CISCO VALIDATED DESIGN

Intelligent WAN High Availability and Scalability Deployment Guide

April 2017

CISCO VALIDATED DESIGN

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 (this guide)
- IWAN Multiple Data Center Deployment Guide
- IWAN Multiple Transports Deployment 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 High Availability and Scalability

Use this guide to add IWAN Performance Routing (PfR) high availability and scalability to an existing IWAN deployment.

PROCESS

Configuring Hub Master Controller High Availability

1. Copy the configuration from existing router to the new router
2. Configure the loopback interfaces on the original hub MC
3. Configure the router-id on original hub MC
4. Configure the loopback interfaces
5. Configure connectivity to the LAN
6. Configure the routing protocol for the LAN
7. Test the failover from the primary hub MC

Use this optional process if you want to deploy a second hub MC for high availability (HA) using IP Anycast. Skip this process if you do not want to add HA to your hub MC.

This concept works with all of the IWAN design models, and it can be used with any standalone master controller, such as a transit master controller at a second data center or a standalone branch MC at a large remote site.

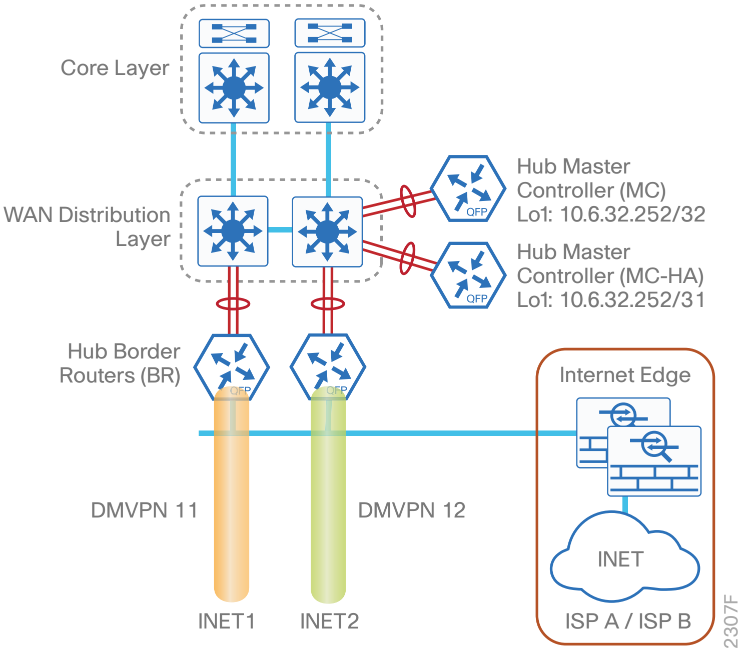
For this process, you configure a second hub MC with the same base configuration as the first one. You have to make a few minor changes to allow it to take over when the first hub MC goes offline. The two hub MCs must be kept in sync manually, but the failover will occur automatically within a few minutes depending on the size of your IWAN implementation.

Tech Tip

The Hub MC HA feature is used to protect against the failure of the MC device at a single location. The redundant hub MC cannot be at a different location.

The following diagram shows the hub MC HA and where it fits into the IWAN dual Internet design model.

Figure 1 *IWAN dual Internet design model—Hub MC high availability*



To accommodate the use of loopback0 for managing both hub MCs when they are active, it is recommended you create a new loopback1 for PfR. If you have already deployed IWAN, it is easier to continue to the use the IP address for PfR and use different IP addresses for loopback0.

The table below shows the two new loopback0 IP addresses for each device. The pair of hub MCs have the same loopback 1 IP address, except for the network mask. The second hub MC uses a /31 mask, which makes it a less desirable choice by the adjacent router's routing table unless the first hub MC is no longer reachable. The loopback0 and port channel IP addresses are unique.

Table 1 *Hub MC IP addresses*

IWAN design model	Host name	Loopback0 IP address (Mgmt)	Loopback1 IP address (PfR)	Port-channel IP address
Dual Internet	DI-MC-ASR1004-1	10.6.32.253/32	10.6.32.252/32	10.6.32.163/26
Dual Internet	DI-MC-ASR1004-2	10.6.32.254/32	10.6.32.252/31	10.6.32.164/26

Follow the process "Configuring Hub Master Controller" and the first three procedures of the process "Configuring PfR for Hub Location" using the base PfR information from the first hub MC. Make the required changes from the procedures below in order to enable hub MC HA in the IWAN domain.

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

Optional

If the hardware for the second hub MC is identical to the first, 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. Skip this procedure if you do not want to copy the configuration from an existing router.

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

```
DI-MC-ASR1004-1# copy running-config ftp://cisco:cisco@10.4.48.27
Address or name of remote host [10.4.48.27]?
Destination filename [di-mc-asr1004-1-confg]?
Writing di-mc-asr1004-1-confg !
6175 bytes copied in 0.700 secs (8821 bytes/sec)
```

Step 2: From the console of the new hub MC, 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 loopback interfaces on the original hub MC

In this procedure, you configure system settings on the original hub MC to accommodate the new hub MC HA.

Step 1: Change the IP address of the 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 Loopback0
 description Device Management Loopback
 ip address 10.6.32.253 255.255.255.255
```

Step 2: Configure the IP address of the PfR loopback interface.

Use the original IP address of the loopback0 interface for PfR in order to avoid changing the hub master configuration for all of the hub BR and remote site routers.

Increase the **hold-queue in** and **hold-queue out** to a queue length of 1024 on the loopback interface to allow the RTP application-table to be properly exported using Flexible Net Flow.

```
interface Loopback1
 description PfR Loopback w/ IP Anycast
 ip address 10.6.32.252 255.255.255.255
 hold-queue 1024 in
 hold-queue 1024 out
```

Procedure 3 Configure the router-id on original hub MC

In this procedure, you configure system settings on the original hub MC to accommodate the new hub MC HA.

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 router-id

This design uses a best practice of assigning the router ID to a loopback address, so the router-id will have to be changed on the original hub MC to the new loopback0 address.

Step 1: Change the EIGRP router-id on the original hub MC.

```
router eigrp IWAN-EIGRP
 address-family ipv4 unicast autonomous-system 400
  eigrp router-id 10.6.32.253
 exit-address-family
```

Option 2: OSPF router-id

This design uses a best practice of assigning the router ID to a loopback address, so the router-id will have to be changed on the original hub MC to the new loopback0 address.

Step 1: Change the OSPF router-id on the original hub MC.

```
router ospf 100
 router-id 10.6.32.253
```

Procedure 4 Configure the loopback interfaces

In this procedure and the ones following, you configure system settings that are unique to the new hub MC HA.

Step 1: Configure the IP address of the 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 Loopback0
 description Device Management Loopback
 ip address 10.6.32.254 255.255.255.255
```

Step 2: Configure the IP address of the PfR loopback interface.

Use the original IP address of the loopback0 interface for PfR in order to avoid changing the hub master configuration for all of the hub BR and remote site routers. Change the network mask to a /31 for IP anycast.

Increase the **hold-queue in** and **hold-queue out** to a queue length of 1024 on the loopback interface to allow the RTP application-table to be properly exported using Flexible Net Flow.

```
interface Loopback1
 description PfR Loopback w/ IP Anycast
 ip address 10.6.32.252 255.255.255.254
 hold-queue 1024 in
 hold-queue 1024 out
```

Procedure 5 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 and an IP address that is different from the first hub MC.

Step 1: Configure a Layer 3 interface.

```
interface Port-channel23
  description IW-WAN-D3750X
  ip address 10.6.32.164 255.255.255.192
  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 IW-WAN-D3750X Gig1/0/14

interface GigabitEthernet0/0/1
 description IW-WAN-D3750X Gig2/0/14

interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
  no ip address
  cdp enable
  channel-group 23
  no shutdown
```

Procedure 6 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

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

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
  eigrp router-id 10.6.32.254
 exit-address-family
```

Step 2: Configure the EIGRP interface.

Allow EIGRP to form neighbor relationships across the interface in order 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-channel23
   no passive-interface
   authentication mode md5
   authentication key-chain LAN-KEY
  exit-af-interface
 exit-address-family
```

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 10.6.32.254
```

Step 2: Remove passive interface for the LAN interface.

```
router ospf 100
 no passive-interface Port-channel23
```

Procedure 7 Test the failover from the primary hub MC

Optional

Use this optional procedure if you want to test the failover to the second hub MC. Skip this procedure if you do not want to test the HA functionality of your hub MC.

During a primary hub MC failure, the remote site will register with the hub MC HA as soon as the branch MC sends the next set of smart probes. The branch MC will continue to use the existing PfR policies until the swi-tchover occurs. If you follow the procedures outlined above, the hub MC HA policy will be identical to the primary hub MC policy.

Step 1: To monitor the progress, log into the second hub MC HA from the console port or using SSH.

Step 2: If you plan to use SSH, turn on console monitoring with **terminal monitor**.

```
DI-MC-ASR1004-2#terminal monitor
```

Step 3: From the console port of primary hub MC, turn off the port-channel interface to the LAN to simulate a failure.

```
DI-MC-ASR1004-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DI-MC-ASR1004-1(config)#interface Port-channel22
DI-MC-ASR1004-1(config-if)#shut
```

Step 4: From the second hub MC HA, you will see the following messages when the hub BRs and branch MCs register to the backup MC. Depending on the size of the IWAN domain, this step can take several minutes to complete.

```
DI-MC-ASR1004-2#
Sep 16 13:25:26.375: %DUAL-5-NBRCHANGE: EIGRP-IPv4 400: Neighbor 10.6.32.163 
(Port-channel23) is down: holding time expired
10.255.246.43 (Loopback0) is up: new adjacency
Sep 16 13:26:37.629: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.6.32.247 
(Loopback0) is up: new adjacency
Sep 16 13:27:00.748: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.255.246.13 
(Loopback0) is up: new adjacency
Sep 16 13:27:04.580: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.6.32.246 
(Loopback0) is up: new adjacency
Sep 16 13:27:20.402: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.255.246.44 
(Loopback0) is up: new adjacency
Sep 16 13:27:23.259: %DUAL-5-NBRCHANGE: EIGRP-SFv4 59501: Neighbor 10.255.246.14 
(Loopback0) is up: new adjacency
```

Step 5: After the messages stop, confirm that the second hub MC is acting as the hub MC with **show domain [domain name] master status**.

```
DI-MC-ASR1004-2#show domain iwan2 master status
  *** Domain MC Status ***
 Master VRF: Global
  Instance Type:    Hub
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 10.6.32.252
  Global Config Last Publish status: Peering Success
  Load Balancing:
   Admin Status: Enabled
   Operational Status: Up
   Enterprise top level prefixes configured: 1
   Max Calculated Utilization Variance: 0%
   Last load balance attempt: never
   Last Reason:  Variance less than 20%
   Total unbalanced bandwidth:
         External links: 0 Kbps  Internet links: 0 Kbps
  External Collector: 10.4.48.36 port: 9991
  Route Control: Enabled
  Transit Site Affinity: Enabled
  Load Sharing: Enabled
  Mitigation mode Aggressive: Disabled
  Policy threshold variance: 20
  Minimum Mask Length: 28
  Syslog TCA suppress timer: 180 seconds
  Traffic-Class Age out Timer: 5 minutes
  Channel Unreachable Threshold Timer: 4 seconds
  Minimum Packet Loss Calculation Threshold: 15 packets
  Minimum Bytes Loss Calculation Threshold: 1 bytes
  Borders:
    IP address: 10.6.32.246
    Version: 2
    Connection status: CONNECTED (Last Updated 00:00:54 ago )
    Interfaces configured:
      Name: Tunnel20 | type: external | Service Provider: INET1 path-id:1 | 
Status: UP | Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0
    Tunnel if: Tunnel0
    IP address: 10.6.32.247
    Version: 2
    Connection status: CONNECTED (Last Updated 00:00:52 ago )
    Interfaces configured:
      Name: Tunnel21 | type: external | Service Provider: INET2 path-id:2 | 
Status: UP | Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0
    Tunnel if: Tunnel0
```

After you have verified that the second hub MC is operational, log into the primary hub MC to bring it back online.

Step 6: From the console port of the primary hub MC, turn on the port-channel interface to the LAN.

```
DI-MC-ASR1004-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DI-MC-ASR1004-1(config)#interface Port-channel22
DI-MC-ASR1004-1(config-if)#no shut
```

PROCESS

Configuring Hub Border Router Scalability

1. Copy the configuration from existing router to the new router
2. Configure the hub BR platform
3. Configure connectivity to the LAN
4. Configure the routing protocol for the LAN
5. Connect to the Internet
6. Configure the mGRE tunnel
7. Configure network address translation on the firewall
8. Configure PfR domain in the hub BR
9. Configure remote sites for additional hub BRs

Use this optional process if you want to deploy additional hub BRs at the same location for horizontal scaling. Skip this process if you do not want to horizontally scale your hub BRs.

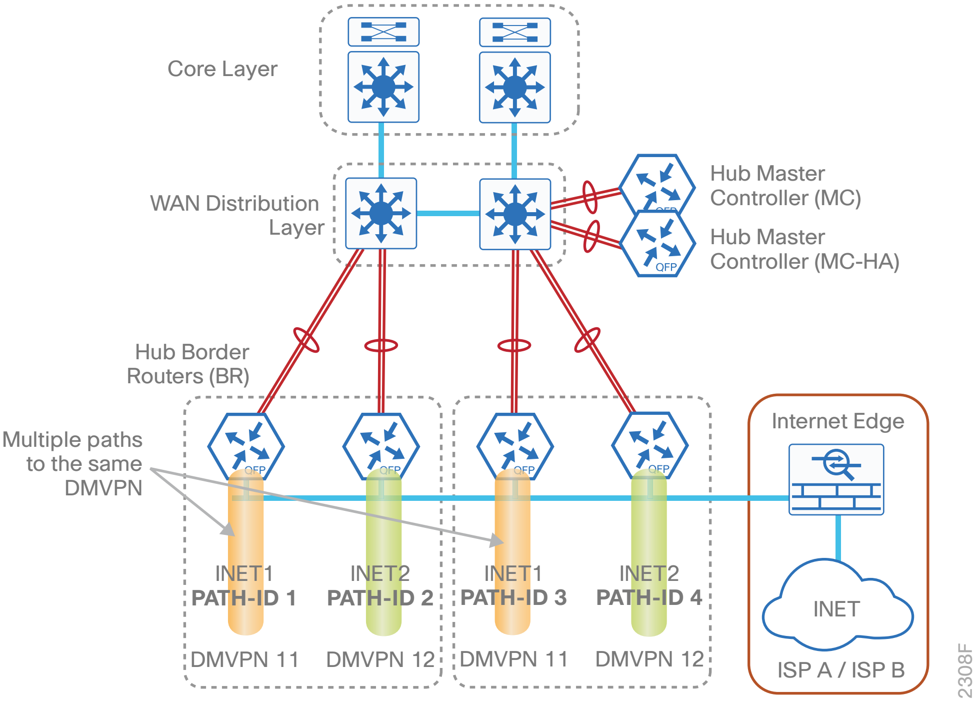
This concept works with any of the IWAN design models.

This type of configuration offers the following benefits:

- Distribute traffic across multiple hub BRs on a single DMVPN to utilize all WAN and router capacity
- Convergence across hub BRs should only occur when all exits in a hub BR fail or reach their maximum bandwidth limits
- If the current exit to a remote site fails, converge to an alternate exit on the same (DMVPN1) network or converge to the alternate (DMVPN2) network

The following diagram shows two additional hub BRs and where they fit into the IWAN dual Internet design model.

Figure 2 IWAN dual Internet design model—Hub BR scalability



For this process, you configure two additional hub BRs with base configurations similar to the existing hub BRs'. You have to make changes to the base configurations and the remote site routers in order to take advantage of the new hub BRs

The additional routers have unique path information, IP addresses, and port-channel assignments, but the rest of the configurations are the same.

Table 2 Hub BR path and IP addresses

Host name	Path	Path ID	Loopback IP address	Port-channel IP address	Internet DMZ IP address
DI-INET1-ASR1002X-11	INET1	1	10.6.32.246/32	10.6.32.42/30	192.168.146.20/24
DI-INET1-ASR1002X-12	INET2	2	10.6.32.247/32	10.6.32.46/30	192.168.146.21/24
DI-INET1-ASR1002X-11b	INET1	3	10.6.32.248/32	10.6.32.50/30	192.168.146.22/24
DI-INET1-ASR1002X-12b	INET2	4	10.6.32.249/32	10.6.32.54/30	192.168.146.23/24

Follow the process "Configuring DMVPN Hub Router" using the base PfR information from the first two hub BRs. Make the required changes from the procedures below to horizontally scale your IWAN domain.

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

Optional

If the hardware for the corresponding hub BR is identical to the first, 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. Skip this procedure if you do not want to copy the configuration from an existing router.

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

```
DI-INET1-ASR1002X-11# copy running-config ftp://cisco:cisco@10.4.48.27
Address or name of remote host [10.4.48.27]?
Destination filename [di-inet1-asr1002x-11-confg]?
Writing di-inet1-asr1002x-11-config !
13228 bytes copied in 0.7500 secs (9921 bytes/sec)
```

Step 2: From the console of the new hub 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 hub BR platform

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

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

```
hostname DI-INET1-ASR1002X-11b
```

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 10.6.32.248 255.255.255.255
```

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 and an IP address that is different from the other hub BRs.

Step 1: Configure a Layer 3 interface.

```
interface Port-channel13
  description IW-WAN-D3750X
  ip address 10.6.32.50 255.255.255.252
  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 IW-WAN-D3750X Gig1/0/5

interface GigabitEthernet0/0/1
 description IW-WAN-D3750X Gig2/0/5

interface range GigabitEthernet0/0/0, GigabitEthernet0/0/1
  no ip address
  cdp enable
  channel-group 13
  no shutdown
```

Procedure 4 Configure the routing protocol for the LAN

The following table shows the EIGRP LAN delay in use.

Table 3 EIGRP LAN delay for IWAN hub routers

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

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

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
  eigrp router-id 10.6.32.248
 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-channel13
   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-channel13
  delay 50000
```

Procedure 5 Connect to the Internet

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 in order 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.

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

```
interface GigabitEthernet0/0/3
 description INET1
 vrf forwarding IWAN-TRANSPORT-11
 ip address 192.168.146.22 255.255.255.0
 no shutdown
```

Procedure 6 Configure the mGRE tunnel

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

Table 4 *DMVPN tunnel parameters*

Hostname	Tunnel type	Tunnel number	Tunnel IP address
DI-INET1-ASR1002X-11b	INET1	20	10.6.64.2/23
DI-INET1-ASR1002X-12b	INET2	21	10.6.66.2/23

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 Tunnel20
 ip address 10.6.64.2 255.255.254.0
```

Step 2: Configure NHRP.

Hub BRs require an additional configuration statement in order to create an EIGRP neighbor adjacency with the other hub BR. This statement includes the NBMA definition for the DMVPN hub router tunnel endpoint.

The routing protocol relies on a multicast transport and requires that NHRP automatically add routers to the multicast NHRP mappings.

The value used for the NHS is the mGRE tunnel address for the DMVPN hub router. The NBMA entry must be set to the hub router's DMZ IP address because both of the hub routers are behind the firewall. This design uses the values shown in the following table.

Table 5 NHRP parameters

Hostname	Tunnel type	Tunnel number	Tunnel IP address	DMZ IP address
DI-INET1-ASR1002X-11	INET1	20	10.6.64.1	192.168.146.20
DI-INET1-ASR1002X-12	INET2	21	10.6.66.1	192.168.146.21
DI-INET1-ASR1002X-11b	INET1	20	10.6.64.2	192.168.146.22
DI-INET1-ASR1002X-12b	INET2	21	10.6.66.2	192.168.146.23

The two corresponding hub BRs must point at each other in order to allow an EIGRP neighbor adjacency to be formed. For the nbma address on the adjacent hub BRs, use the DMZ IP address instead of the externally routable IP address.

Example: INET1 hub border router—DI-INET1-ASR1002X-11

```
interface Tunnel20
 ip nhrp nhs 10.6.64.2 nbma 192.168.146.22 multicast
```

Example: INET1 transit border router—DI-INET1-ASR1002X-11b

```
interface Tunnel20
 ip nhrp nhs 10.6.64.1 nbma 192.168.146.20 multicast
```

Procedure 7 Configure network address translation on the firewall

You have to add the new hub BRs to your existing 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 table.

Table 6 DMVPN NAT address mapping

Hostname	DMVPN hub router DMZ address	DMVPN hub router public address (externally routable after NAT)
DI-INET1-ASR1002X-11b	192.168.146.22	172.16.140.12 (ISP-A)
DI-INET1-ASR1002X-12b	192.168.146.23	172.17.140.12 (ISP-B)

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

Table 7 External DMZ firewall network objects

Network object name	Object type	IP address	Description
outside-dmvpn-11b-ISPa	Host	172.16.140.12	DMVPN hub router 11b on ISP A (outside)
outside-dmvpn-12b-ISPb	Host	172.17.140.12	DMVPN hub router 12b on ISP B (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-11b-ISPa)

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

Step 5: In the **IP Address** box, enter the address. (Example: 172.16.140.12)

Step 6: In the **Description** box, enter a useful description, and then click **OK**. (Example: DMVPN hub router 11b on ISP A)

Step 7: Repeat Step 2 through Step 6 for each object listed in the table above. 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 8 Private DMZ firewall network objects

Network object name	Object type	IP address	Description
dmz-dmvpn-11b	Host	192.168.146.22	DMVPN hub router 11b on vpn-dmz
dmz-dmvpn-12b	Host	192.168.146.23	DMVPN hub router 12b 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-11b)

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

Step 13: In the **IP Address** box, enter the address. (Example: 192.168.146.22)

Step 14: In the **Description** box, enter a useful description, and then click **OK**. (Example: DMVPN hub router 11b 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-11b-ISPa)

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**.

Procedure 8 Configure PfR domain in the hub BR

The additional hub 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 MC. The hub BR routers are also used to advertise the path names and path-ids specified in the hub MC configuration.

Step 1: Create the hub BR domain.

```
domain [name]
 vrf [name]
  border (create the BR)
   source-interface [interface]
   master [PfR loopback IP address of local MC]
   password [password of hub MC]
```

Example

```
domain iwan2
 vrf default
  border
   source-interface Loopback0
   master 10.6.32.252
   password c1sco123
```

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

```
interface Tunnel [value]
 domain [name] path [name] path-id [number]
```

Example

This example is the additional hub BR using Tunnel 20 with INET1 as the provider.

```
interface Tunnel20
 domain iwan2 path INET1 path-id 3
```

This example is the additional hub BR using Tunnel 21 with INET2 as the provider.

```
interface Tunnel21
 domain iwan2 path INET2 path-id 4
```

Step 3: Verify the border is operational by using the **show domain [name] border status** command.

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

Procedure 9 Configure remote sites for additional hub BRs

An additional NHRP command has to be added to the tunnel interfaces of remote site BRs for them to begin using the new hub BRs.

Table 9 *NHRP parameters for additional hub BRs*

Hostname	Tunnel number	Tunnel IP address	Public IP address
DI-INET1-ASR1002X-11b	20	10.6.38.2	172.16.140.12 (ISP A)
DI-INET1-ASR1002X-12b	21	10.6.40.2	172.17.140.12 (ISP B)

Step 1: Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes. Remote routers use NHRP in order to determine the tunnel destinations for peers attached to the mGRE tunnel.

The spoke router requires an additional configuration statement in order to define the NHRP server. This statement includes the NBMA definition for the DMVPN hub router tunnel endpoint. Spoke routers require the NHRP multicast keyword in this statement.

The value used for the NHS is the mGRE tunnel address for the DMVPN hub router. The NBMA entry must be set to either the MPLS DMVPN hub router's actual public address or the outside NAT value of the DMVPN hub, as configured on the Cisco ASA 5500. This design uses the values shown in the table above.

Example: Single-router remote site for dual INET–RS13-2911

```
interface Tunnel20
 ip nhrp nhs 10.6.64.2 nbma 172.16.140.12 multicast

interface Tunnel21
 ip nhrp nhs 10.6.66.2 nbma 172.17.140.12 multicast
```

Step 2: Confirm that the new hub BRs are reachable with **show ip eigrp neighbors**.

```
RS13-2911#show ip eigrp neighbors
EIGRP-IPv4 VR(IWAN-EIGRP) Address-Family Neighbors for AS(400)
H   Address       Interface    Hold Uptime   SRTT   RTO  Q  Seq
                               (sec)         (ms)       Cnt Num
2   10.6.64.2     Tu20           42 1d01h       1   100  0  574
3   10.6.64.1     Tu20           58 1d01h       1   100  0  631
1   10.6.66.2     Tu21           59 1d02h       1   100  0  646
0   10.6.66.1     Tu21           55 1d02h       1   100  0  804
```

Step 3: Repeat this procedure for each remote site that will use the new hub BRs.

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:
    - Removed EIGRP tagging and filtering, which is no longer needed for the hub BR scalability configuration
- 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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.