

CI CO

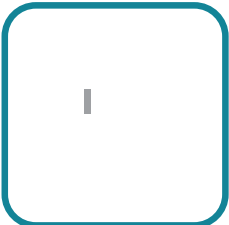


Table of Contents

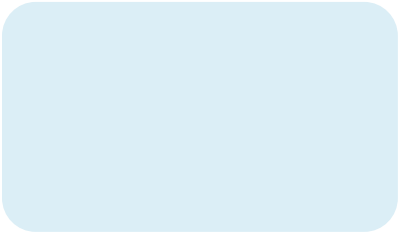
- Preface..... 1
- CVD Navigator..... 2
 - Use Cases2
 - Scope2
 - Pro ciency >. 6D-70.00.7(..... 3..... C)-16(o)-9

Deploying the Transport Independent Design 20

- Design Overview20
- DMVPN Hub Routers.....20

CVD Navigator

Figure 9 - IWAN dual router remote-site: Connection to distribution layer



IP Multicast

Figure 11 -

The IP routing is straightforward and can be handled entirely by static routes at the WAN-aggregation site and static default routes at the remote site. However, there is significant value to configuring this type of site with

Design Details

EIGRP

Cisco uses EIGRP as the primary routing protocol because it is easy to configure, does not require a large

There are dynamic methods for network clients to discover the path MTU, which allow the clients to reduce the size of packets they transmit. However, in many cases, these dynamic methods are unsuccessful, typically because security devices filter the necessary discovery traffic. This failure to discover the path MTU drives the need for a method that can reliably inform network clients of the appropriate packet size. The solution is to implement the `ip tcp adjust mss [size]` command on the WAN routers, which influences the TCP maximum window size.

Each interface is in its own VRF and there is no routing between the interfaces. Three static routes allow the IOS CA to reach each network individually.

Figure 19 - IOS CA with three non-routed inieg

Terminal access controller access control system plus (TACACS+) is the primary protocol used to authenticate management logins on the infrastructure devices to the AAA server. A local AAA user database is also defined (in Step 2) on each network infrastructure device in order to provide a fallback authentication source in case the



Configuring DMVPN Hub Router

1. Configure the distribution switch
- 2.





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-2 0.0.0.0 0.0.0.0 192.168.146.1
```




Step 2:





Step 12: Click Apply.



Step 13: In Configuration > Device Management > High Availability > click Failover.

Step 14: On the Interfaces tab, for the interface created in Step 4, enter the IP address of the standby unit in the Standby IP address

Step 17: (Optional) Repeat this procedure for the IOS CA VLAN by using the appropriate information.

Step 8: After adding all of the objects listed, click **Apply** on the Network Objects/Groups pane. Next, you add a network object for the private DMZ address of the DMVPN hub router.

Table 20 - Private DMZ firewall network objects

Table 21 - Firewall policy rules for DMZ-VPN DMVPN hub routers





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

Table 24 -

Step 3:

Because the DMVPN hub router is behind a NAT device, the IPsec transform must be configured for transport

Option 1:

Step 2:

Option 2: Configure with a certificate authority

The `crypto pki trustpoint` is the method of specifying the parameters associated with a CA. This router has already authenticated to the CA and enrolled in order to obtain its identity certificate in a previous procedure.

Step 1:

Enabling encryption on this interface requires the application of the IPsec profile configured in the previous procedure.

```
interface Tunnel11
  tunnel source GigabitEthernet0/1
  tunnel mode gre multipoint
  tunnel key 102
  tunnel vrf IWAN-TRANSPORT-2
  tunnel protection ipsec profile DMVPN-PROFILE-TRANSPORT-2
```

Step 3: Configure NHRP.

The DMVPN hub router is the NHRP server for all of the spokes in the DMVPN cloud.

Step 2: Configure and apply the access list.



Configuring Remote-Site DMVPN Router (Router 2)

- 1.





Step 2:



Step 3: 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 Tunnel11  
  ip pim dr-priority 0
```



```
ip pim sparse-mode
standby version 2
standby 1 ip 10.7.19.1
standby 1 priority 105
standby 1 preempt
standby 1 authentication md5 key-string cisco123
```







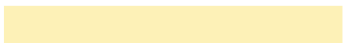
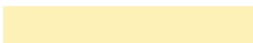



Applying DMVPN QoS Policy to DMVPN Hub Routers

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



Step 1:



The first design model is the IWAN Hybrid, which uses a primary MPLS transport paired with Internet VPN as a secondary transport. In this design model, the MPLS WAN provides SLA class of service guarantees for key

Configuring PfR Hub Master Controller

- 1.





Example

This example shows a primary site network with two class B private address blocks of 10.4.0.0 and 10.6.0.0.

```
ip prefix-list
```








[Redacted]

[Redacted]

[Redacted]

[Redacted]



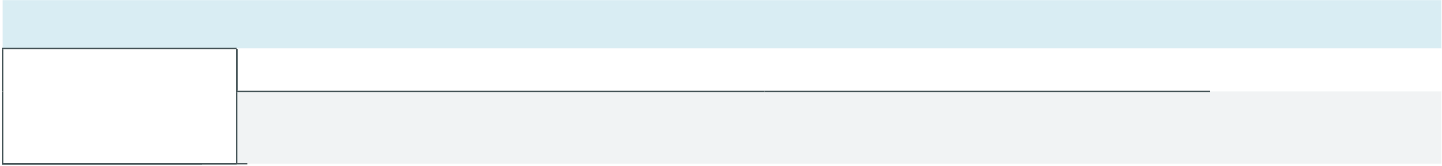
Deploying IWAN Monitoring





Appendix A: Product List

WAN Aggregation



--

Internet Edge

Internet Edge				



Please use the [feedback form](#) to send us your feedback.

|