



Apply Network Wide Settings

Applying Network Wide Settings occurs after changes have been entered in Network Wide Settings. This includes further hub router configuration.

- [Apply Changes, page 5-1](#)
- [Hub Router Configuration, page 5-1](#)

Apply Changes

This (Apply Changes) section might not be required since the Save and Continue option performs this action now. Please confirm



Note

(Important) Before clicking Apply Changes, ensure that the settings you applied when setting up the hub site settings are as expected. If the settings are incorrect, and you click Apply Changes below, you will need to perform the installation again.

After checking the hub site settings and reviewing the settings that you made, click **Apply Changes**—available on the right side of the window. You may choose to apply changes immediately or schedule a time to apply the changes in the future.



Note

The **Apply Now** option does not check for validations in conflict with future scheduled workflows. Please reevaluate scheduled jobs based on these changes and update scheduled jobs as required. If there is a conflict when the scheduled job is activated, it may fail at that time.

Wait a short while for the hub routers to be provisioned based on previous settings in [Configure Hub Site and Settings, page 4-1](#).

Hub Router Configuration

Apply the following configurations to the hub router.

- [Additional LAN Routing Protocol Configuration, page 5-2](#)
- [Route Leak Configuration, page 5-2](#)
- [Add Loopback47233 and LAN Interfaces, page 5-3](#)

- [Create Prefix Lists, page 5-3](#)
- [Add Prefix Lists in the Hub1/Master Controller Configuration, page 5-4](#)
- [Route filtering for Redistribution, page 5-4](#)
- [Route Leaking, page 5-6](#)

Additional LAN Routing Protocol Configuration

When IWAN App is behind a hub core router and not connected directly to a hub branch router, the following configuration must be entered in the hub router for specifying the LAN routing protocol. This is to ensure that IWAN App is aware of reaching WAN when the hub branch WAN is configured under a VPN routing and forwarding (VRF).

```
ip access-list extended APP
 permit 172.16.0.0 0.0.255.255
route-map WAN-TO-APP permit 10
 match ip address APP
 set global
ip route 172.16.0.0 255.255.0.0 GigabitEthernet0/0/1 254
```

Enter the following configuration in the hub router, if the LAN protocol used is EIGRP 400:

```
router eigrp IWAN-EIGRP
 !
 address-family ipv4 unicast autonomous-system 400
 !
 topology base
 redistribute eigrp 200 route-map SET-TAG-ALL
```

Enter the following configuration in the hub router, if the LAN protocol used is EIGRP 100:

```
router bgp 6500
 redistribute eigrp 400
```

Enter the following configuration in the hub router, if the LAN protocol used is BGP:

```
router bgp 6500
 redistribute eigrp 400
```

Enter the following configuration in the hub router, if the LAN protocol used is OSPF:

```
router ospf 100
 redistribute eigrp 400
```

Route Leak Configuration

The following additional route leak configuration is required for virtual IP support in multi-host, high availability -(HA) based controller environments. Route leak configuration is required for connection between controller (IWAN App) and spoke after VRF is configured on the hub branch. IWAN App leverages the virtual IP address of the cluster to automatically configure the route leaks. However, the controller uses virtual IP address as inbound connection and uses physical IP address of the service resident host for outbound traffic. Thus, route leak is required for all three physical IP addresses of the cluster along with virtual IP address.

```
ip access-list extended APP
 permit ip any host 192.168.20.2 //virtual IP address, already available in the
configuration
```

```
permit ip any host 10.88.182.235 //virtual IP address, already available in the
configuration
permit ip any host 192.168.20.101 //To manually add the physical IP address
permit ip any host 192.168.20.102 //To manually add the physical IP address
permit ip any host 192.168.20.103 //To manually add the physical IP address
```

Add Loopback47233 and LAN Interfaces

For the hub router, apply configuration steps such as the ones in the example below. This adds the loopback47233 interface and LAN interface to the EIGRP routing added by IWAN on APIC-EM.

EIGRP should be configured on the router or switch connected to the LAN interfaces of the hub.

Example

```
router eigrp IWAN-EIGRP
!
address-family ipv4 unicast autonomous-system 400
!
af-interface default
passive-interface
exit-af-interface
!
af-interface GigabitEthernet0/0/0 (LAN interface)
no passive-interface
exit-af-interface

af-interface Tunnel11
authentication mode md5
authentication key-chain WAN-KEY
hello-interval 20
hold-time 60
no next-hop-self
no split-horizon
exit-af-interface
!
topology base
exit-af-topology
network 10.0.0.0 0.1.255.255
network 10.0.1.129 0.0.0.0 • (Network for loopback0)
network 10.8.0.0 0.0.255.255 •(Network for the HUB site & Data Center)
eigrp router-id 10.0.1.129
```

Create Prefix Lists

The following sections describe how to create prefix lists for the enterprise and data center (or hub site), used for PFRv3.

- [Enterprise Prefix, page 5-3](#)
- [Site Prefix, page 5-4](#)

Enterprise Prefix

Create an enterprise prefix list to match IP packets or routes.

Example

```
ip prefix-list ENTERPRISE_PREFIX seq 10 permit 10.0.0.0/8
```

The enterprise prefix list is mainly used to determine the enterprise boundary. IP prefixes can be summarized routes.

Using an enterprise prefix list ensures that traffic that goes towards a remote site router that is not PfR-enabled will not be influenced by load balancing. Otherwise, if you do not use an enterprise prefix list, traffic going towards a remote site router that is not PfR-enabled will be learned as an internet traffic class and subjected to load balancing.

Site Prefix

Create a site prefix list to match IP packets or routes.

Example

```
ip prefix-list DC_PREFIX seq 10 permit 10.8.0.0/16
```

Include IP prefixes that are part of the data center (hub site).

Add Prefix Lists in the Hub1/Master Controller Configuration

In the hub router configuration, include steps such as the ones shown in the following example.

Example

```
domain ONE
vrf default
master hub
source-interface Loopback47233
enterprise-prefix prefix-list ENTERPRISE_PREFIX
site-prefixes prefix-list DC1_PREFIX
```

Route filtering for Redistribution

This design uses a single EIGRP autonomous system for the WAN and all of the WAN remote sites. Every remote site is connected for resiliency. However, due to the multiple paths that exist within this topology, effort must be made to avoid routing loops and to prevent remote sites from becoming transit sites if WAN failures were to occur.

The following logic is used to control the routing.

- All prefixes that are advertised towards the WAN are tagged with the DMVPN of the hub that advertises the route.
- All prefixes, except those that originate locally from a hub, that are advertised towards the LAN are tagged with the DMVPN of the hub that advertises the route.
- The IWAN design always uses DMVPN hub routers in pairs. Each DMVPN hub router blocks routes from the LAN that are tagged with the opposite hub's DMVPN.

Outbound distribute-lists are used to set tags on the DMVPN hub routers towards the WAN and LAN. The tags set towards the WAN are used by the remote-site routers to protect against becoming transit sites.

An inbound distribute-list is used on the DMVPN hub routers to limit which routes are accepted for installation into the route table. These routers are configured to only accept routes which do not originate from the MPLS and DMVPN WAN sources. To do this task, the DMVPN learned WAN routes must be explicitly tagged by their DMVPN hub router during the route redistribution process. The specific route tags in use are shown in the following table.

In the table below 10.6.34.0 is used for Hub 1, DMVPN Tag Tunnel 10 and 10.6.36.0 for Hub 2, Tag Tunnel 11. Replace these tags with the Tunnel networks provisioned by IWAN on APIC-EM.

DMVPN Hub	DMVPN Prefix (tag)	Tag Tunnel	Tag LAN	Block LAN
Hub-1	10.6.34.0	100 (all routes)	10.6.34.0 (WAN routes)	Tagged 200
Hub-2	10.6.36.0	200 (all routes)	10.6.36.0 (WAN routes)	Tagged 100

For route filtering, configure Hub-1 and Hub-2 as shown in the examples below:

Example: Hub-1

```

route-map SET-TAG-ALL permit 10
  description tag all routes advertised through the tunnel
  set tag 100

ip access-list standard DMVPN-1-SPOKES
  permit 10.6.34.0 0.0.1.255

route-map SET-TAG-DMVPN-1 permit 100
  description tag routes sourced from DMVPN-1
  match ip route-source DMVPN-1-SPOKES
  set tag 100

route-map SET-TAG-DMVPN-1 permit 100
  description Advertise all other routes with no tag

route-map BLOCK-DMVPN-2 deny 10
  match tag 200
route-map BLOCK-DMVPN-2 permit 100

router eigrp IWAN-EIGRP?
  address-family ipv4 unicast autonomous-system 400
  topology base?
  distribute-list route-map SET-TAG-DMVPN-1 out GigabitEthernet0/0/0
  distribute-list route-map SET-TAG-ALL out Tunnel10
  distribute-list route-map BLOCK-DMVPN-2 in GigabitEthernet0/0/0

```

Example: Hub-2

```

route-map SET-TAG-ALL permit 10
  description tag all routes advertised through the tunnel
  set tag 200

ip access-list standard DMVPN-2-SPOKES
  permit 10.6.36.0 0.0.1.255

route-map SET-TAG-DMVPN-2 permit 10
  description tag routes sourced from DMVPN-2

```

```

match ip route-source DMVPN-2-SPOKES
set tag 200

route-map SET-TAG-DMVPN-2 permit 100
description Advertise all other routes with no tag

route-map BLOCK-DMVPN-1 deny 10
match tag 100
route-map BLOCK-DMVPN-1 permit 100

router eigrp IWAN-EIGRP
address-family ipv4 unicast autonomous-system 400
topology base?
distribute-list route-map SET-TAG-DMVPN-2 out GigabitEthernet0/0/0
distribute-list route-map SET-TAG-ALL out Tunnel11
distribute-list route-map BLOCK-DMVPN-1 in GigabitEthernet0/0/0

```

Route Leaking

Routes are redistributed between the LAN and WAN. IWAN Application pushes route leaking if the Cisco APIC-EM is not reachable through the DMZ interface.

Example

```

ip access-list extended IWAN-CONTROLLER
permit ip any 2.1.1.0 0.0.0.255 <<< 2.1.1.0 is subnet where Controller located
route-map MPLS-INTERNAL permit 10
match ip address IWAN-CONTROLLER
set global
int gig0/0/1
ip vrf forwarding IWAN-PRIMARY <<< VRF should match whatever P0 configured on this router
ip address 172.16.0.3 255.255.255.0
ip policy route-map MPLS-INTERNAL
ip route vrf IWAN-PRIMARY 0.0.0.0 0.0.0.0 172.16.0.5
ip route 172.16.0.0 255.255.255.0 int g0/0/1 <<< global route to 172.16.0.0/24

```

Where to go Next

After specifying network settings, go to [“Set Up Branch Sites, page 6-1”](#) shown on the main IWAN menu.