN NAT address mapping for hub BRs

Hostname	DMVPN hub router DMZ address	DMVPN hub router public address (externally routable after NAT)
DHY-M2I2I3-ASR1002X-2	192.168.146.11	172.17.140.1 (ISP-B)
	192.168.146.12	172.18.140.1 (ISP-C)

Table 29 DMVPN NAT address mapping for transit BRs

Hostname	DMVPN hub router DMZ address	DMVPN hub router public address (externally routable after NAT)
DHY-M2I2I3-ASR1002X-T2	192.168.146.14	172.17.140.2 (ISP-B)
	192.168.146.15	172.18.140.2 (ISP-C)

First, to simplify the configuration of the security policy, you create the External DMZ network objects that are used in the firewall policies.

Table 30 External DMZ firewall network objects for hub BRs

Network object name	Object type	IP address	Description
outside-dmvpn-4-ISPb	Host	172.17.140.1	DMVPN transport 4 on ISP B (outside)
outside-dmvpn-5-ISPc	Host	172.18.140.1	DMVPN transport 5 on ISP C (outside)

Table 31 External DMZ firewall network objects for transit BRs

Network object name	Object type	IP address	Description
outside-dmvpn-T4-ISPb	Host	172.17.140.2	DMVPN transport T4 on ISP B (outside)
outside-dmvpn-T5-ISPc	Host	172.18.140.2	DMVPN transport T5 on ISP C (outside)

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 2: Click **Add > Network Object**.

The Add Network Object dialog box appears.

Step 3: In the **Name** box, enter the name. (Example: outside-dmvpn-4-ISPb)

Step 4: In the **Type** list, choose **Host** or **Network**. (Example: Host)

Step 5: In the **IP Address** box, enter the address. (Example: 172.17.140.1)

Step 6: In the **Description** box, enter a useful description, and then click **OK**. (Example: DMVPN hub router 4 on ISP B)

Step 7: Repeat Step 2 through Step 6 for each object listed in the above tables. If an object already exists, then skip to the next object listed in the table.

Step 8: After adding all of the objects listed, on the Network Objects/Groups pane, click **Apply**.

Next, you add a network object for the private DMZ address of the DMVPN hub router.

Table 32 Private DMZ firewall network objects for hub BRs

Network object name	Object type	IP address	Description
dmz-dmvpn-4	Host	192.168.146.11	DMVPN transport 4 on vpn-dmz
dmz-dmvpn-5	Host	192.168.146.12	DMVPN transport 5 on vpn-dmz

Table 33 Private DMZ firewall network objects for transit BRs

Network object name	Object type	IP address	Description
dmz-dmvpn-T4	Host	192.168.146.14	DMVPN transport T4 on vpn-dmz
dmz-dmvpn-T5	Host	192.168.146.15	DMVPN transport T5 on vpn-dmz

Step 9: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**.

Step 10: Click **Add > Network Object**.

The Add Network Object dialog box appears.

Step 11: In the **Name** box, enter the name. (Example: dmz-dmvpn-4)

Step 12: In the **Type** list, choose **Host** or **Network**. (Example: Host)

Step 13: In the **IP Address** box, enter the address. (Example: 192.168.146.11)

Step 14: In the **Description** box, enter a useful description, and then click **OK**. (Example: DMVPN hub router 4 on vpn-dmz)

Step 15: Click the two down arrows. The NAT pane expands.

Step 16: Select **Add Automatic Address Translation Rules**.

Step 17: In the **Translated Address** list, choose the network object created previously. (Example: outside-dmvpn-4-ISPb)

Step 18: Select **Use one-to-one address translation**, and then click **OK**.

Step 19: Repeat Step 10 through Step 18 for each object listed in the table above. If an object already exists, then skip to the next object listed in the table.

Step 20: After adding all of the objects listed, on the Network Objects/Groups pane, click **Apply**.

Step 21: Repeat this process for each new transport you add to your IWAN domain.

PROCESS

Configuring PfR for Multiple WAN Transports

1. Configure PfR in the hub MC

For this process, you configure the PfR policy on the hub master controller to use the new WAN transports.

Procedure 1 Configure PfR in the hub MC

There are many options for configuring the PfR policy with multiple transports. The following changes are an example of how you can update your policy to use the new transports, but this is not the only way it can be done. Please configure your policy using the rules that make the most sense for your organization.

Step 1: Update the hub MC load balance preferences.

The dual hybrid design has two MPLS and two INET paths for redundancy. Limit the load balance paths to the two INET paths with fallback to the routing protocol using the **load-balance advanced** feature.

```
domain iwan
 vrf default
  master hub
   load-balance advanced
    path-preference INET1 INET2 fallback routing
```

Step 2: Update the PfR policy.

The policies use the PfR predefined templates. The path preference for voice and low latency data use the two MPLS paths with fallback to the two INET paths and a path of last resort. .

Tech Tip

The PLR feature provides the ability to designate a transport such that when the primary and fallback transports become unavailable or are out of bandwidth, traffic is routed over the path of last resort. This feature is used for metered links where data is charged on a usage basis and the path is only used when no other transports are available.

The path preference for real time video uses the two MPLS paths with fallback to the two INET paths. The bulk data and default classes use the two INET paths with fallback to the two MPLS paths and the scavenger class uses two INET paths with fallback to blackhole. The rest of the traffic will be load-balanced between the two INET paths with fallback to routing based on the changes from the previous step.

```
domain iwan
 vrf default
  master hub
   load-balance
   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
```

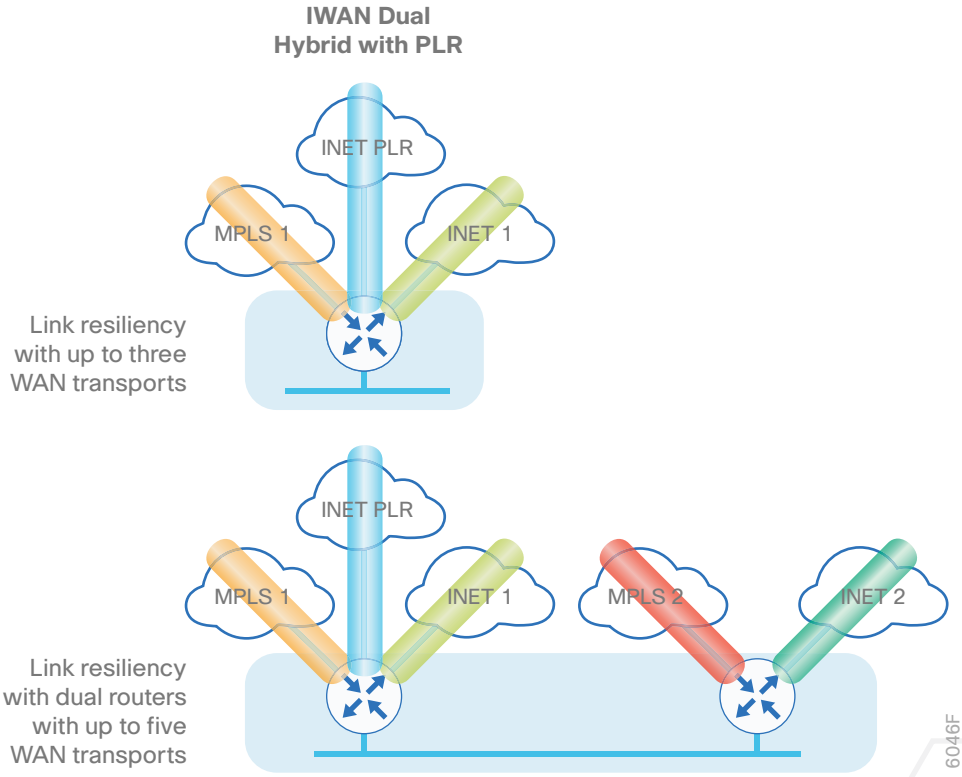
PROCESS

Configuring Remote-Site Routers for Multiple WAN Transports

1. Configure the WAN-facing VRF
2. Connect to the MPLS WAN or Internet
3. Configure the mGRE Tunnel
4. Configure the routing protocol on the WAN
5. Configure POP selection at remote site
6. Configure IP multicast routing for tunnel

The IWAN dual hybrid with PLR design model supports three WAN transports at a single-router remote site and five WAN transports at a dual-router remote site.

Figure 3 *IWAN dual hybrid with PLR design model for remote sites*



These procedures describe configuring an existing remote site router for an additional WAN transport using MPLS2 as an example.

Procedure 1 Configure the WAN-facing VRF

You create a new WAN-facing VRF in order to support FVRF for the additional WAN transports. The VRF name is arbitrary, but it is useful to select a name that describes the VRF. The VRF must be enabled for IPv4.

Table 34 VRF assignments

Transport Name	WAN VRF
MPLS1	IWAN-TRANSPORT-1
INET1	IWAN-TRANSPORT-2
MPLS2	IWAN-TRANSPORT-3
INET2	IWAN-TRANSPORT-4
PLR	IWAN-TRANSPORT-5

This design uses VRF Lite, so the selection is only locally significant to the device. It is a best practice to use the same VRF/RD combination across multiple devices when using VRFs in a similar manner. However, this convention is not strictly required.

Step 1: Configure the primary WAN VRF.

Example: MPLS2 in the IWAN dual hybrid with PLR design model

```
vrf definition IWAN-TRANSPORT-3
 address-family ipv4
```

Procedure 2 Connect to the MPLS WAN or Internet

The remote sites that are using DMVPN can use either static or dynamically assigned IP addresses. Cisco tested the design with static addresses for MPLS connections and DHCP assigned external addresses for Internet connections, which also provides a dynamically configured default route.

If you are using MPLS in this design, the DMVPN spoke router is connected to the service provider's MPLS PE router. The IP addressing used between IWAN CE and MPLS PE routers must be negotiated with your MPLS carrier.

The DMVPN spoke router connects directly to the Internet without a separate firewall. This connection is secured in two ways. Because the Internet interface is in a separate VRF, no traffic can access the global VRF except traffic sourced through the DMVPN tunnel. This design provides implicit security. Additionally, an IP access list permits only the traffic required for an encrypted tunnel, as well as DHCP and various ICMP protocols for troubleshooting.

Option 1: MPLS WAN Physical WAN Interface

The DMVPN design uses FVRF, so you must place this interface into the VRF configured in the previous procedure.

Step 1: Enable the interface, select VRF, and assign the IP address.

Example: MPLS2 in IWAN dual hybrid with PLR design model

```
interface GigabitEthernet0/0/0
 description MPLS2
 vrf forwarding IWAN-TRANSPORT-3
 ip address 192.168.7.21 255.255.255.252
 no shutdown
```

Do not enable PIM on this interface, because no multicast traffic should be requested from this interface.

Step 2: Configure the VRF-specific default routing.

The VRF created for FVRF must have its own default route to the Internet. This default route points to the MPLS PE router's IP address and is used by DMVPN for tunnel establishment.

```
ip route vrf IWAN-TRANSPORT-3 0.0.0.0 0.0.0.0 192.168.7.22
```

Option 2: Internet WAN Physical WAN Interface

The DMVPN design uses FVRF, so you must place this interface into the VRF configured in the previous procedure.

Step 1: Enable the interface, select VRF, and enable DHCP.

Example: PLR in the IWAN dual hybrid with PLR design model

```
interface GigabitEthernet0/0/3
 description PLR
 vrf forwarding IWAN-TRANSPORT-5
 ip address dhcp
 no cdp enable
 no shutdown
```

Do not enable PIM on this interface, because no multicast traffic should be requested from this interface.

It is not necessary to create VRF specific default route for Internet interfaces. The router will use the default route from the DHCP request to the provider.

Step 2: Configure and apply the access list.

The IP access list must permit the protocols specified in the following table. The access list is applied inbound on the WAN interface, so filtering is done on traffic destined to the router.

Table 35 *Required DMVPN protocols*

Name	Protocol	Usage
non500-isakmp	UDP 4500	IPsec using NAT-T
isakmp	UDP 500	ISAKMP
esp	IP 50	IPsec
bootpc	UDP 68	DHCP

Example: PLR in the IWAN dual hybrid with PLR design model

```
interface GigabitEthernet0/0/3
 ip access-group ACL-INET-PUBLIC in

ip access-list extended ACL-INET-PUBLIC
 permit udp any any eq non500-isakmp
 permit udp any any eq isakmp
 permit esp any any
 permit udp any any eq bootpc
```

The additional protocols listed in the following table may assist in troubleshooting but are not explicitly required to allow DMVPN to function properly.

Table 36 *Optional protocols: DMVPN spoke router*

Name	Protocol	Usage
icmp echo	ICMP Type 0, Code 0	Allow remote pings
icmp echo-reply	ICMP Type 8, Code 0	Allow ping replies (from your requests)
icmp ttl-exceeded	ICMP Type 11, Code 0	Allow traceroute replies (from your requests)
icmp port-unreachable	ICMP Type 3, Code 3	Allow traceroute replies (from your requests)
UDP high ports	UDP > 1023, TTL=1	Allow remote traceroute

The additional optional entries for an access list to support ping are as follows:

```
permit icmp any any echo
permit icmp any any echo-reply
```

The additional optional entries for an access list to support traceroute are as follows:

```
permit icmp any any ttl-exceeded      ! for traceroute (sourced)
permit icmp any any port-unreachable  ! for traceroute (sourced)
permit udp any any gt 1023 ttl eq 1   ! for traceroute (destination)
```

Procedure 3 Configure the mGRE Tunnel

This procedure uses the parameters in the table below. Choose the rows that represent the design model that you are configuring. This procedure applies to the secondary WAN.

Table 37 DMVPN tunnel parameters

Transport Name	Tunnel VRF	Tunnel number	Tunnel network	NHRP network ID/tunnel key
MPLS1	IWAN-TRANSPORT-1	10	10.6.34.0/23	101
INET1	IWAN-TRANSPORT-2	11	10.6.36.0/23	102
MPLS2	IWAN-TRANSPORT-3	12	10.6.38.0/23	103
INET2	IWAN-TRANSPORT-4	13	10.6.40.0/23	104
PLR	IWAN-TRANSPORT-5	14	10.6.44.0/23	105

Step 1: Configure the basic interface settings.

The tunnel number is arbitrary, but it is best to begin tunnel numbering at 10 or above, because other features deployed in this design may also require tunnels and they may select lower numbers by default.

The bandwidth setting must be set to match the bandwidth of the respective transport, which corresponds to the actual interface speed. Or, if you are using a subrate service, use the policed rate from the carrier. QoS and PfR require the correct bandwidth setting in order to operate properly.

Configure the **ip mtu** to 1400 and the **ip tcp adjust-mss** to 1360. There is a 40 byte difference, which corresponds to the combined IP and TCP header length.

```
interface Tunnel12
 description MPLS2
 bandwidth 100000
 ip address 10.6.38.31 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip tcp adjust-mss 1360
```

Step 2: Configure the tunnel.

DMVPN uses mGRE tunnels. This type of tunnel requires a source interface only. Use the same source interface that you use to connect to the Internet. Set the **tunnel vrf** command to the VRF defined previously for FVRF.

Tech Tip

The crypto configurations have been simplified in this version of the guide in order to minimize the number of variations from previous guides. With the new configurations, it is not necessary to configure IKEv2 and IPsec again. All IKEv2 and IPsec sessions use the same parameters.

Enabling encryption on this interface requires the application of the IPsec profile configured previously.

```
interface Tunnel12
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 103
 tunnel vrf IWAN-TRANSPORT-3
 tunnel protection ipsec profile DMVPN-IPSEC-PROFILE
```

Step 3: Configure NHRP.

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 data center 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 38 DMVPN tunnel NHRP parameters: MPLS1 and INET1

	Transport 1	Transport 2
VRF	IWAN-TRANSPORT-1	IWAN-TRANSPORT-2
DMVPN hub public address (actual)	192.168.6.1	192.168.146.10
DMVPN hub public address (externally routable after NAT)	n/a (MPLS1)	172.16.140.1
DMVPN hub tunnel IP address (NHS)	10.6.34.1	10.6.36.1
Tunnel number	10	11
NHRP network ID	101	102

Table 39 DMVPN tunnel NHRP parameters: MPLS2 and INET2

	Transport 3	Transport 4
VRF	IWAN-TRANSPORT-3	IWAN-TRANSPORT-4
DMVPN hub public address (actual)	192.168.7.1	192.168.146.11
DMVPN hub public address (externally routable after NAT)	n/a (MPLS2)	172.17.140.1
DMVPN hub tunnel IP address (NHS)	10.6.38.1	10.6.40.1
Tunnel number	12	13
NHRP network ID	103	104

Table 40 DMVPN tunnel NHRP parameters: PLR

	Transport 5
VRF	IWAN-TRANSPORT-5
DMVPN hub public address (actual)	192.168.146.12
DMVPN hub public address (externally routable after NAT)	172.18.140.1
DMVPN hub tunnel IP address (NHS)	10.6.44.1
Tunnel number	14
NHRP network ID	105

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.

```
interface Tunnel12
 ip nhrp authentication cisco123
 ip nhrp network-id 103
 ip nhrp holdtime 600
 ip nhrp nhs 10.6.38.1 nbma 192.168.7.1 multicast
 ip nhrp registration no-unique
 ip nhrp shortcut
 if-state nhrp
```

By default, NHRP will not install shortcuts for paths not seen in the RIB of the router. In a location with a single router and multiple WAN transports, only the preferred path is in the RIB. If you have a remote site location with more than one WAN transport, you need to disable the **nhrp route-watch** feature on each of the tunnel interfaces in order to allow NHRP to install the non-preferred shortcut path.

```
interface Tunnel12
 no nhrp route-watch
```

Procedure 4 Configure the routing protocol on the WAN

If you are planning to use EIGRP, choose option 1. If you are planning to use BGP on the WAN and OSPF on the LAN, choose option 2.

Option 1: EIGRP on the WAN

The following table shows the DMVPN tunnel names and EIGRP WAN delay in use.

Table 41 EIGRP WAN delay for IWAN remote-site routers

DMVPN Tunnel	EIGRP WAN Delay (10 usec)
Tunnel10	1000 (MPLS1)
Tunnel11	20000 (INET1)
Tunnel12	1100 (MPLS2)
Tunnel13	21000 (INET2)
Tunnel14	22000 (PLR)

A single EIGRP process runs on the DMVPN spoke router, which has already been enabled during the first DMVPN tunnel's configuration. All interfaces on the router are EIGRP interfaces, but only the DMVPN tunnel interfaces are non-passive. The network range must include all interface IP addresses either in a single network statement or in multiple network statements.

Step 1: Add the network range for the secondary DMVPN tunnel and configure as non-passive.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
   af-interface Tunnel12
    no passive-interface
   exit-af-interface
 network 10.6.38.0 0.0.1.255
exit-address-family
```

Step 2: Configure EIGRP values for the mGRE tunnel interface.

The EIGRP hello interval is increased to 20 seconds and the EIGRP hold time is increased to 60 seconds in order to accommodate up to 2000 remote sites on a single DMVPN cloud. Increasing the EIGRP timers also slows down the routing convergence to improve network stability and the IWAN design allows PfR to initiate the fast failover, so changing the timers is recommended for all IWAN deployments.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
   af-interface Tunnel12
    hello-interval 20
    hold-time 60
   exit-af-interface
 exit-address-family
```

Step 3: Configure EIGRP neighbor authentication. Neighbor authentication enables the secure establishment of peering adjacencies and exchange route tables over the DMVPN tunnel interface.

```
key chain WAN-KEY
 key 1
  key-string c1sco123

router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  af-interface Tunnel12
   authentication mode md5
   authentication key-chain WAN-KEY
  exit-af-interface
 exit-address-family
```

Step 4: Configure EIGRP route summarization.

The remote-site LAN networks must be advertised. The IP assignment for the remote sites was designed so that all of the networks in use can be summarized within a single aggregate route. As configured below, the **summary-address** command suppresses the more specific routes. If any network within the summary is present in the route table, the summary is advertised to the DMVPN hub, which offers a measure of resiliency. If the various LAN networks cannot be summarized, EIGRP continues to advertise the specific routes.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  af-interface Tunnel12
   summary-address 10.7.0.0 255.255.248.0
  exit-af-interface
 exit-address-family
```

Step 5: Configure the throughput delay on the tunnel interface.

The tunnel interface throughput delay setting should be set to influence the routing protocol path preference. Set the WAN path delay using the values from the table at the top of this procedure. The delay command is entered in 10 usec units.

```
interface Tunnel12
 delay 1100
```

Step 6: Add stub-site wan-interface.

With EIGRP stub-site, route tagging and blocking is no longer needed at the remote sites. You add one command to each af-interface tunnel in order to identify it as the stub-site wan-interface.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  af-interface Tunnel12
   stub-site wan-interface
  exit-af-interface
 exit-address-family
```

Step 7: Proceed to Procedure 6, "Configure IP multicast routing for tunnel."

Option 2: BGP on the WAN

Step 1: Configure BGP values for the mGRE tunnel interface.

A single BGP process runs on the DMVPN spoke router, which has already been enabled during the first DMVPN tunnel's configuration. For internal BPG, use the same AS number for the remote sites. Use the tunnel interface as the update source. Adjust the BGP hello and hold timers to 20 seconds and 60 seconds, respectively. Peer to the hub border router.

```
router bgp 65100
 neighbor MPLS2-HUB peer-group
 neighbor MPLS2-HUB remote-as 65100
 neighbor MPLS2-HUB description To IWAN MPLS2 Hub Router
 neighbor MPLS2-HUB update-source Tunnel12
 neighbor MPLS2-HUB timers 20 60
 neighbor 10.6.38.1 peer-group MPLS2-HUB
```

Step 2: Configure the BGP address family.

Send the community string, set next-hop-self, set the weight to 50000, and turn on soft reconfiguration inbound. Activate the BGP connection to the DMVPN hub border router.

```
router bgp 65100
 address-family ipv4
  neighbor MPLS2-HUB send-community
  neighbor MPLS2-HUB next-hop-self all
  neighbor MPLS2-HUB weight 50000
  neighbor MPLS2-HUB soft-reconfiguration inbound
  neighbor 10.6.38.1 activate
exit-address-family
```

Step 3: Apply the prefix route maps for BGP.

The route map to allow prefixes to go out on the tunnel interface was already defined. Apply the route map to the BGP address family for the hub border router.

```
router bgp 65100
 address-family ipv4
  neighbor MPLS2-HUB route-map SPOKE-OUT out
```

Procedure 5 Configure POP selection at remote site

If you are planning to use EIGRP, choose option 1. If you are planning to use BGP on the WAN and OSPF on the LAN, choose option 2.

Option 1: EIGRP on the WAN

The following tables show specific EIGRP route tags in use from the previous procedure.

Table 42 Route tag information for hub location

Tunnel interface	DMVPN tunnel key	Tag tunnel	Metric
Tunnel 10 (DMVPN 1)	101 (MPLS1)	101 (All routes)	+10000
Tunnel 11 (DMVPN 2)	102 (INET1)	102 (All routes)	+20000
Tunnel 12 (DMVPN 3)	103 (MPLS2)	103 (All routes)	+11000
Tunnel 13 (DMVPN 4)	104 (INET2)	104 (All routes)	+21000
Tunnel 14 (DMVPN 5)	105 (PLR)	105 (All routes)	+22000

Table 43 Route tag information for transit location

Tunnel interface	DMVPN tunnel key	Tag tunnel	Metric
Tunnel 10 (DMVPN 1)	106 (MPLS1)	106 (All routes)	+10000
Tunnel 11 (DMVPN 2)	107 (INET1)	107 (All routes)	+20000
Tunnel 12 (DMVPN 3)	108 (MPLS2)	108 (All routes)	+11000
Tunnel 13 (DMVPN 4)	109 (INET2)	109 (All routes)	+21000
Tunnel 14 (DMVPN 5)	110 (PLR)	110 (All routes)	+22000

Set the EIGRP metric value higher for the routes tagged from the non-preferred site.

Step 1: Define the route maps to identify the tags from border routers in POP1 and POP 2.

Example: Remote site that prefers POP1

```
route-map POP-SELECT permit 10
 description Prefer POP1 for MPLS1
 match tag 106
 set metric +10000

route-map POP-SELECT permit 20
 description Prefer POP1 for INET1
 match tag 107
 set metric +20000

route-map POP-SELECT permit 30
 description Prefer POP1 for MPLS2
 match tag 108
 set metric +11000

route-map POP-SELECT permit 40
 description Prefer POP1 for INET2
 match tag 109
 set metric +21000
```

```
route-map POP-SELECT permit 50
 description Prefer POP1 for PLR
 match tag 110
 set metric +22000

route-map POP-SELECT permit 100
 description Allow the rest
```

Example: Remote site that prefers POP2

```
route-map POP-SELECT permit 10
 description Prefer POP2 for MPLS1
 match tag 101
 set metric +10000

route-map POP-SELECT permit 20
 description Prefer POP2 for INET1
 match tag 102
 set metric +20000

route-map POP-SELECT permit 30
 description Prefer POP2 for MPLS2
 match tag 103
 set metric +11000

route-map POP-SELECT permit 40
 description Prefer POP2 for INET2
 match tag 103
 set metric +21000

route-map POP-SELECT permit 50
 description Prefer POP2 for PLR
 match tag 105
 set metric +22000

route-map POP-SELECT permit 100
 description Allow the rest
```

Step 2: Apply the POP select route map on the inbound tunnel interfaces.

Example: Single-router dual-link remote site with MPLS2 and INET2

```
router eigrp IWAN-EIGRP
  address-family ipv4 unicast autonomous-system 400
  topology base
   distribute-list route-map POP-SELECT in Tunnel12
   distribute-list route-map POP-SELECT in Tunnel13
  exit-af-topology
```

Step 3: Repeat this process for each remote site that will use the transit BRs.

Option 2: BGP on the WAN

Step 1: Configure BGP to display communities in the format AA:NN.

```
ip bgp-community new-format
```

Step 2: Define the community lists to identify the border routers from POP1 and POP 2.

```
ip community-list standard POP1-MPLS1 permit 65100:100
ip community-list standard POP1-MPLS2 permit 65100:300
ip community-list standard POP1-INET1 permit 65100:200
ip community-list standard POP1-INET2 permit 65100:400
ip community-list standard POP1-INET4G permit 65100:500

ip community-list standard POP2-MPLS1 permit 65100:101
ip community-list standard POP2-MPLS2 permit 65100:301
ip community-list standard POP2-INET1 permit 65100:201
ip community-list standard POP2-INET2 permit 65100:401
ip community-list standard POP2-INET4G permit 65100:501
```

Step 3: Create the inbound route maps and update the outbound route map.

Update the outbound route map with a community string to signal the POP preference to the border routers.

Example:

65100:10 to prefer POP 1 (hub site)

65100:20 to prefer POP 2 (transit site)

Use a community string in the form of AS:NN with AS being the BGP autonomous system number and NN being the value that selects the preferred POP.

On the inbound route maps, set the local preference higher for preferred POP border routers.

Example: Remote site that prefers POP1

```
route-map SPOKE-OUT permit 10
 description Prefer POP1 with community 65100:10
 set community 65100:10

route-map POP-SELECT permit 100
 description Prefer POP1 with higher LP
 match community POP1-MPLS1
 set local-preference 800

route-map POP-SELECT permit 110
 description Prefer POP1 with higher LP
 match community POP1-MPLS2
 set local-preference 790

route-map POP-SELECT permit 120
 description Prefer POP1 with higher LP
 match community POP1-INET1
 set local-preference 780

route-map POP-SELECT permit 130
 description Prefer POP1 with higher LP
 match community POP1-INET2
 set local-preference 770

route-map POP-SELECT permit 140
 description Prefer POP1 with higher LP
 match community POP1-INET4G
 set local-preference 760

route-map POP-SELECT permit 200
 match community POP2-MPLS1
 set local-preference 600
```

```
route-map POP-SELECT permit 210
 match community POP2-MPLS2
 set local-preference 590

route-map POP-SELECT permit 220
 match community POP2-INET1
 set local-preference 580

route-map POP-SELECT permit 230
 match community POP2-INET2
 set local-preference 570

route-map POP-SELECT permit 240
 match community POP2-INET4G
 set local-preference 560

route-map POP-SELECT permit 1000
 description If no match do not set LP
```

Example: Remote site that prefers POP2

```
route-map SPOKE-OUT permit 10
 description Prefer POP2 with community 65100:20
 set community 65100:20

route-map POP-SELECT permit 100
 match community POP1-MPLS1
 set local-preference 600

route-map POP-SELECT permit 110
 match community POP1-MPLS2
 set local-preference 590

route-map POP-SELECT permit 120
 match community POP1-INET1
 set local-preference 580
```

```
route-map POP-SELECT permit 130
 match community POP1-INET2
 set local-preference 570

route-map POP-SELECT permit 140
 match community POP1-INET4G
 set local-preference 560

route-map POP-SELECT permit 200
 description Prefer POP2 with higher LP
 match community POP2-MPLS1
 set local-preference 800

route-map POP-SELECT permit 210
 description Prefer POP2 with higher LP
 match community POP2-MPLS2
 set local-preference 790

route-map POP-SELECT permit 220
 description Prefer POP2 with higher LP
 match community POP2-INET1
 set local-preference 780

route-map POP-SELECT permit 230
 description Prefer POP2 with higher LP
 match community POP2-INET2
 set local-preference 770

route-map POP-SELECT permit 240
 description Prefer POP2 with higher LP
 match community POP2-INET4G
 set local-preference 760

route-map POP-SELECT permit 1000
 description If no match do not set LP
```

Step 4: Apply the POP select route map on the inbound WAN transport.

Example: Single-router dual-link remote site with MPLS2 and INET2

```
router bgp 65100
 address-family ipv4
  neighbor MPLS2-HUB route-map POP-SELECT in
  neighbor INET2-HUB route-map POP-SELECT in
 exit-address-family
```

Step 5: Repeat this process for each remote site that will use the new BRs.

Procedure 6 Configure IP multicast routing for tunnel

Optional

This optional procedure includes additional steps for configuring IP Multicast for a DMVPN tunnel on a router with IP Multicast already enabled. Skip this procedure if you do not want to use IP Multicast in your environment.

Step 1: Configure PIM on the DMVPN tunnel interface.

Enable IP PIM sparse mode on the DMVPN tunnel interface.

```
interface Tunnel12
 ip pim sparse-mode
```

Step 2: Configure the DR priority for the DMVPN spoke router.

Proper multicast operation across a DMVPN cloud requires that the hub router assumes the role of PIM DR. Spoke routers should never become the DR. You can prevent that by setting the DR priority to 0 for the spokes.

```
interface Tunnel12
 ip pim dr-priority 0
```

Step 3: Repeat this process for each new WAN transport at your remote sites.

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.

Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- Routing updates:
  - Simplified the EIGRP tagging and removed the filtering that was no longer needed
  - Added the EIGRP data center affinity use case to hub and remote sites
  - Added maximum secondary paths for the MTT use case with EIGRP and BGP
- Hub BR updates:
  - Added the Multiple Tunnel Termination feature
- Guide updates:
  - This new guide is one in a series of IWAN advanced deployment guides.

Please 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.