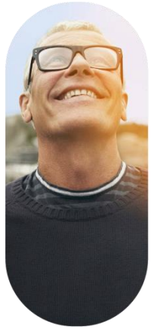
Design and Deployment using the Cisco Smart Business Architecture (SBA)



Anastasia Marchenko

Systems Engineer Cisco

amarchen@cisco.com

Design and Deployment Using SBA

Agenda

- SBA WAN Overview
- SBA WAN Design Methodology
- Key Aspects of the Design
- Summary

The Challenge

How can I anticipate what the network might need to do in the future so I don't have to revisit my design and deployment?

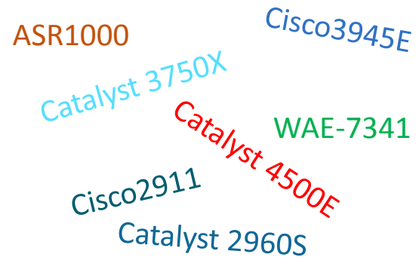
How can I do it quickly?

How do I manage it?

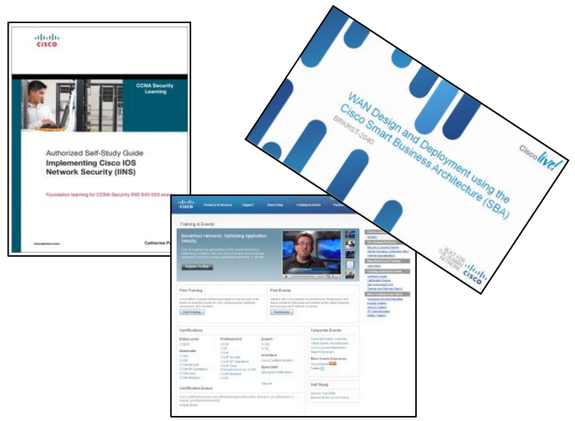
How do I put it all together?

Which platform should I choose?

Many to choose from at each place in the network



What are the best practices?

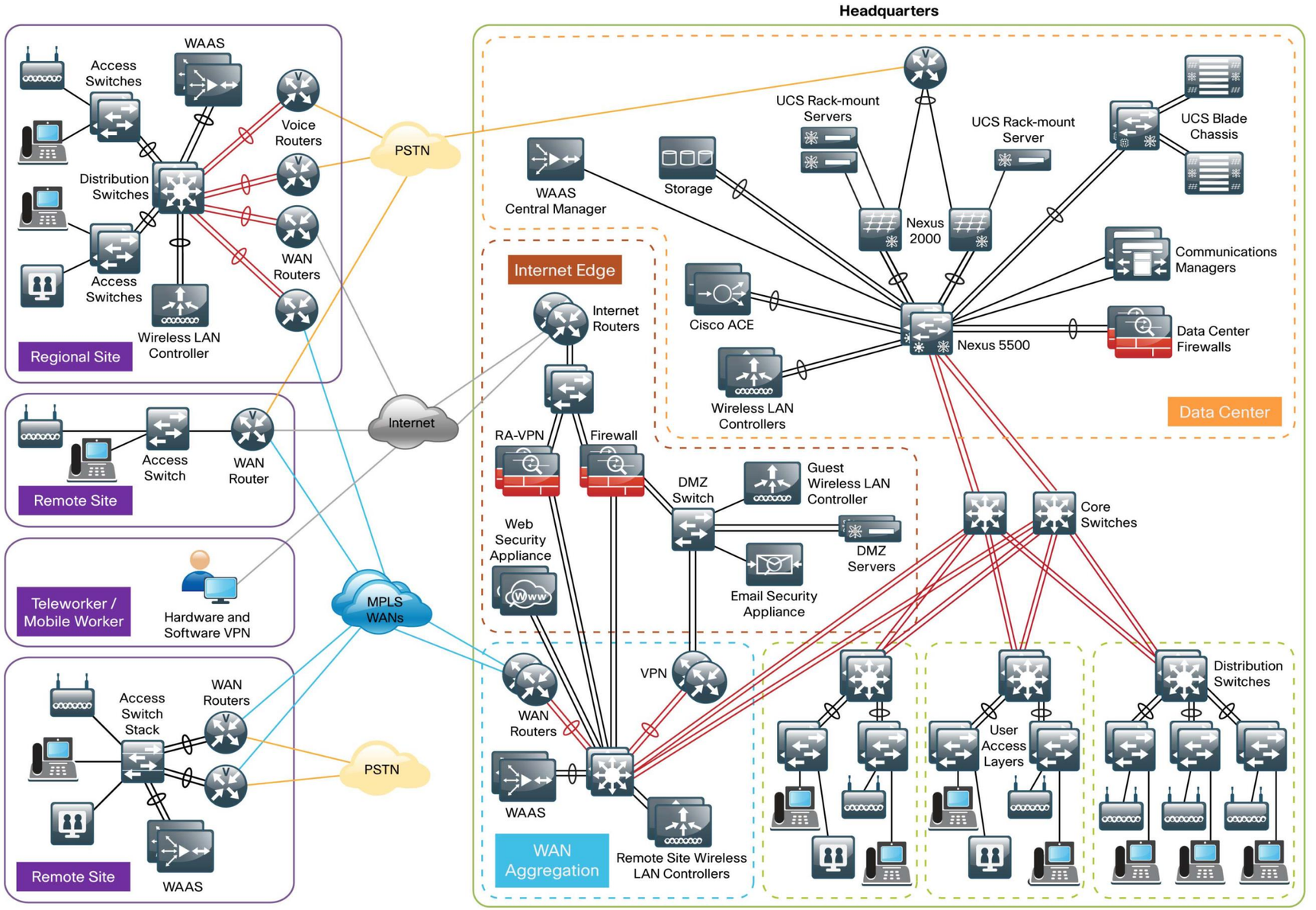


Cisco Smart Business Architecture

Overview

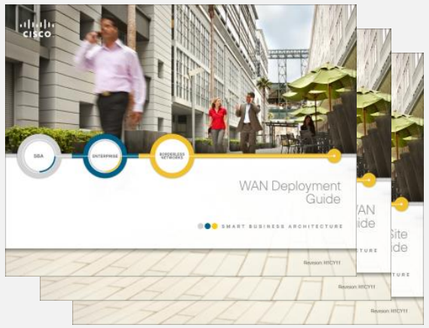
Tested	A **reference design**, tested, and supported by Cisco
Optimized	One architecture to scale for different size organizations Multiple tiers to match your organization's needs without changing the network architecture
Flexible	Flexible architecture to help ensure easy migration as the organization grows
Comprehensive	Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
Secure	Security and high availability for corporate information resources, and Internet-facing applications
Performance	Improved network performance and cost reduction through the use services like WAN optimization

Cisco SBA Design Overview



SBA WAN Deployment Principles

- **Ease of Deployment:** Deploy the design consistently across all products included in the architecture. The configurations used in the deployment represent a best-practice methodology to enable a fast and resilient deployment.
- **Flexibility and Scalability:** The architecture can grow with the organization without being redesigned.
- **Resiliency and Security:** The architecture keeps the network operating even during unplanned outages and attacks.
- **Easy to Manage:** The deployment guidance includes configuring devices to be managed by a network management system (NMS) or as unique elements of the network.
- **Advanced Technology Ready:** Implementing advanced technologies like collaboration is easy because the network foundation is already configured with the required baseline network services.



Borderless Networks SBA Guides for Enterprise:

MPLS WAN Deployment Guide
Layer 2 WAN Deployment Guide
VPN WAN Deployment Guide

http://www.cisco.com/go/sba

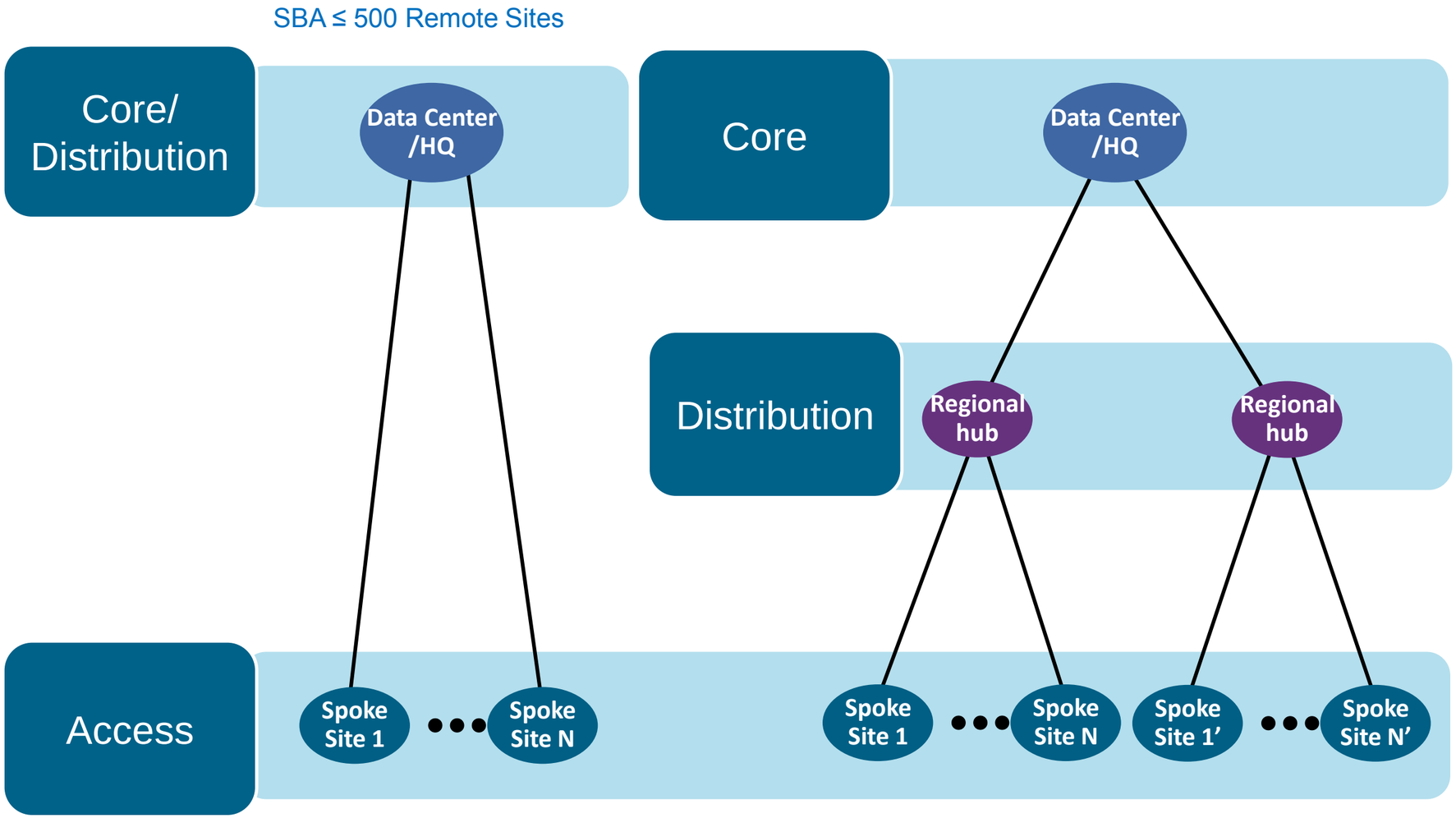
Deployment Guide	Transports	Usage	WAN Aggregation Design Models
MPLS WAN	MPLS L3 VPN	Primary/Secondary	Dual MPLS MPLS Dynamic MPLS Static
Layer 2 WAN	Layer 2 WAN	Primary	Trunked Demarcation Simple Demarcation
VPN WAN	Internet/DMVPN	Primary/Secondary	Dual DMVPN DMVPN Only DMVPN Backup Dedicated DMVPN Backup Shared
VPN Remote Site over 3G/4G	3G/4G Internet/DMVPN	Primary/Secondary	Remote site only
Group Encrypted Transport VPN	MPLS L3 VPN Layer 2 WAN	Primary/Secondary Primary	Compatible with all design models

WAN Design and Deployment Using SBA

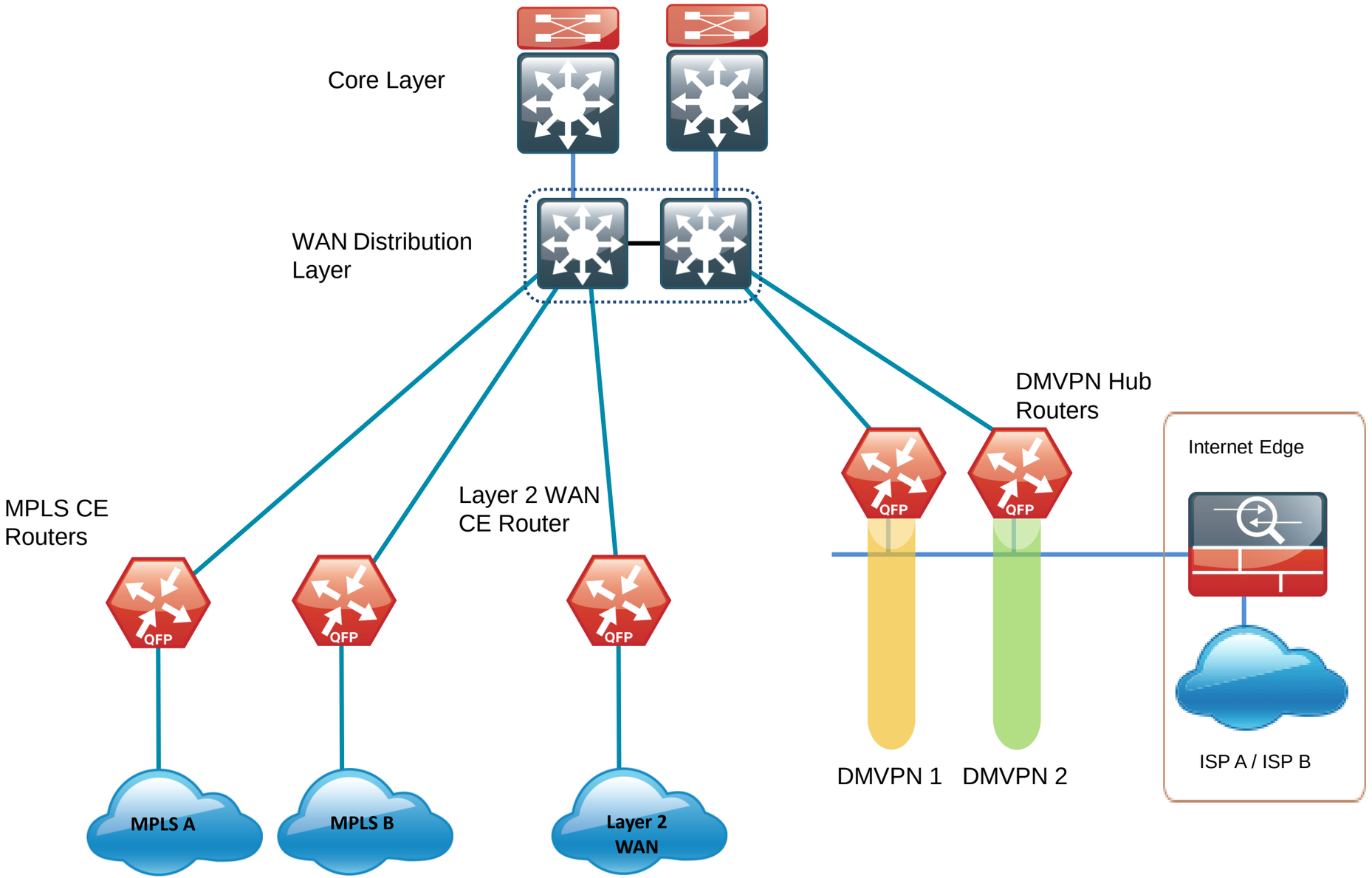
Agenda

- SBA WAN Overview
- SBA WAN Design Methodology
- Key Aspects of the Design
- Summary

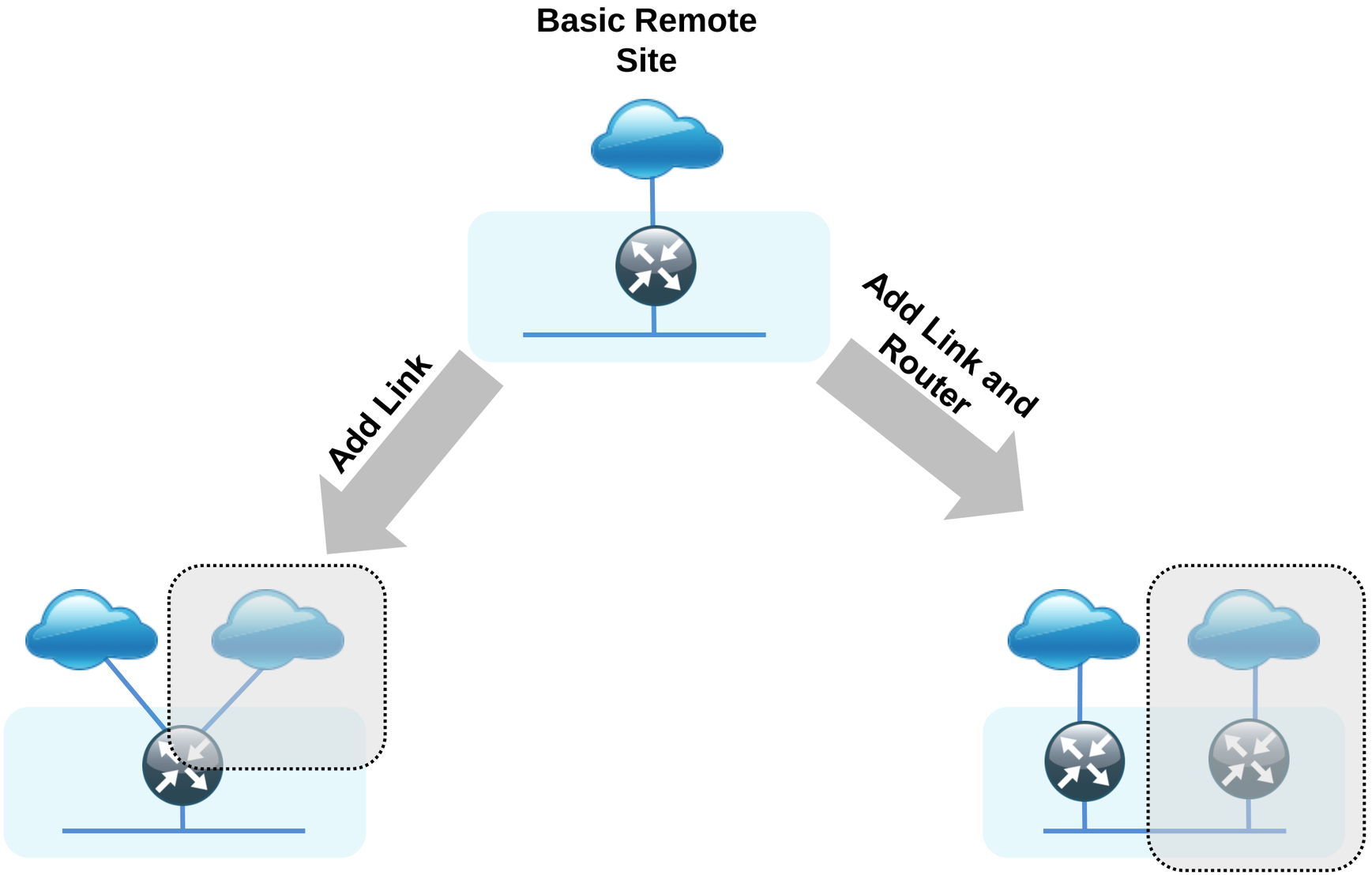
Hierarchical WAN Design



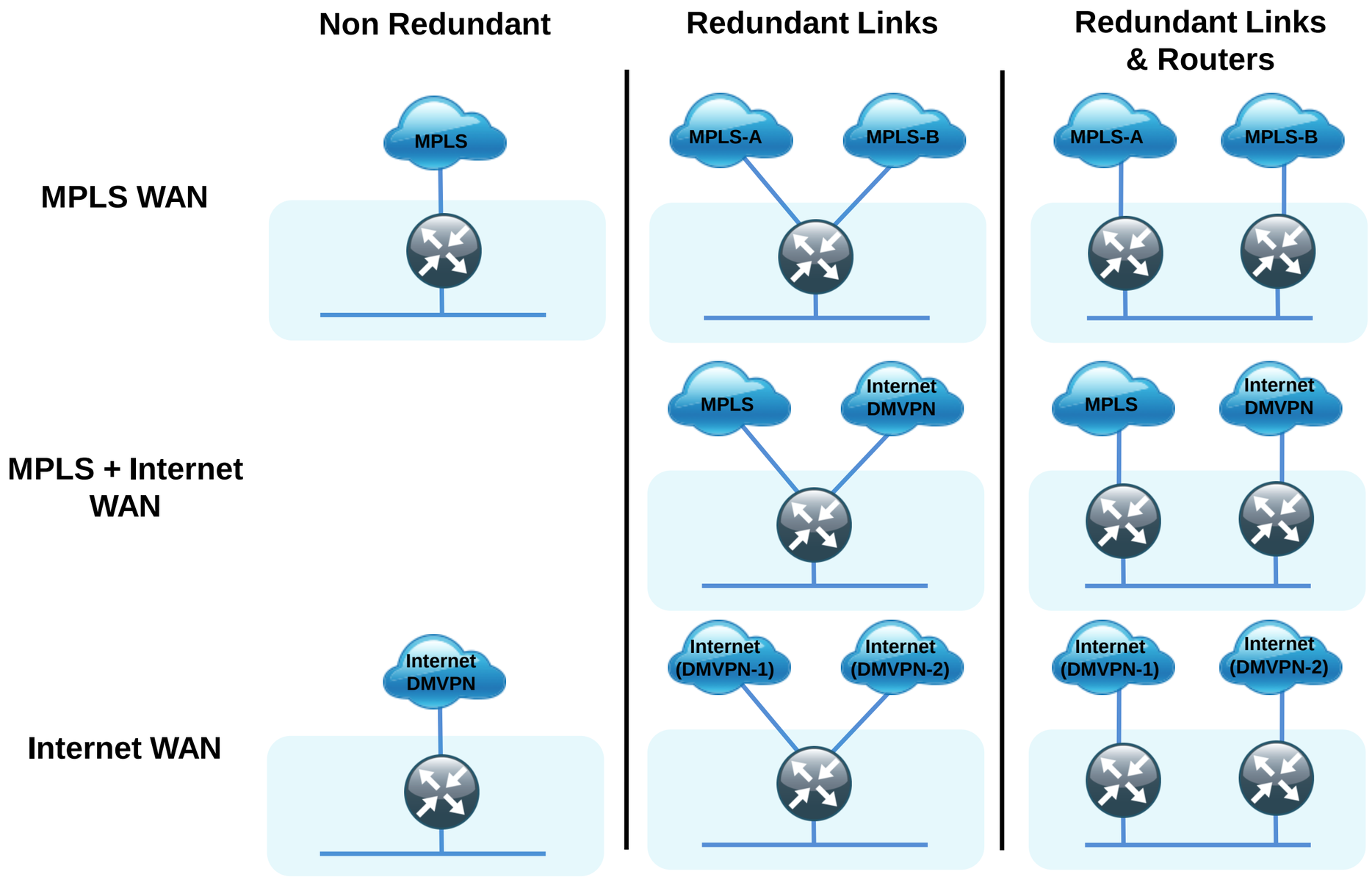
WAN-Aggregation Reference Design



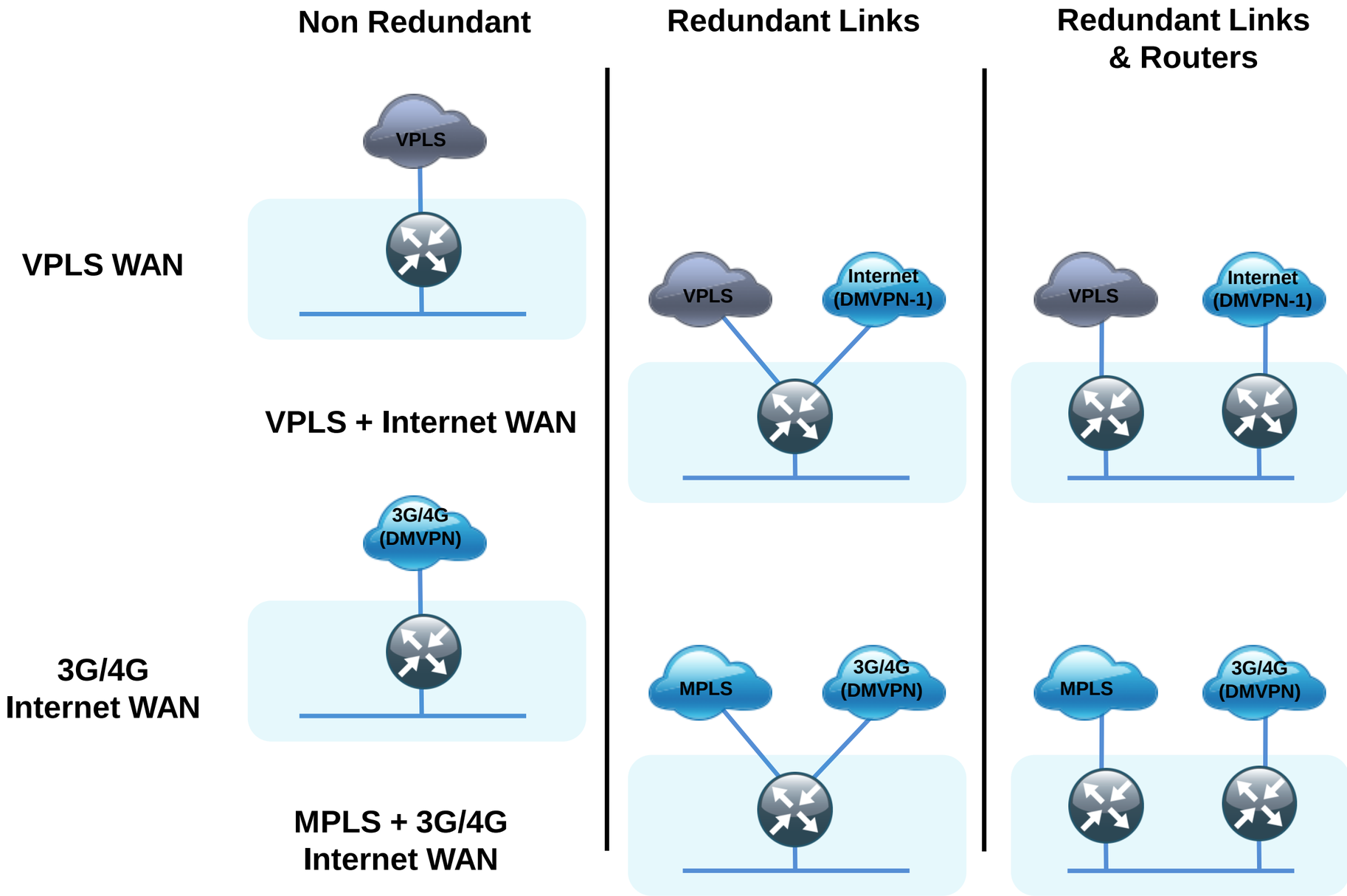
WAN Remote Site Designs



WAN Remote Site Designs (MPLS and DMVPN)

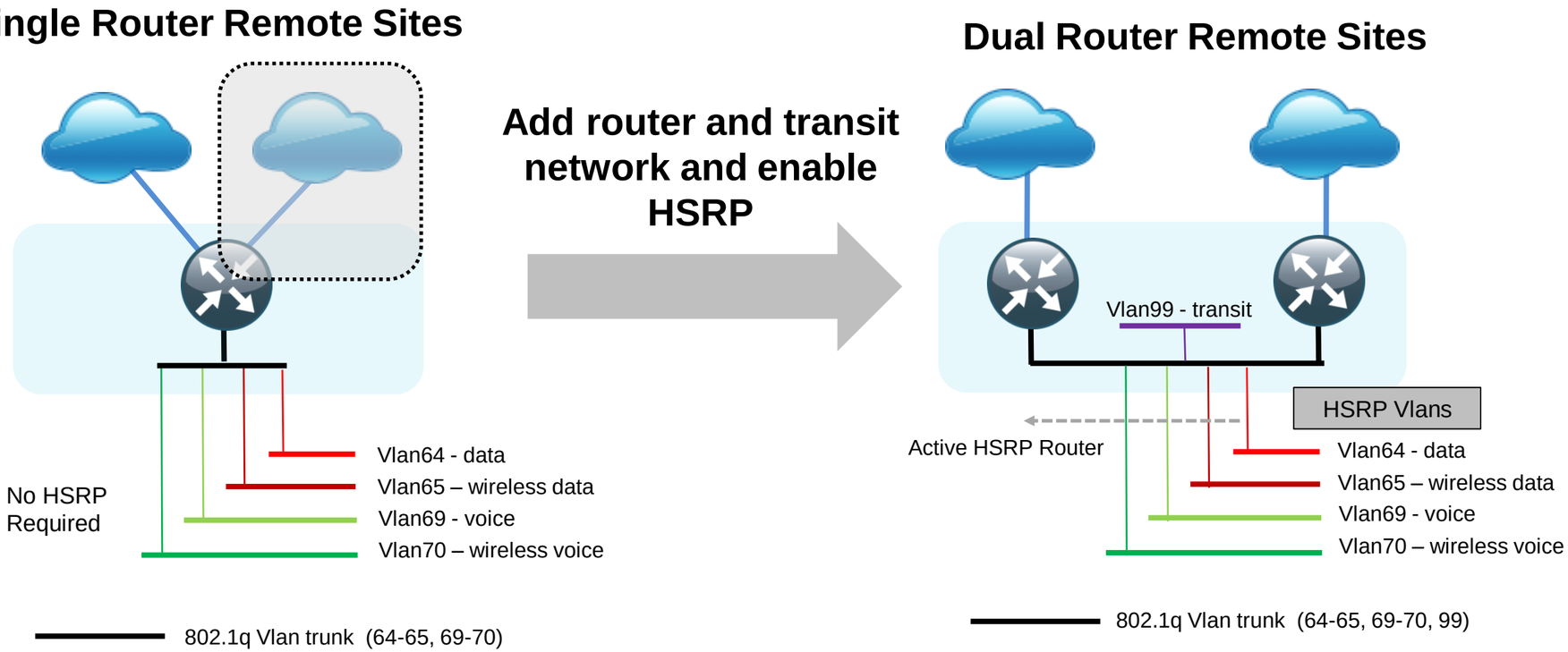


WAN Remote Site Designs (L2, 3G/4G and DMVPN)



WAN Remote Site Reference Designs

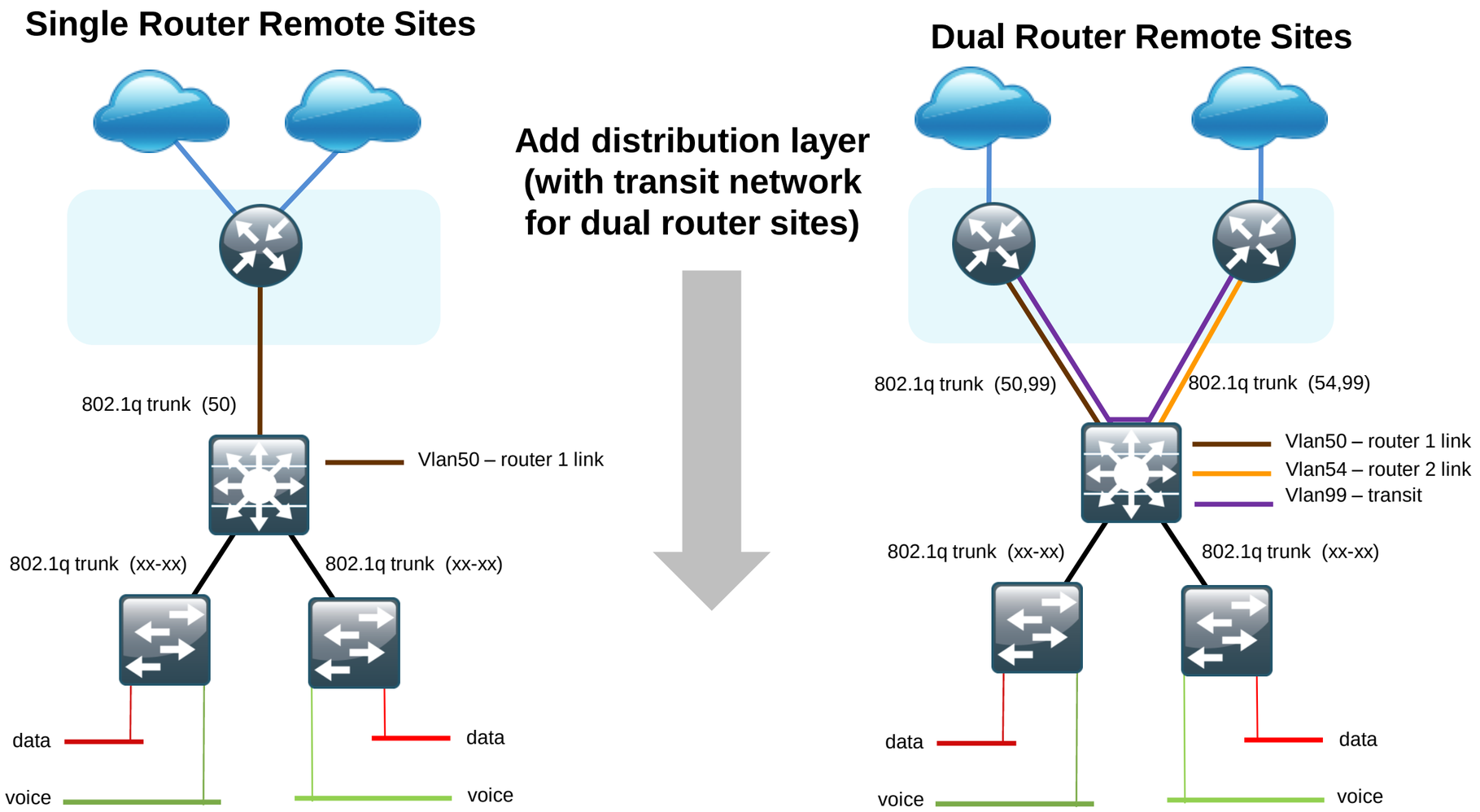
Access Layer Only



Vlan	Usage	Access Layer Only Designs	IP Network Assignment (Example)
Vlan65	Wireless Data	Yes	10.5.50.0/24
Vlan70	Wireless Voice	Yes	10.5.51.0/24
Vlan64	Data 1	Yes	10.5.52.0/24
Vlan69	Voice 1	Yes	10.5.53.0/24
Vlan99	Transit	Yes (dual router only)	10.5.48.0/30

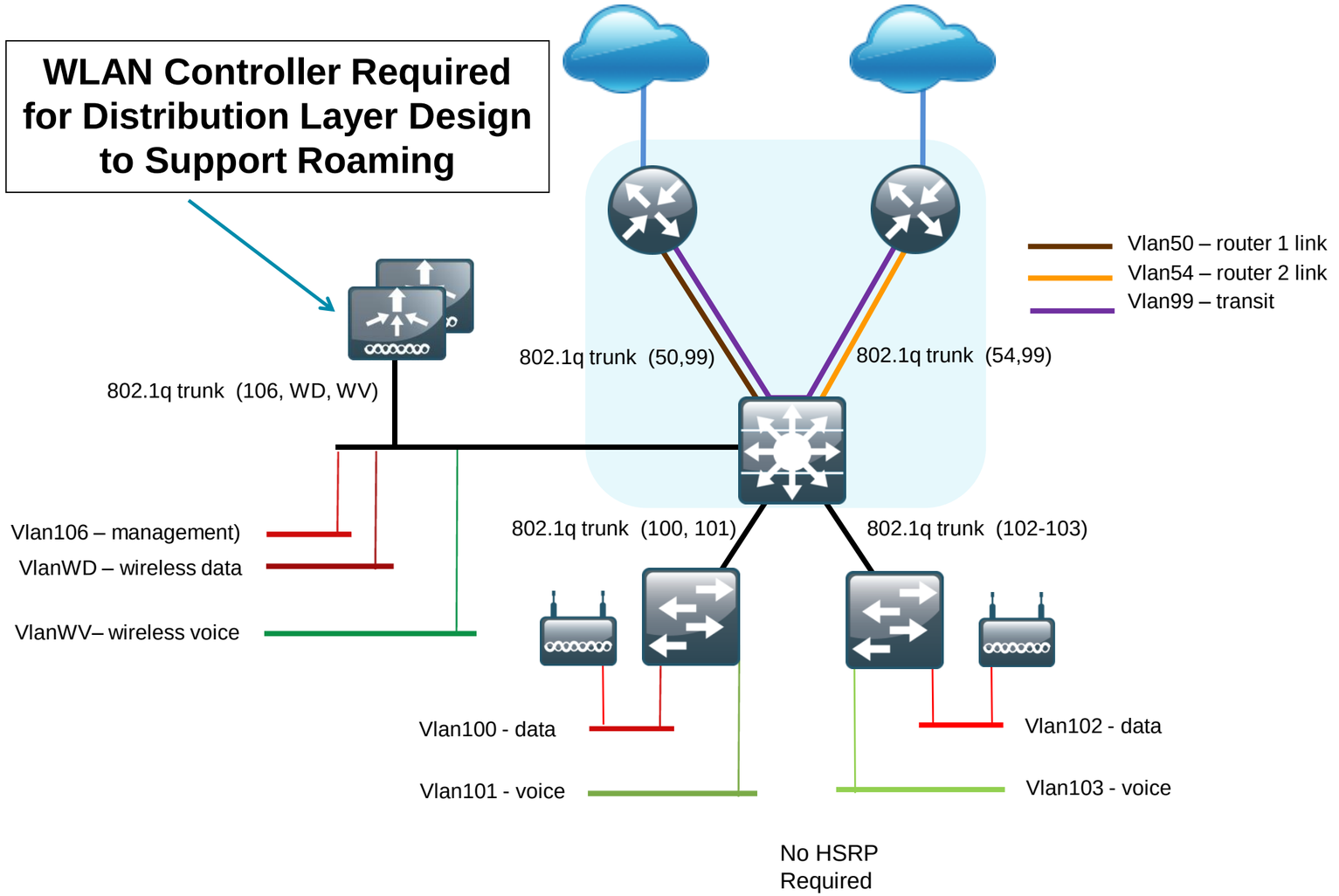
WAN Remote Site Reference Designs

Distribution and Access Layer



WAN Remote Site Reference Design

Distribution Layer Wireless LAN Integration



WAN Design and Deployment Using SBA

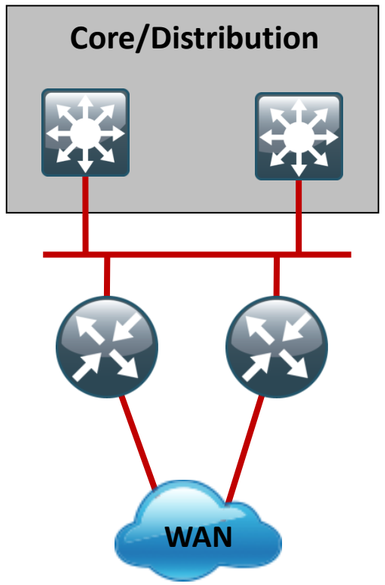
Agenda

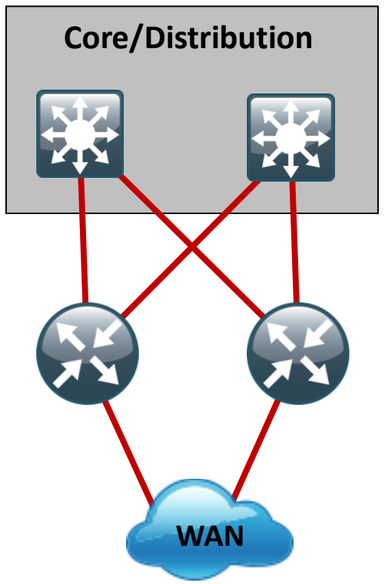
- SBA WAN Overview
- SBA WAN Design Methodology
- Key Aspects of the Design
- Summary

WAN Edge

This Topic Is Covered in Detail in BRKCRS-2030

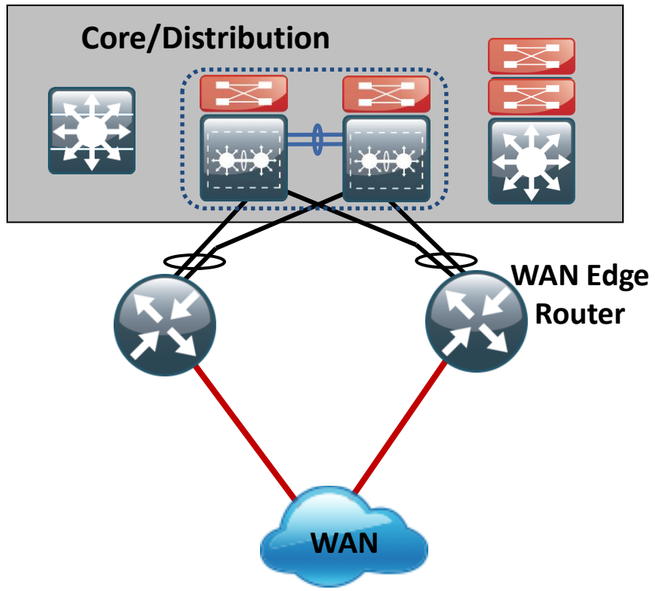
Connection Methods Compared





- All
  - No static routes
  - No FHRPs

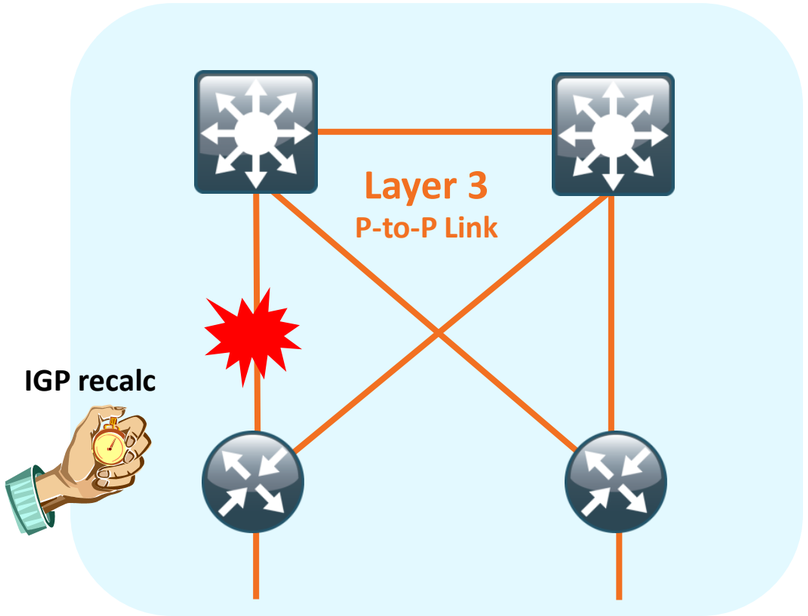
SBA Recommended



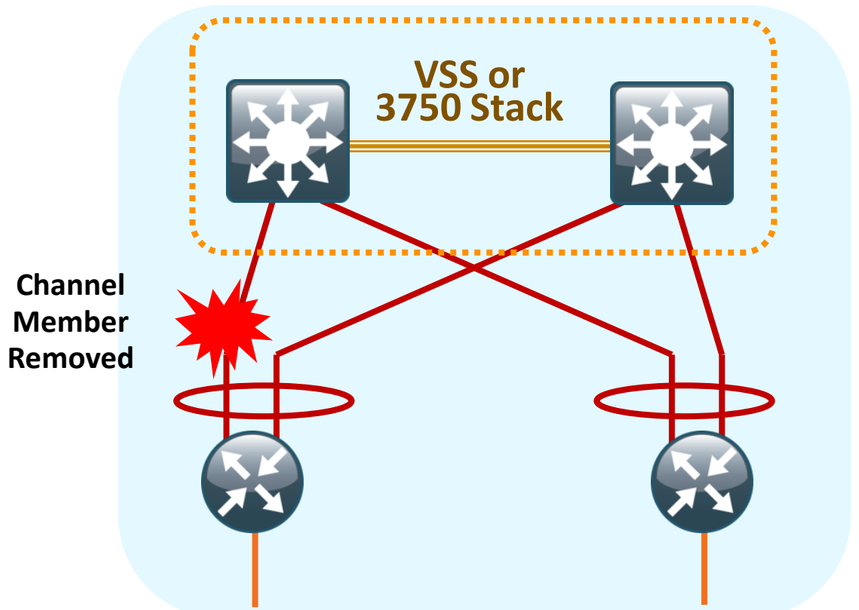
- Single Logical Control Plane
- Port-Channel for H/A

Optimize Convergence and Redundancy

Multichassis EtherChannel



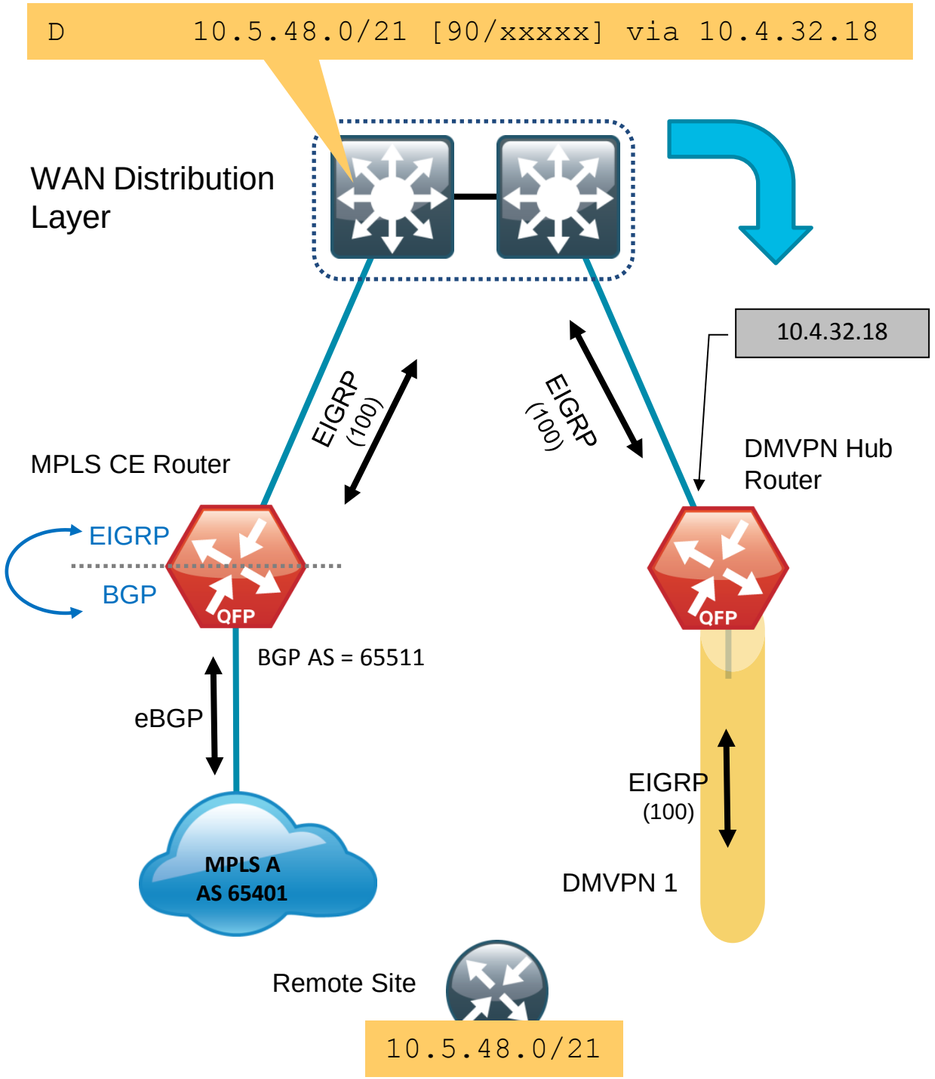
- Link redundancy achieved through redundant L3 paths
- Flow based load-balancing through CEF forwarding across
- Routing protocol reconvergence when uplink failed
- Convergence time may depends on routing protocol used and the size of routing entries



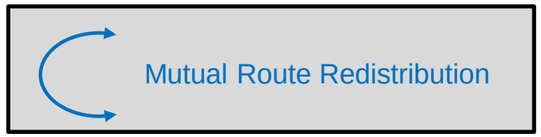
- Provide Link Redundancy and reduce peering complexity
- Tune L3/L4 load-balancing hash to achieve maximum utilization
- No L3 reconvergence required when member link failed
- No individual flow can go faster than the speed of an individual member of the link

WAN Dual-Path Route Preference

Incorrect Choice of Primary Path (DMVPN)



- eBGP routes are redistributed into EIGRP-100 as external routes with default Administrative Distance =170
- Running same EIGRP AS for both campus and DMVPN network would result in Internet path preferred over MPLS path



WAN Dual-Path Route Preference

Correct Choice of Primary Path (MPLS)

- Multiple EIGRP AS processes can be used to provide control of the routing

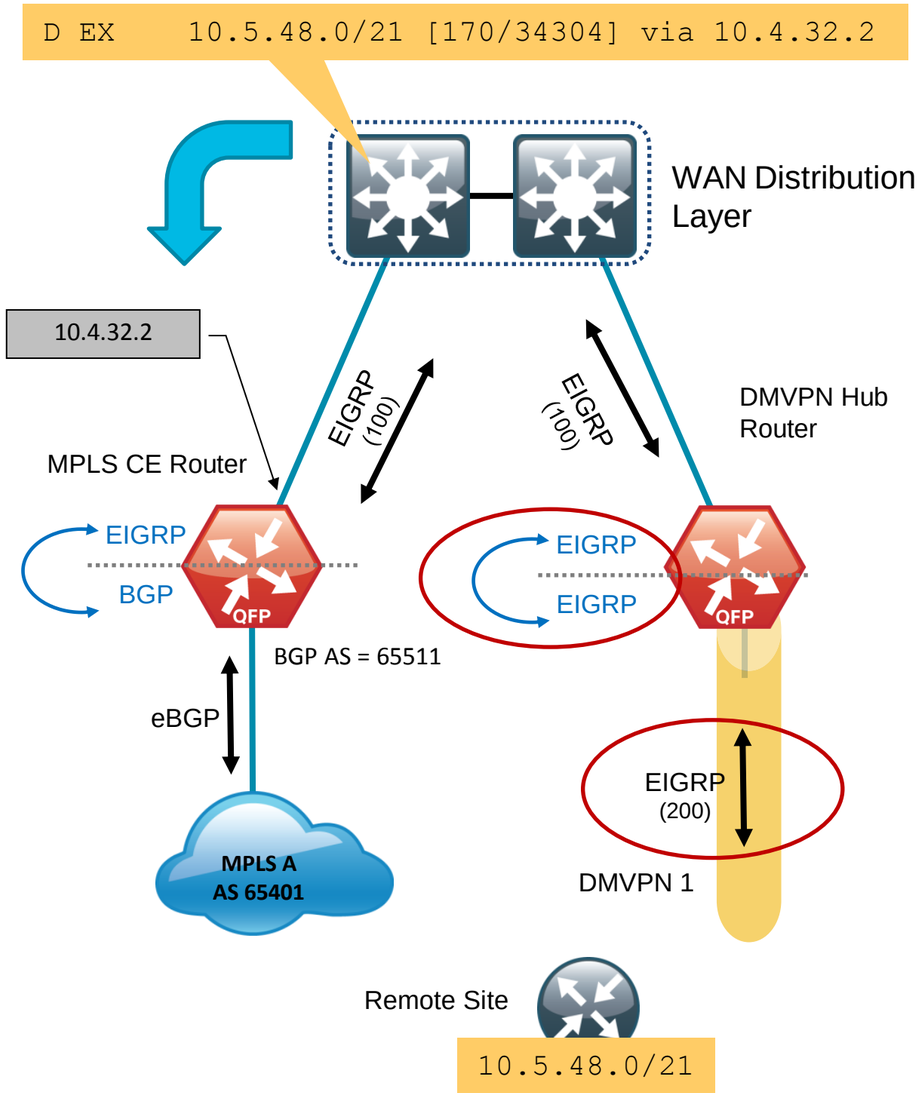
  EIGRP 100 is used in HQ location
  EIGRP 200 over DMVPN tunnel

- Routes from EIGRP 200 redistributed into EIGRP 100 appear as external route (distance = 170)

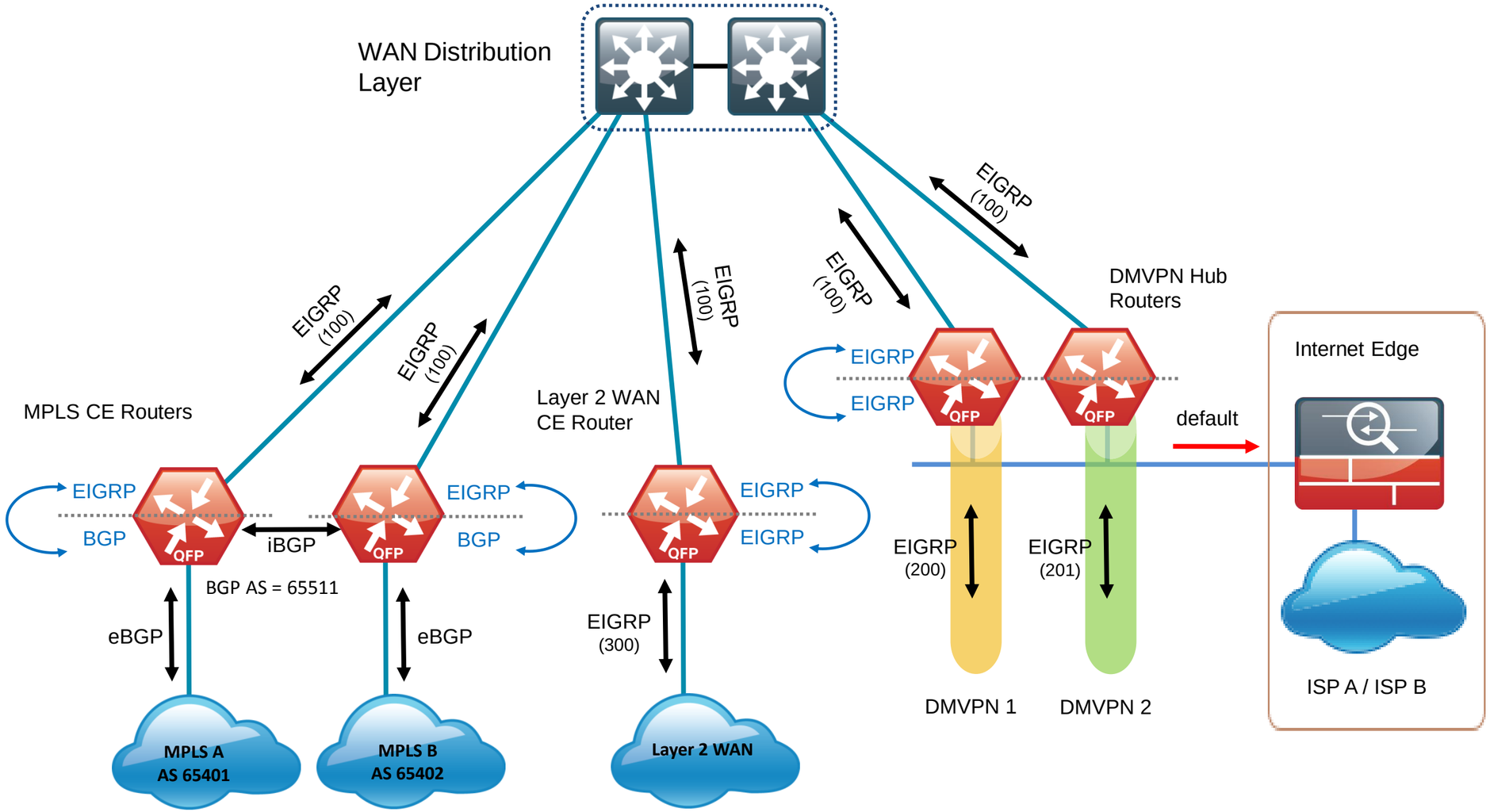
```
DMVPN hub router#
router eigrp 100
 redistribute eigrp 200
```

  - EIGRP uses bandwidth and delay metrics if prefix and distance are the same.
  - If routes from both WAN sources are equal-cost paths use EIGRP delay to modify path preference

```
MPLS CE router#
router eigrp 100
 default-metric 1000000 10 255 1 1500
```



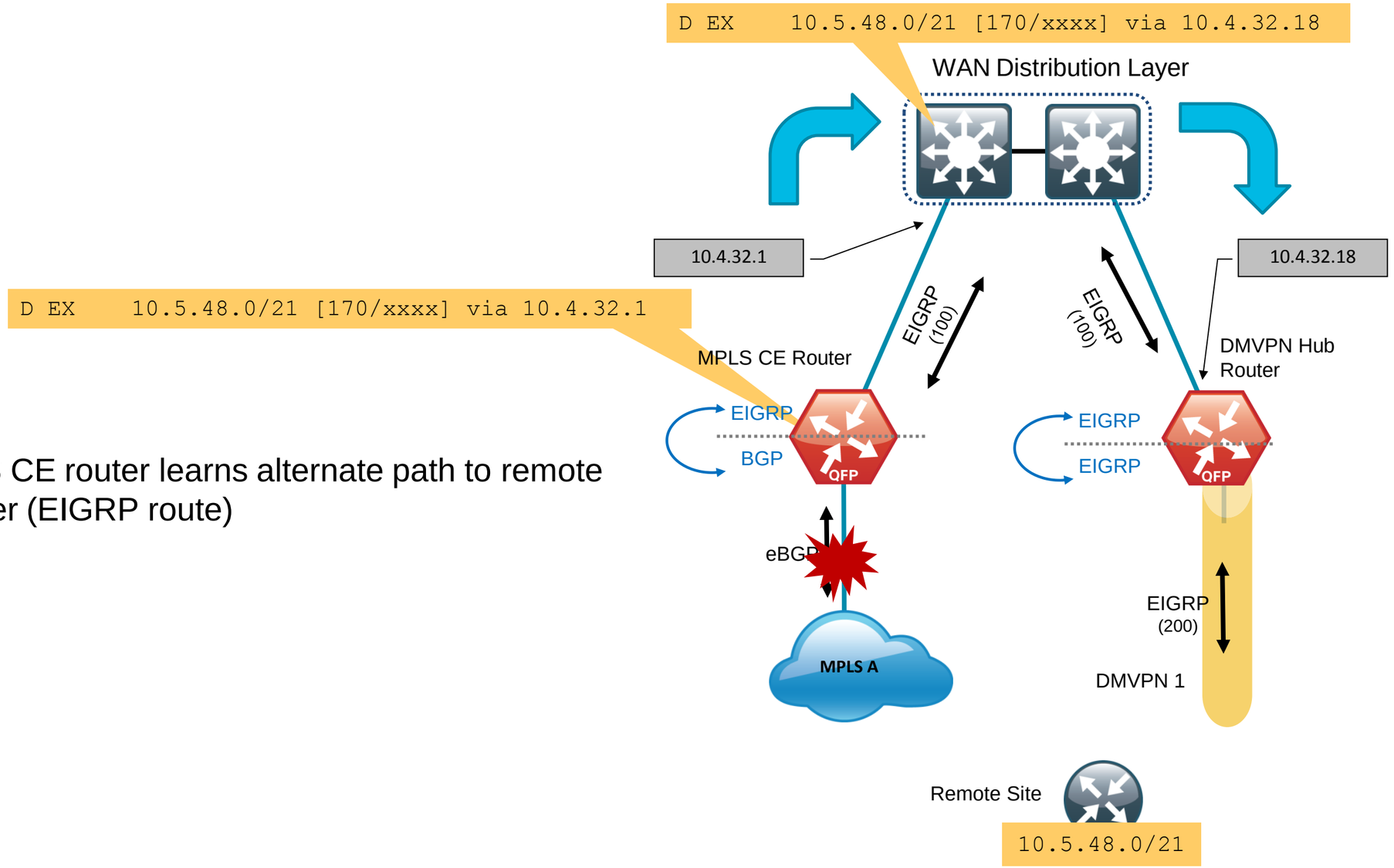
WAN-Aggregation IP Routing Detail



WAN Dual-Path Route Preference

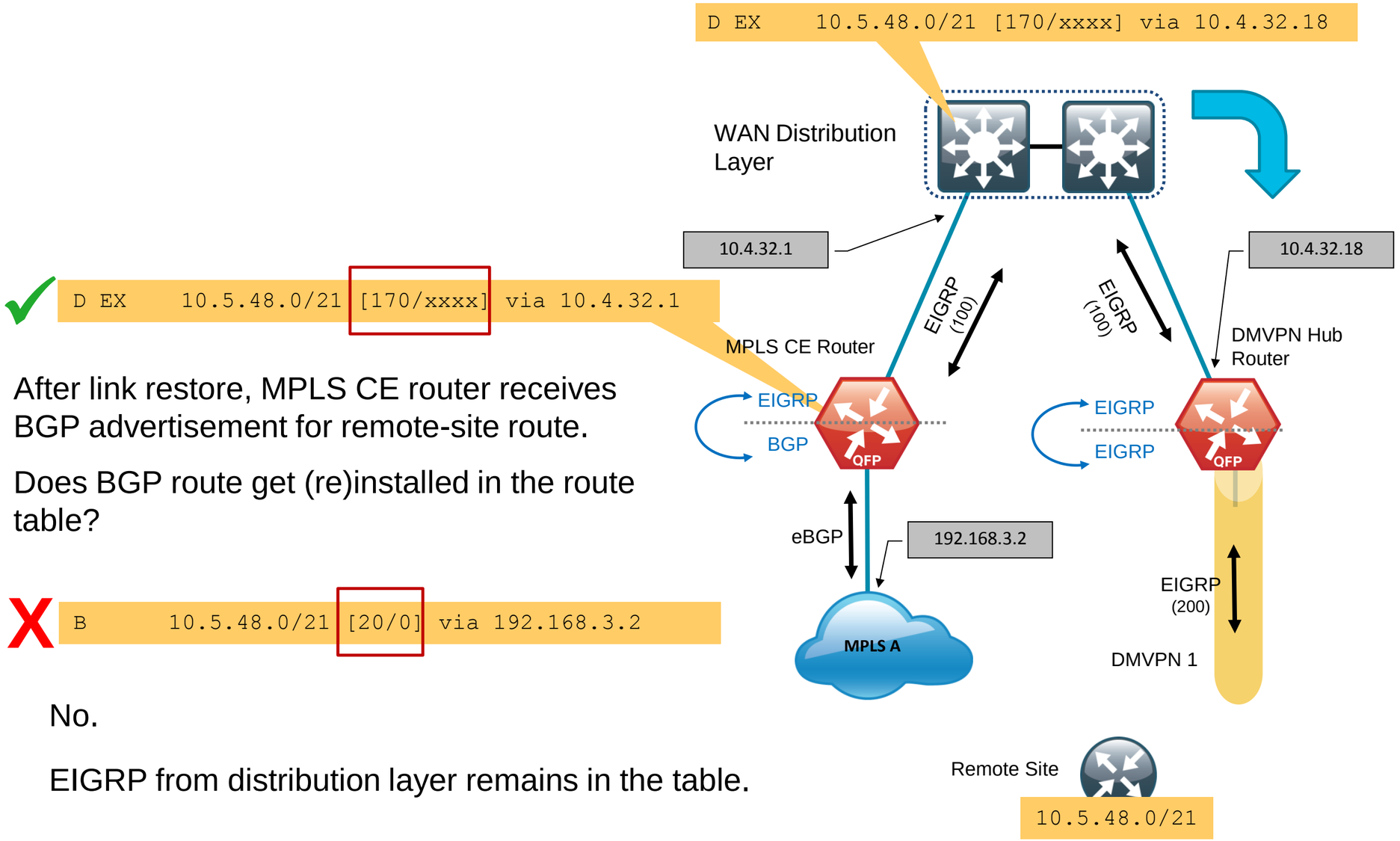
Is Route Control Needed?

- After link failure, MPLS CE router learns alternate path to remote site via distribution layer (EIGRP route)



WAN Dual-Path Route Preference

Is Route Control Needed? Yes.



- After link restore, MPLS CE router receives BGP advertisement for remote-site route.
- Does BGP route get (re)installed in the route table?

No.

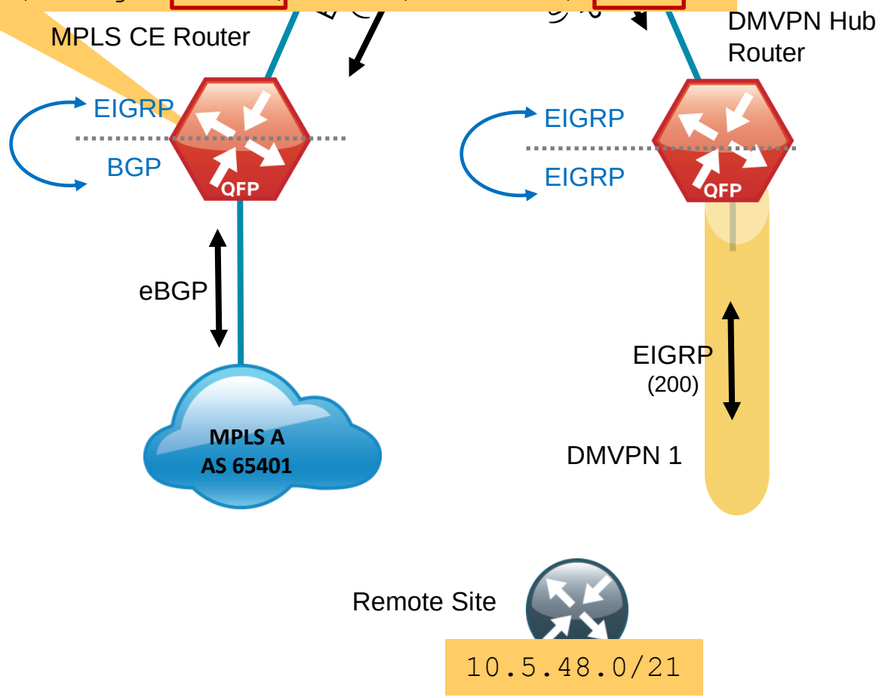
EIGRP from distribution layer remains in the table.

WAN Dual-Path Route Preference

Route Control is Needed

```
CE-1#show ip bgp 10.5.48.0 255.255.248.0
BGP routing table entry for 10.5.48.0/21, version 1293
Paths: (3 available, best #3, table default)
  Advertised to update-groups:
     4           5
  65401 65401, (aggregated by 65511 10.5.48.254)
    192.168.3.2 from 192.168.3.2 (192.168.100.3)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
  Local
    10.4.32.1 from 0.0.0.0 (10.4.32.1)
      Origin incomplete, metric 3584, localpref 100, weight 32768, valid, sourced, best
```

eBGP route
(no weight defined)

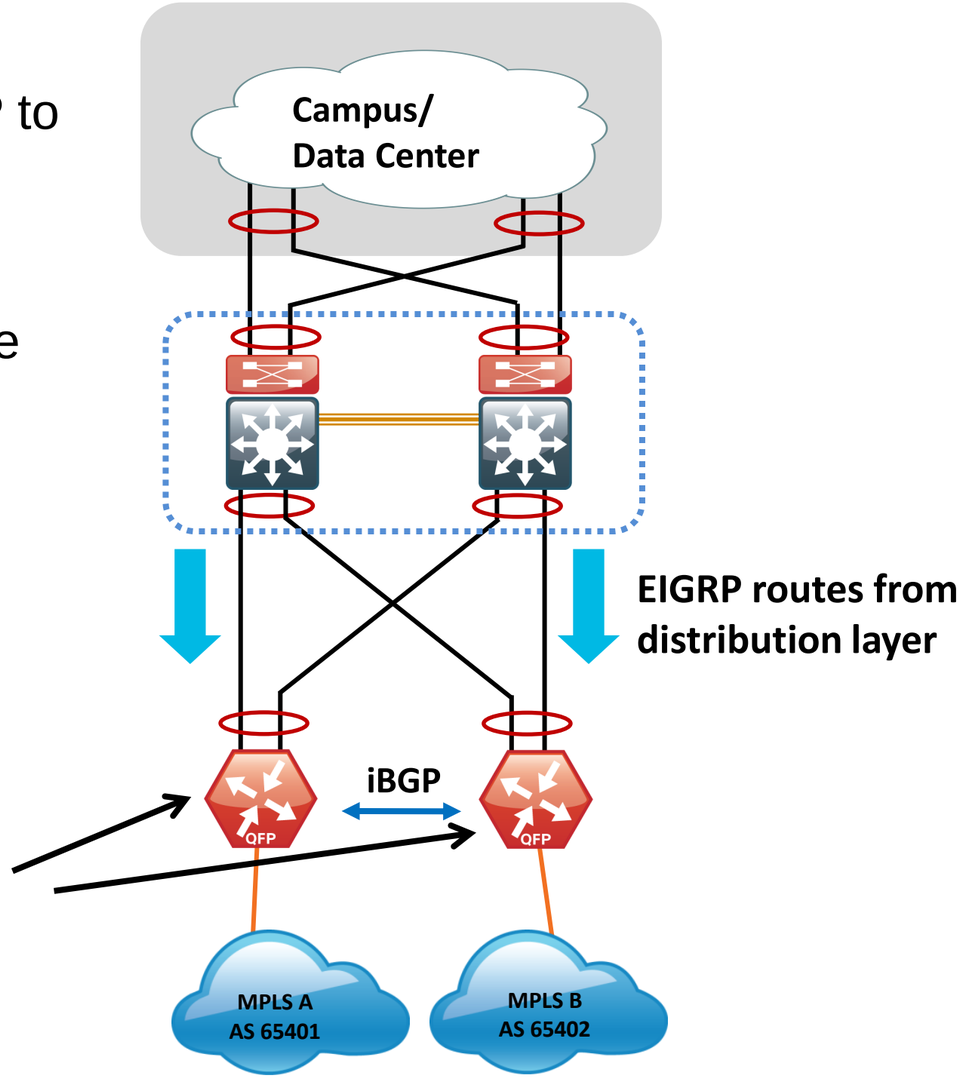


- Remote-site route is redistributed into BGP with weight = 32768
- After link is restored, distribution layer route remains in table due to BGP weight
- Routes from distribution layer should be blocked
- Also protects from other “backdoor” and routing loop conditions

Best Practice: Route Tag and Filter

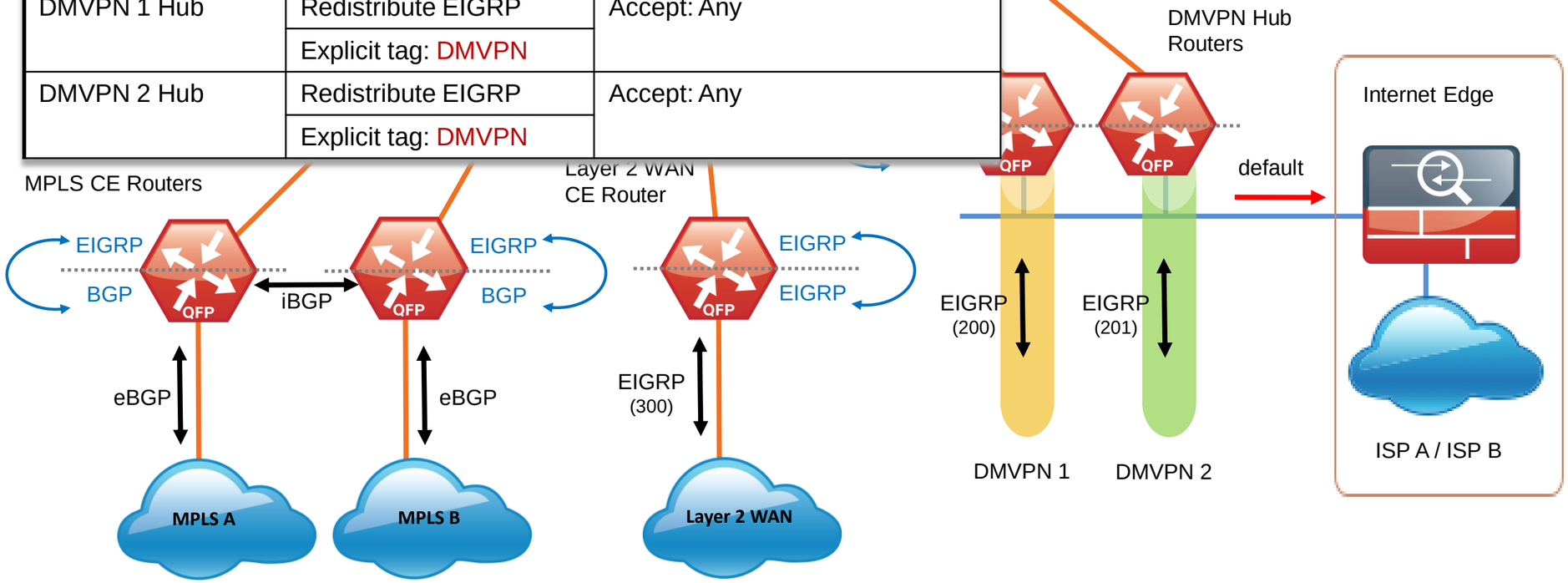
- Routes are implicitly tagged when distributed from eBGP to EIGRP with carrier AS
- Configure explicit tags for other routing protocol sources
- Use route-map to block re-learning of WAN routes via the distribution layer (MPLS routes already known via iBGP)

```
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 default-metric [BW] 100 255 1 1500
 redistribute bgp 65511

route-map BLOCK-TAGGED-ROUTES deny 10
 match tag 65401 65402

route-map BLOCK-TAGGED-ROUTES permit 20
```



WAN-Aggregation Mutual Route Redistribution

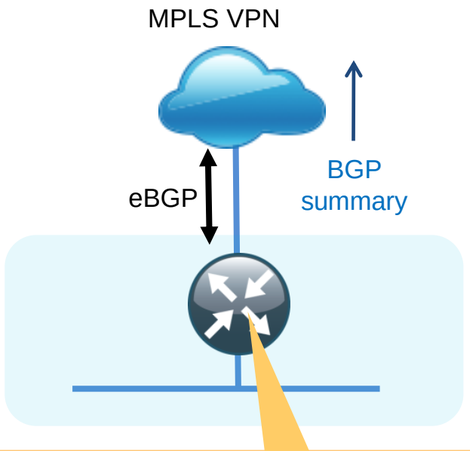
WAN-Aggregation Router	From WAN towards Core/Distribution	From Core/Distribution towards WAN (Redistribute EIGRP 100)
MPLS A CE	Redistribute BGP	Block: MPLS-A, MPLS-B, DMVPN
	Implicit tag: MPLS-A	
MPLS B CE	Redistribute: BGP	Block: MPLS-A, MPLS-B, DMVPN
	Implicit tag: MPLS-B	
Layer 2 WAN CE	Redistribute: EIGRP	Block: DMVPN
	Explicit tag: Layer 2 WAN	
DMVPN 1 Hub	Redistribute EIGRP	Accept: Any
	Explicit tag: DMVPN	
DMVPN 2 Hub	Redistribute EIGRP	Accept: Any
	Explicit tag: DMVPN	



WAN Remote-Site Routing

Single-Router, Single-Link, Access Layer only

Only requires a single WAN facing routing protocol process



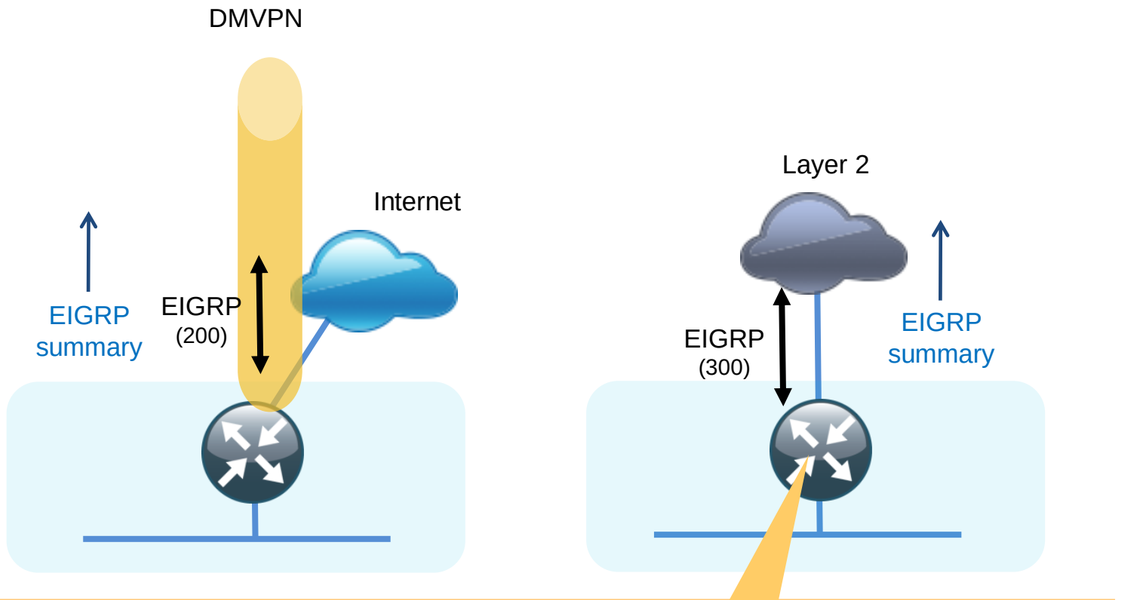

```
router bgp 65511
 bgp router-id 10.5.56.254
 network 10.5.60.0 mask 255.255.255.0
 network 10.5.61.0 mask 255.255.255.0
 network 192.168.3.28 mask 255.255.255.252
 aggregate-address 10.5.56.0 255.255.248.0 summary-only
 neighbor 192.168.3.30 remote-as 65401
 no auto-summary
```

Wired/Wireless Data Subnets

WAN Remote-Site Routing

Single-Router, Single-Link, Access Layer Only

Only requires a single WAN facing routing protocol process




```
router eigrp 300
 network 10.4.38.0 0.0.0.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface GigabitEthernet0/0.38
 eigrp router-id 10.5.144.254
 eigrp stub connected summary
interface GigabitEthernet0/0.38
 ip summary-address eigrp 300 10.5.144.0 255.255.248.0
```

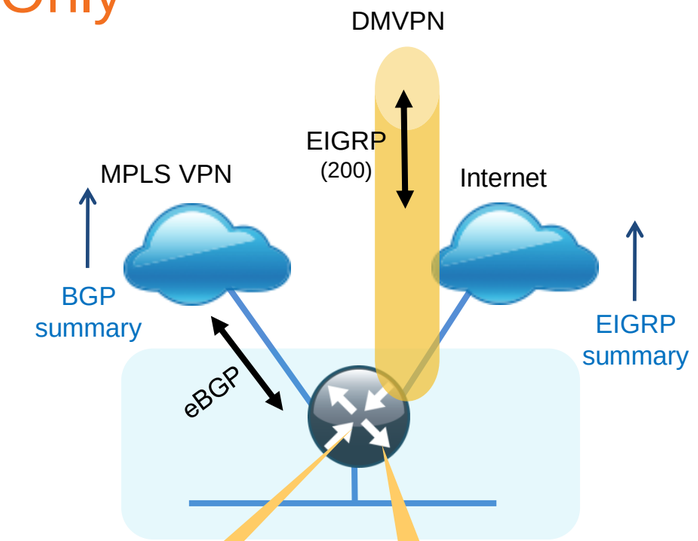
Includes all Remote-site networks

Layer 2 WAN interface

WAN Remote-Site Routing

Single-Router, Dual-Link, Access Layer Only

Requires two separate WAN facing routing protocol processes

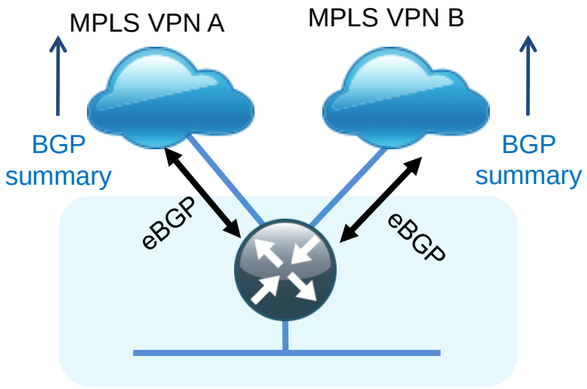



```
router bgp 65511
 bgp router-id 10.5.40.254
 network 10.5.44.0 mask 255.255.255.0
 network 10.5.45.0 mask 255.255.255.0
 network 192.168.3.20 mask 255.255.255.252
 aggregate-address 10.5.40.0 255.255.248.0 summary-only
 neighbor 192.168.3.22 remote-as 65401
 no auto-summary
```

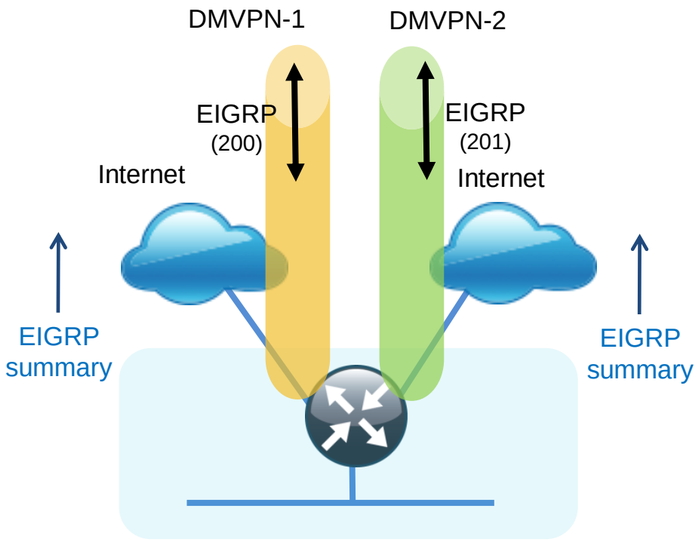
```
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.5.40.254
 eigrp stub connected summary
interface Tunnel10
 ip summary-address eigrp 200 10.5.40.0 255.255.248.0
```

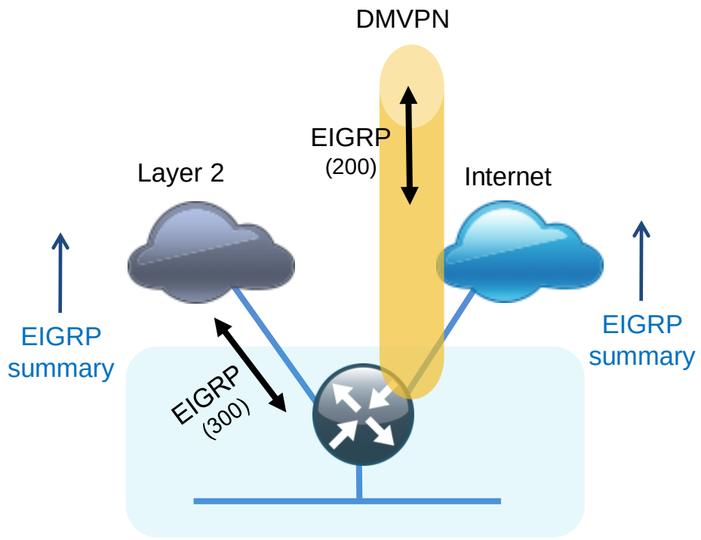
WAN Remote-Site Routing

Single-Router, Dual-Link, Access Layer Only



Requires <u>two</u> separate WAN facing routing protocol processes (except for dual-MPLS)

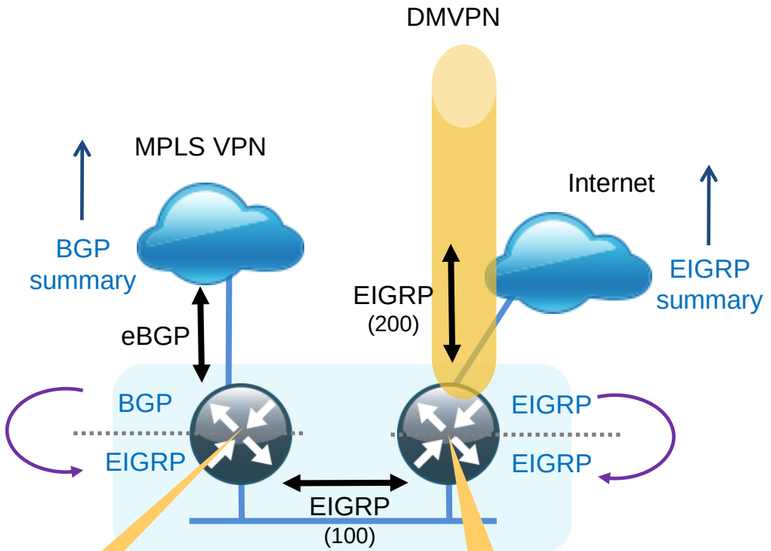




WAN Remote-Site Routing

Dual-Router, Dual-Link, Access Layer Only

Requires Separate WAN and LAN Facing Routing Protocol Processes



One Way Route Redistribution

One Way Redistribution Is Required.

Summary Routes Make Two-Way Redistribution Unnecessary

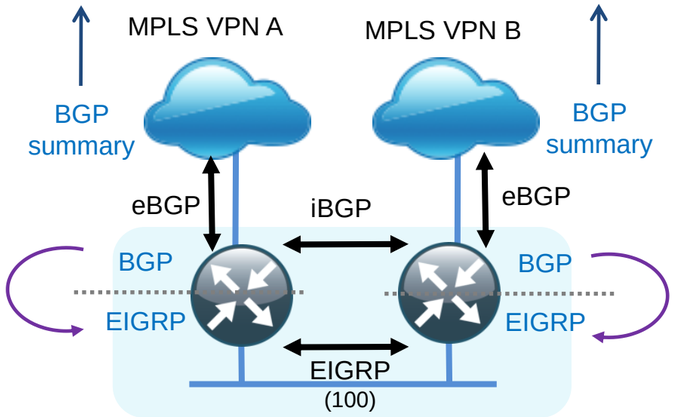
```
router eigrp 100
 default-metric 100000 100 255 1 1500
 network 10.5.0.0 0.0.255.255
 redistribute bgp 65511
 passive-interface default
 no passive-interface GigabitEthernet0/1.99
 eigrp router-id 10.5.48.254
```

```
router eigrp 100
 network 10.5.0.0 0.0.255.255
 redistribute eigrp 200
 passive-interface default
 no passive-interface GigabitEthernet0/1.99
 eigrp router-id 10.5.48.253
```

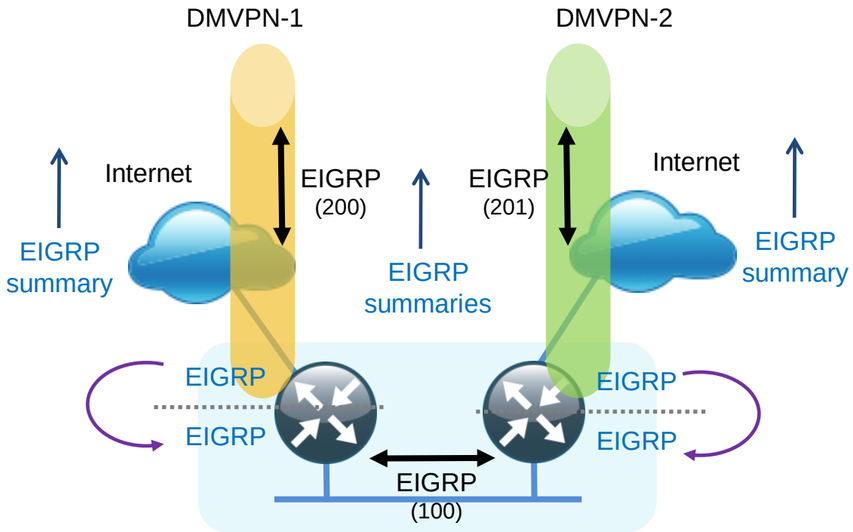
Transit network

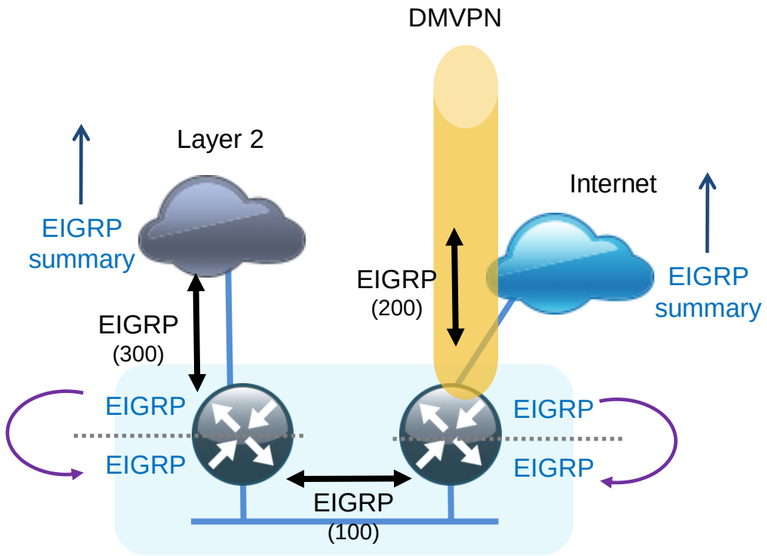
WAN Remote-Site Routing

Dual-Router, Dual-Link, Access Layer Only



Requires Separate WAN and LAN Facing Routing Protocol Processes



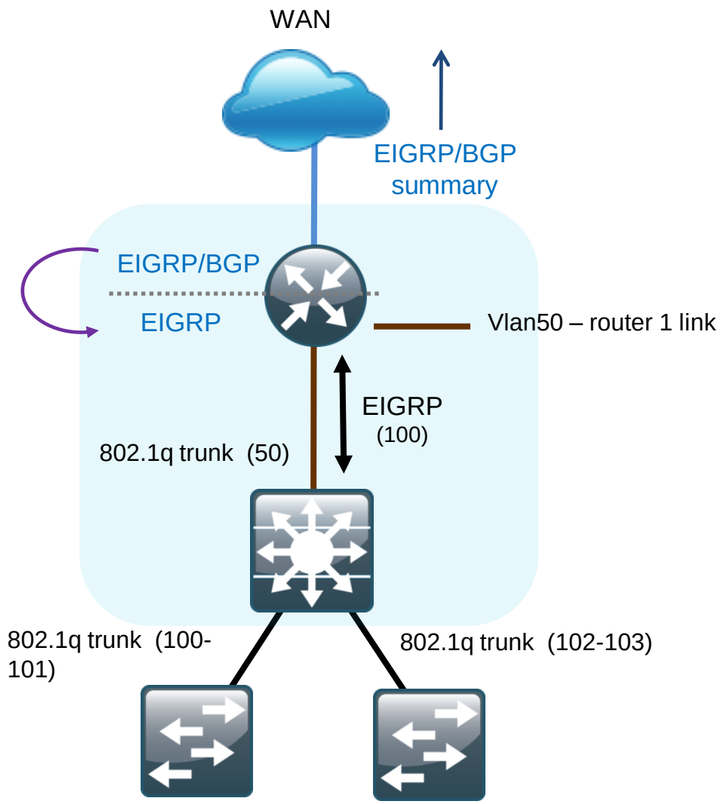


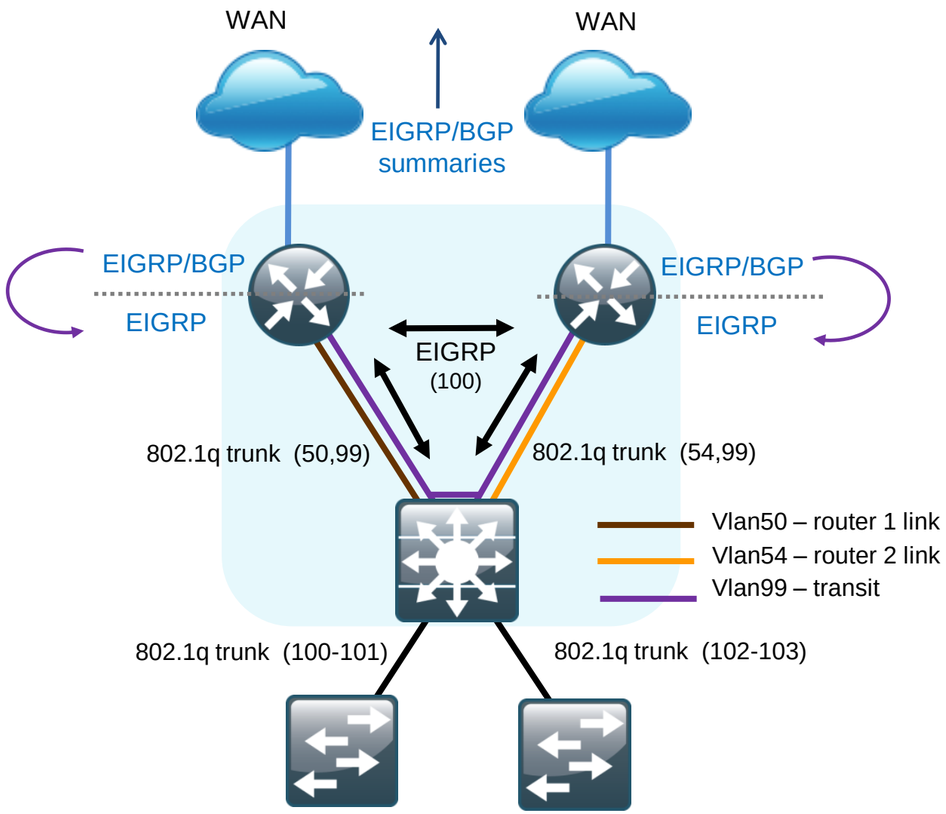
WAN Remote-Site Routing

Distribution/Access Layer Only

Requires Separate WAN and LAN Facing Routing Protocol Processes

WAN EIGRP Is Either: DMVPN (200/201)
Layer 2 WAN (300)

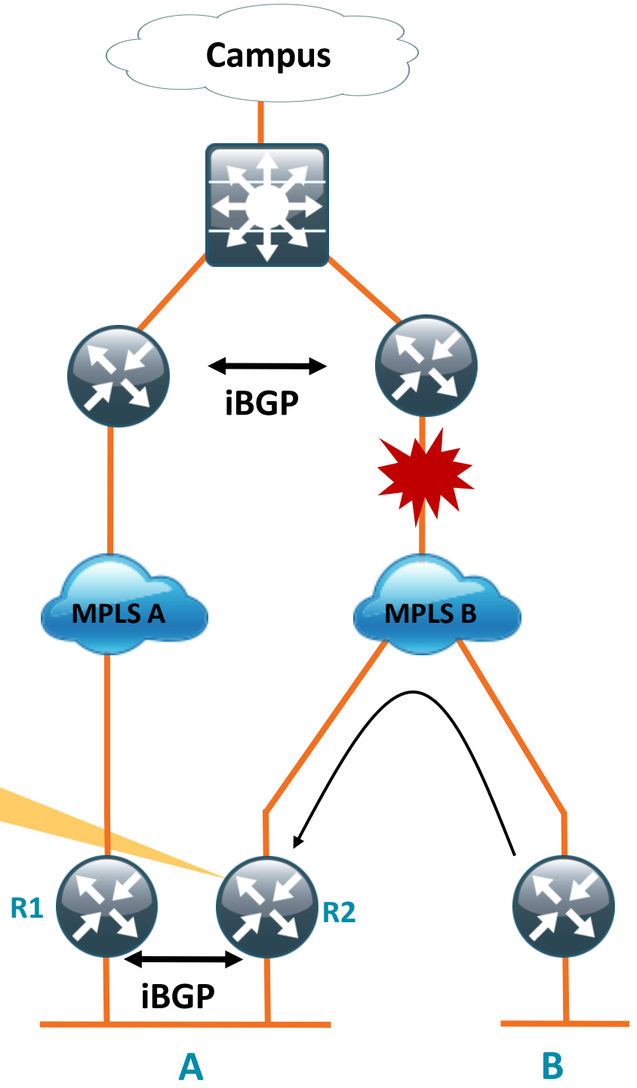




Best Practice: Implement AS-Path Filter

Prevent Remote Site from Becoming Transit Network

- Dual carrier sites can unintentionally become transit network during network failure event and causing network congestion due to transit traffic
- Design the network so that transit path between two carriers only occurs at sites with enough bandwidth
- Implement AS-Path filter to allow only locally originated routes to be advertised on the outbound updates for branches that should not be transit



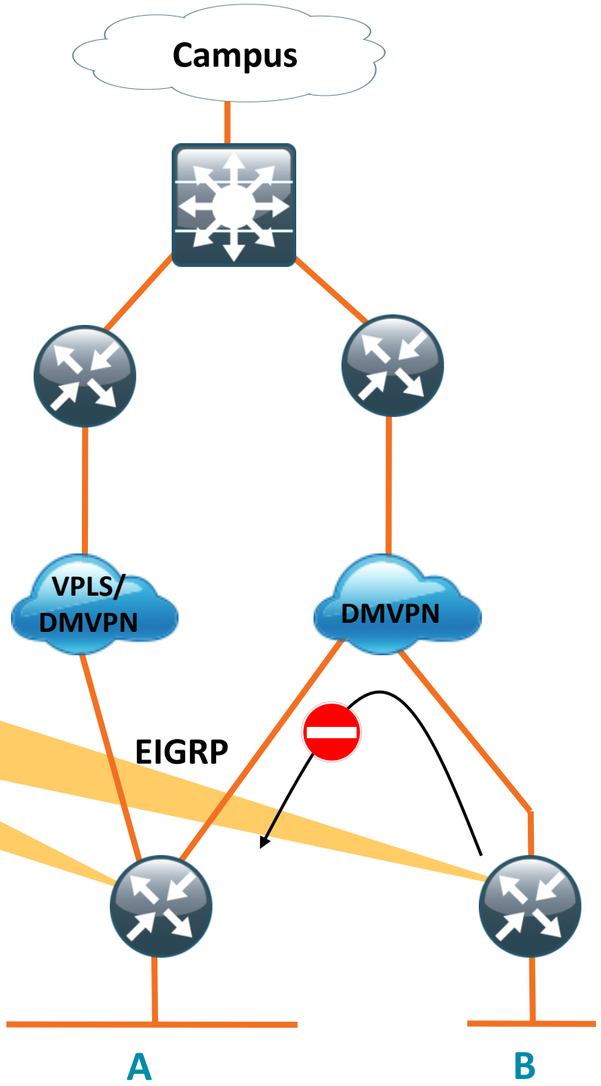

```
router bgp 65511
 neighbor 192.168.4.10 route-map NO-TRANSIT-AS out
!
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```

Best Practice: Stub Routing

Improve Network Stability and Prevent Transit Site

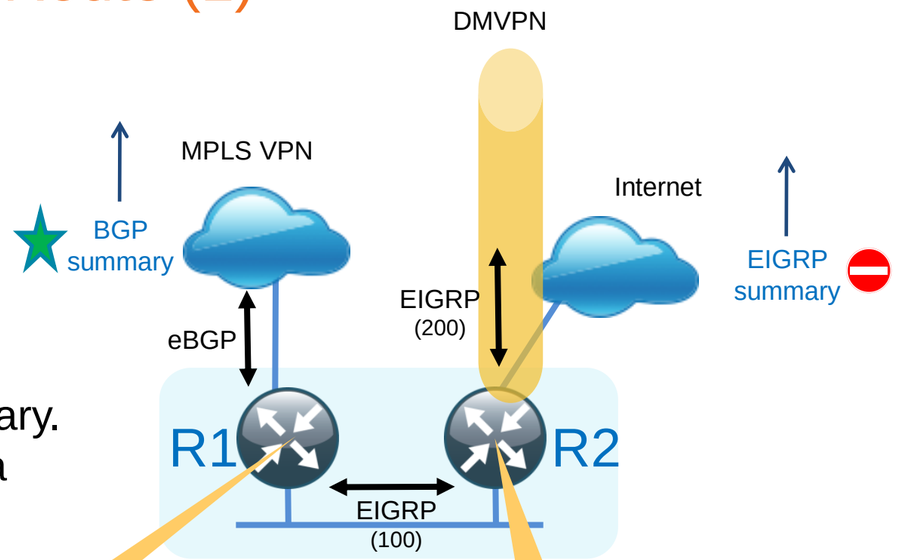
- The stub routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration. Use at all remote sites.
- Implement stub routing to allow only locally originated routes to be advertised on the outbound updates for dual-router sites that should not be transit

```
router eigrp 200
 eigrp stub connected summary
```



WAN Remote-Site Loopback Routing

Initial Approach – Loopbacks within Summary Route (1)



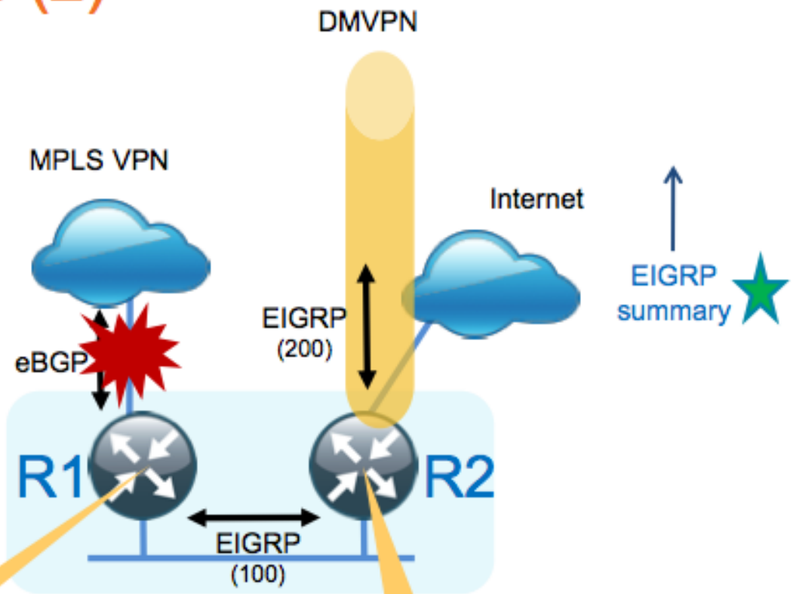
Summaries are advertised via both links, but best path is via primary. When primary link is operational both loopbacks are reachable via primary link.

```
interface Loopback0
 ip address 10.5.48.254 255.255.255.255
router bgp 65511
 bgp router-id 10.5.48.254
 network 10.5.52.0 mask 255.255.255.0
 network 10.5.53.0 mask 255.255.255.0
 network 192.168.3.20 mask 255.255.255.252
 aggregate-address 10.5.48.0 255.255.248.0 summary-only
 neighbor 192.168.3.22 remote-as 65401
 no auto-summary
```

```
interface Loopback0
 ip address 10.5.48.253 255.255.255.255
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.5.48.253
 eigrp stub connected summary
interface Tunnel10
 ip summary-address eigrp 200 10.5.48.0 255.255.248.0
```

WAN Remote-Site Loopback Routing

Initial Approach – Loopbacks within Summary Route (2)



After primary link failure, only summary learned via secondary path is reachable. Both loopbacks are reachable via secondary path.

```
interface Loopback0
 ip address 10.5.48.254 255.255.255.255
router bgp 65511
 bgp router-id 10.5.48.254
 network 10.5.52.0 mask 255.255.255.0
 network 10.5.53.0 mask 255.255.255.0
 network 192.168.3.20 mask 255.255.255.252
 aggregate-address 10.5.48.0 255.255.248.0 summary-only
 neighbor 192.168.3.22 remote-as 65401
 no auto-summary
```

```
interface Loopback0
 ip address 10.5.48.253 255.255.255.255
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.5.48.253
 eigrp stub connected summary
interface Tunnel10
 ip summary-address eigrp 200 10.5.48.0 255.255.248.0
```

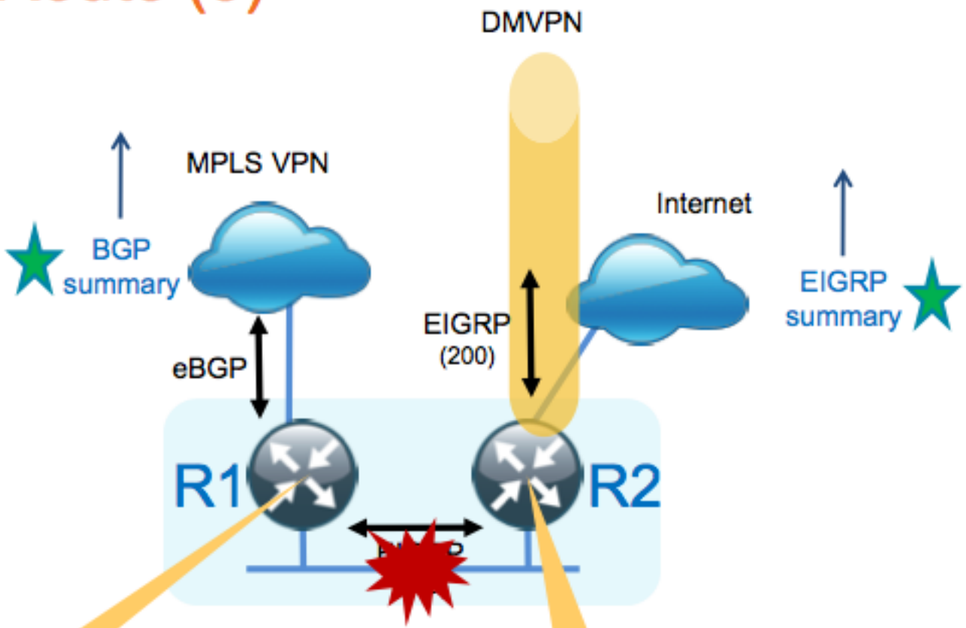
WAN Remote-Site Loopback Routing

Initial Approach – Loopbacks within Summary Route (3)

If the LAN interconnect between routers goes down and the primary link remains operational, then summary remains advertised via the primary link.

R2 has a route to the WAN-aggregation site, but traffic is returned to R1 (follows best summary route).

R2 loopback is unreachable. Traffic from HQ site is blackholed down primary link.




```
interface Loopback0
 ip address 10.5.48.254 255.255.255.255
router bgp 65511
 bgp router-id 10.5.48.254
 network 10.5.52.0 mask 255.255.255.0
 network 10.5.53.0 mask 255.255.255.0
 network 192.168.3.20 mask 255.255.255.252
 aggregate-address 10.5.48.0 255.255.248.0 summary-only
 neighbor 192.168.3.22 remote-as 65401
 no auto-summary
```

```
interface Loopback0
 ip address 10.5.48.253 255.255.255.255
router eigrp 200
 network 10.4.34.0 0.0.1.255
 network 10.5.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel10
 eigrp router-id 10.5.48.253
 eigrp stub connected summary
interface Tunnel10
 ip summary-address eigrp 200 10.5.48.0 255.255.248.0
```

WAN Remote-Site Loopback Routing

Ensure Reachability of Remote-Site Routers for All Failure Scenarios

Must be tolerant of various remote-site failures:

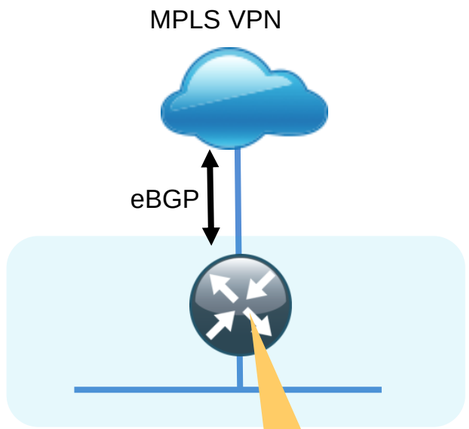
- LAN switch failure
- Primary or Backup WAN failure
- Must work with both single and dual router topologies

Use unique network range for loopbacks that is not summarized.
Creates a host route (/32) for each WAN remote-site router.

WAN Transport (All Sites use 10.255.0.0/16)	Third Octet	Fourth Octet	Examples	
			Router	Loopback0
MPLS A	251	Site #	RS203-2921-1	10.255.251.203
MPLS B	252	Site #	RS202-2911	10.255.252.202
DMVPN 1	253	Site #	RS203-2921-2	10.255.253.203
DMVPN 2	254	Site #	RS232.-2921-2	10.255.254.232
MetroE	255	Site #	RS213-2911	10.255.255.213

WAN Remote-Site Loopback Routing

BGP Configuration for Single-Router




```
interface Loopback0
 ip address 10.255.251.204 255.255.255.255
```

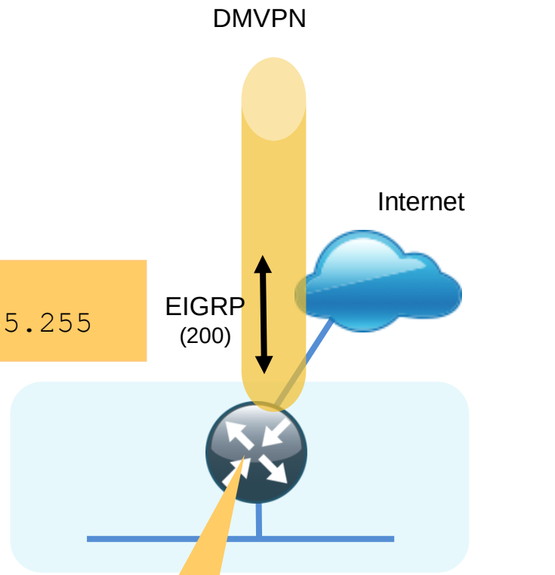
```
router bgp 65511
 bgp router-id 10.255.251.204
 network 10.255.251.204 mask 255.255.255.255
 neighbor 192.168.3.30 remote-as 65401
```

Loopback

WAN Remote-Site Loopback Routing

EIGRP Configuration for Single-Router

```
interface Loopback0
 ip address 10.255.253.205 255.255.255.255
```



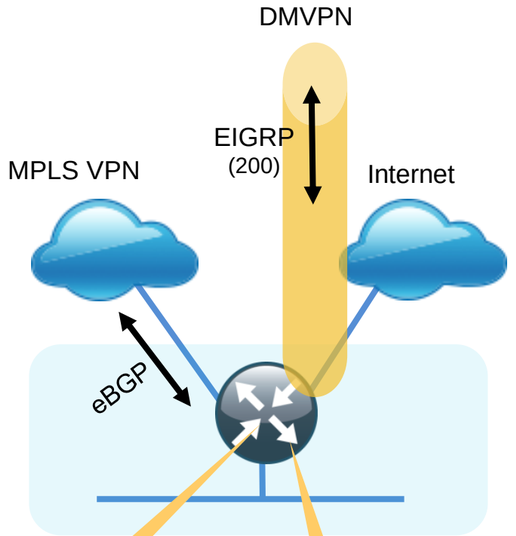

```
router eigrp 200
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.253.205
```

All Loopbacks

WAN Remote-Site Loopback Routing

Configuration for Single-Router (MPLS with DMVPN Backup)

Choose loopback from address block of primary link for single-router, dual-link remote site




```
interface Loopback0
 ip address 10.255.251.201 255.255.255.255
```

```
router bgp 65511
 bgp router-id 10.255.251.201
 network 10.255.251.201 mask 255.255.255.255
 neighbor 192.168.3.22 remote-as 65401
```

← Loopback

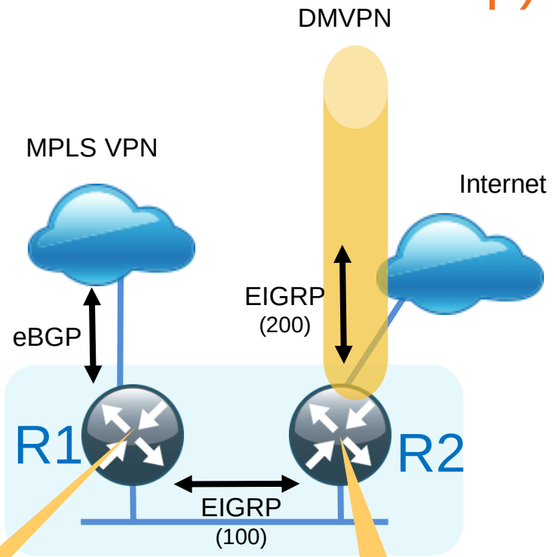
```
router eigrp 200
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.251.201
```

← All Loopbacks

WAN Remote-Site Loopback Routing

Configuration for Dual-Router (MPLS with DMVPN Backup)

Uses the LAN facing routing protocol process to advertise R2 loopback to R1 (and R1 loopback to R2)

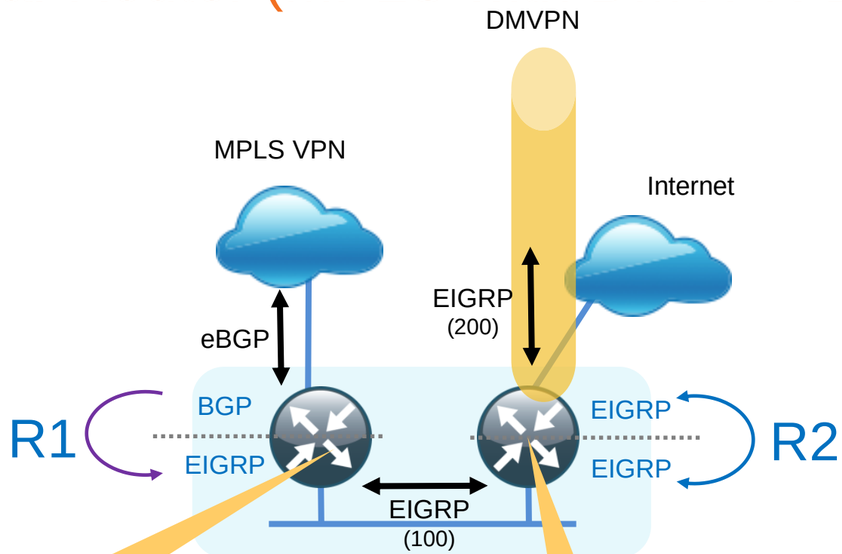



```
interface Loopback0
 ip address 10.255.251.203 255.255.255.255
router eigrp 100
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.255.251.203
```

```
interface Loopback0
 ip address 10.255.253.203 255.255.255.255
router eigrp 100
 network 10.255.0.0 0.0.255.255
 eigrp router-id 10.5.253.203
```

WAN Remote-Site Loopback Routing

(continued) Configuration for Dual-Router (MPLS with DMVPN Backup)



Both loopbacks need to be explicitly listed in the BGP configuration.

```
router bgp 65511
 bgp router-id 10.255.251.203
 network 10.255.251.203 mask 255.255.255.255
 network 10.255.253.203 mask 255.255.255.255
```

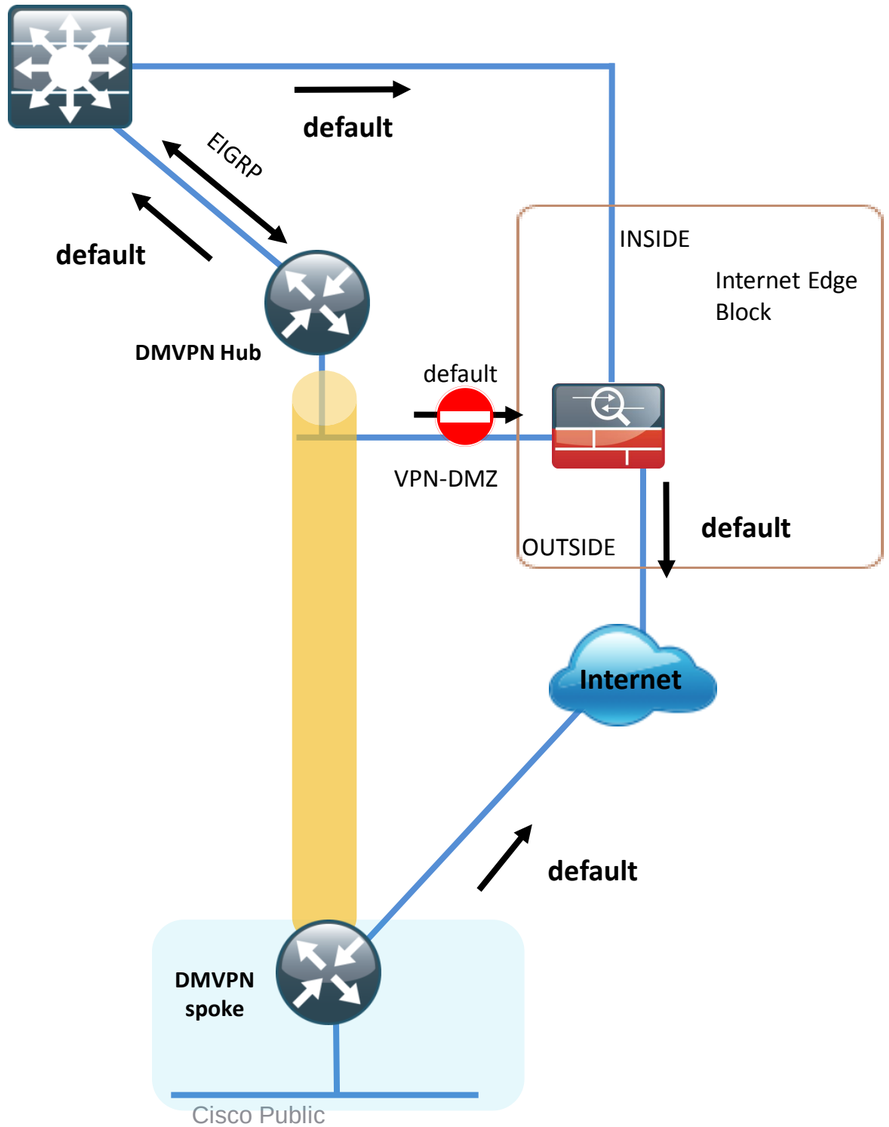
Two way redistribution is required for EIGRP WAN routing protocol (on R2) Only the loopback addresses should be redistributed from LAN to WAN

```
router eigrp 100
 network 10.255.0.0 0.0.255.255
 redistribute eigrp 100 route-map LOOPBACK-ONLY
 eigrp router-id 10.255.253.203
 eigrp stub connected summary redistributed

ip access-list standard R1-LOOPBACK
 permit 10.255.251.203

route-map LOOPBACK-ONLY permit 10
 match ip address R1-LOOPBACK
```

DMVPN Deployment Considerations

How to Accommodate Multiple Default Routers for a VPN Hub Router

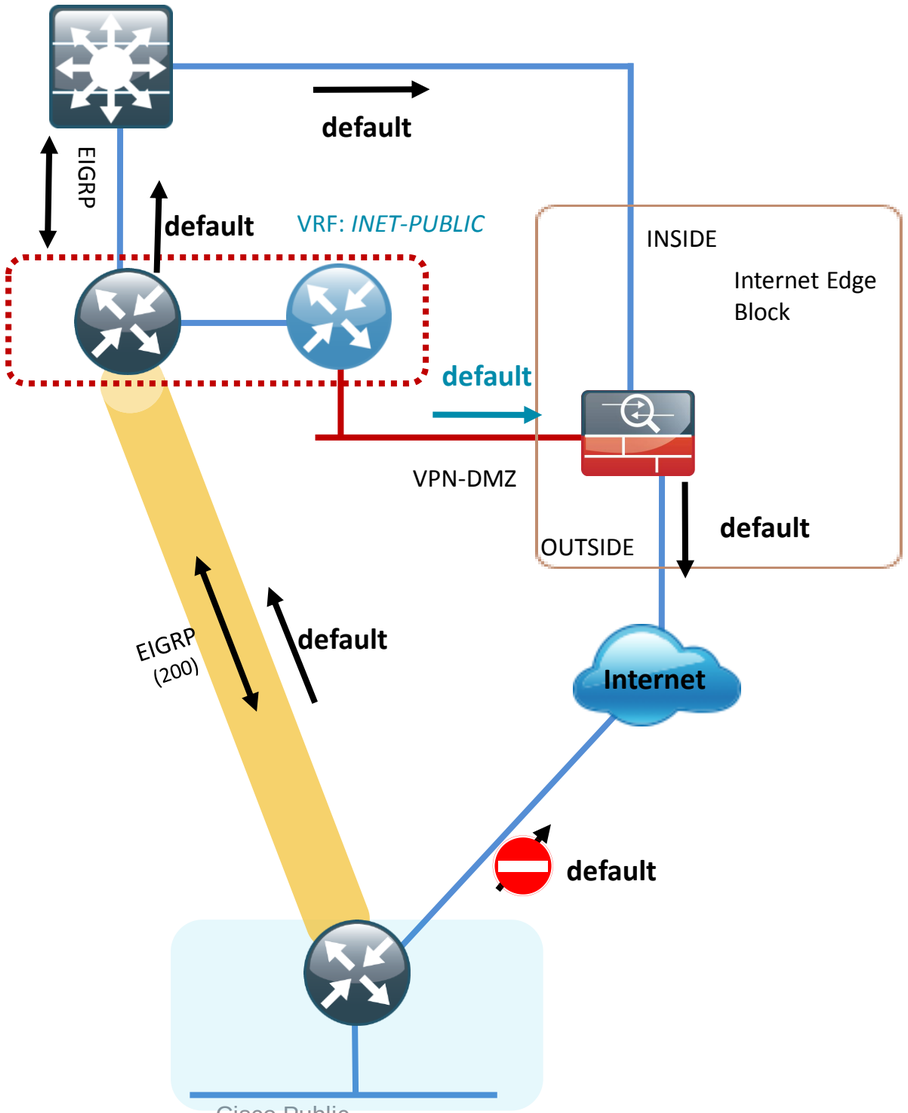
- VPN hub has a default route to ASA firewall's VPN-DMZ interface to reach the Internet
- Remote site policy requires centralized Internet access
- Enable EIGRP between VPN headend & Campus core to propagate default to remote
- Static default (admin dist=1) remains active
- User traffic from remote sites is forwarded to VPN-DMZ (wrong firewall interface for user traffic)
- Adjust admin distances to allow EIGRP default route (to core)
- VPN tunnel drops



DMVPN Deployment over Internet

No Split Tunneling at Remote-Site Location

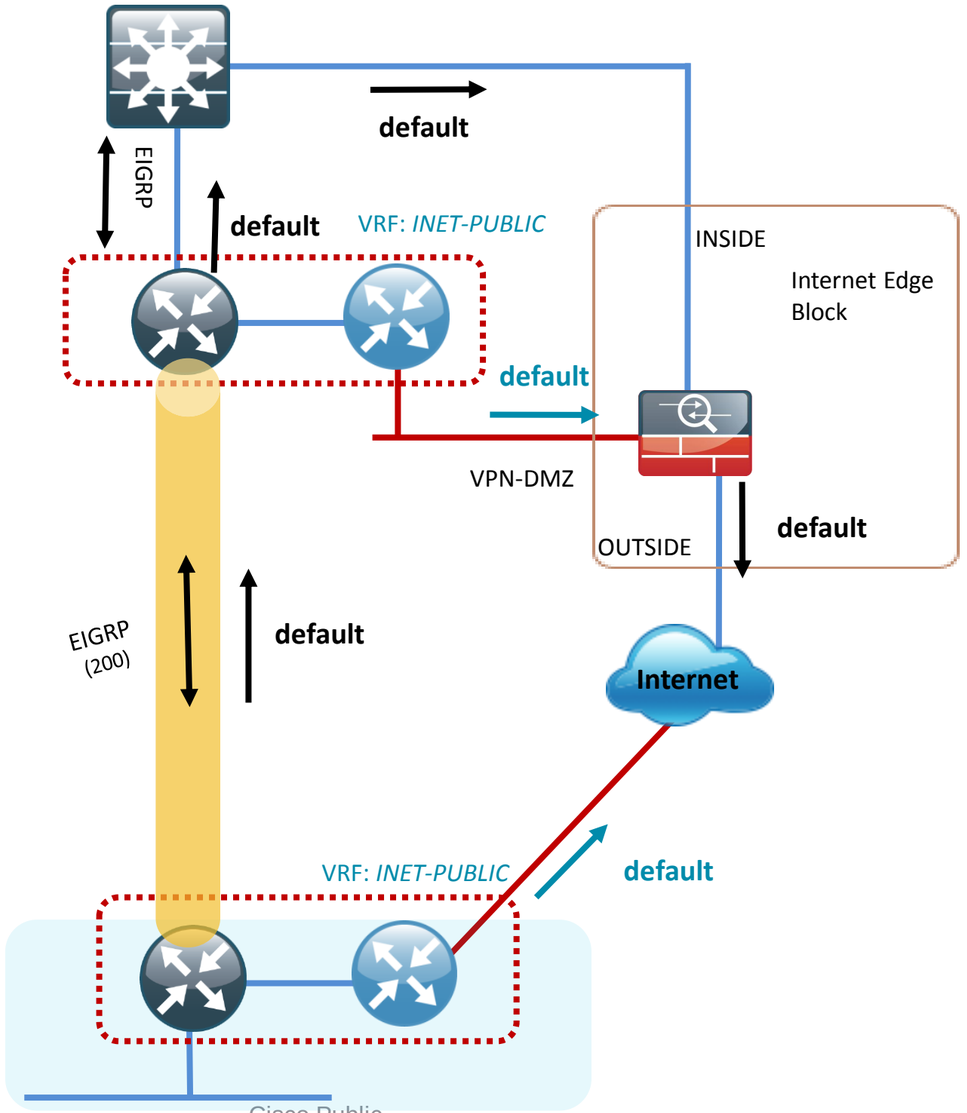
- Enable Front-Door VRF (FVRF) with DMVPN to permit two default routes
- The VRF INET-PUBLIC contains the default route to VPN-DMZ Interface needed for Tunnel Establishment
- A 2nd default route exists in the Global Routing Table used by the user traffic to reach Internet
- To enforce centralized tunneling the default route is advertised to spokes via Tunnel
- Spoke's tunnel drops due to 2nd default route conflict with the one learned from ISP



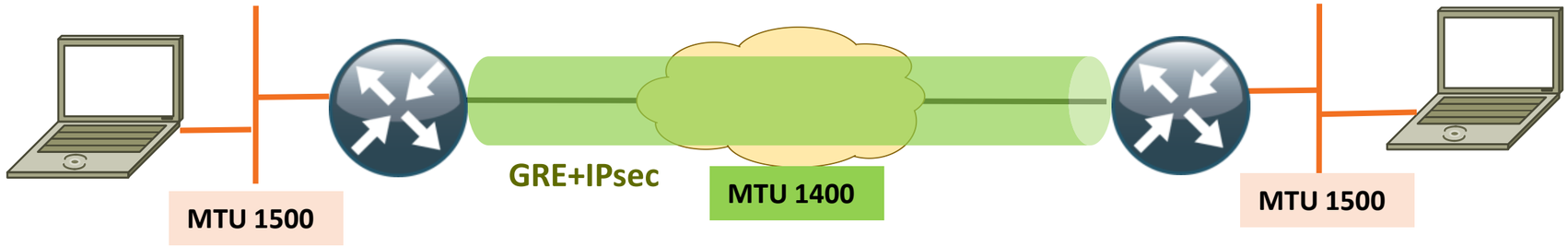
Best Practice: VRF-Aware DMVPN

Keeping the Default Routes in Separate VRFs

- Enable FVRF DMVPN on the Spokes
- Allow the ISP learned Default Route in the VRF INET-PUBLIC and use for tunnel establishment
- Global VRF contains Default Route learned via tunnel. User data traffic follows Tunnel to INSIDE interface on firewall
- Allows for consistent implementation of corporate security policy for all users



Avoid Fragmentation when Tunneling

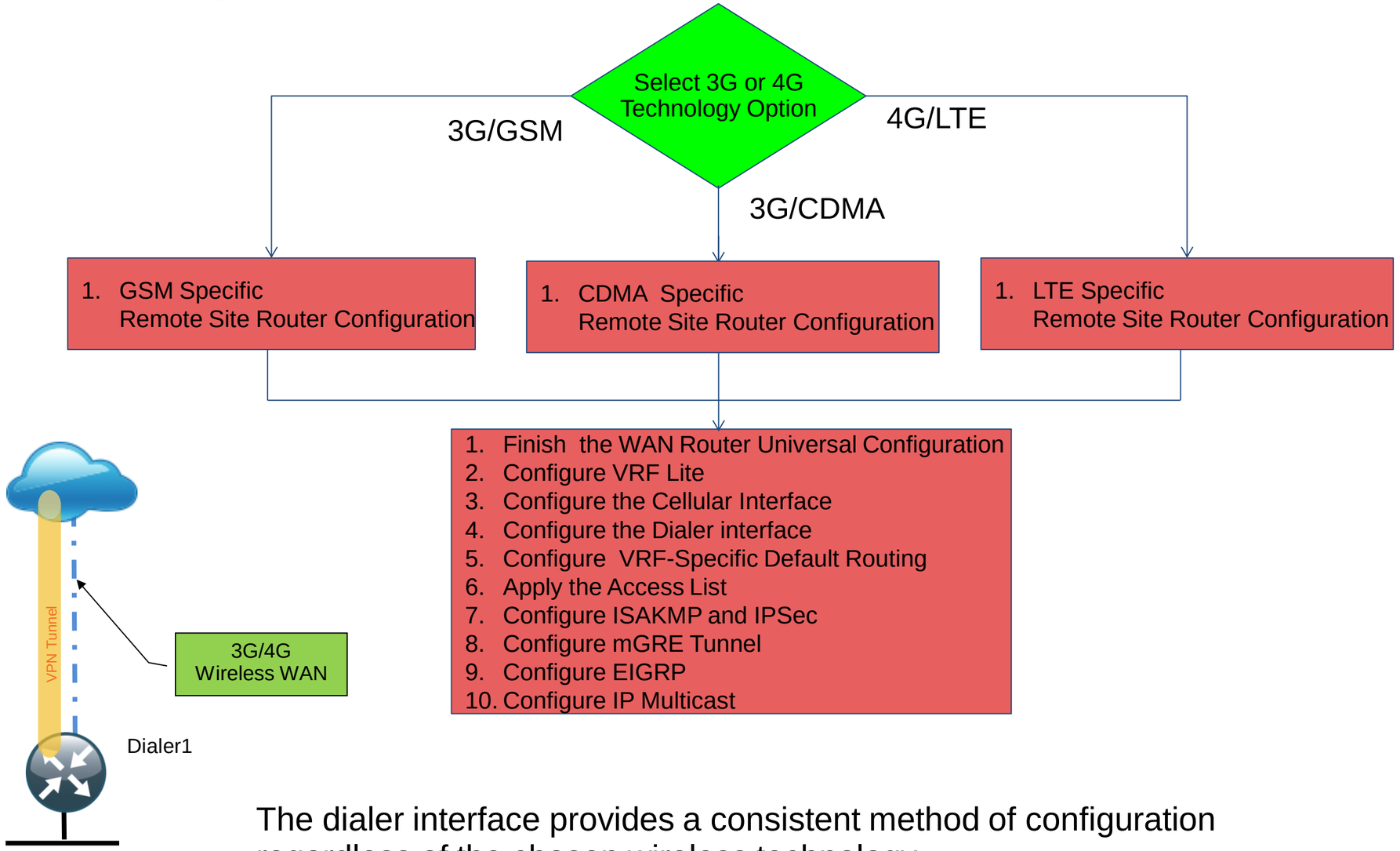


Tunnel Setting (esp-aes 256 esp-sha-hmac)	Maximum MTU	Recommended MTU
GRE/IPSec (Tunnel Mode)	1414 bytes	1400 bytes
GRE/IPSec (Transport Mode)	1434 bytes	1400 bytes

- IP fragmentation will cause CPU and memory overhead and result in lower throughput performance
- When one fragment of a datagram is dropped, the entire original IP datagram will have to be resent
- Use '***mode transport***' on transform-set
  - NHRP requires this for NAT support and it saves 20 bytes of overhead
- Avoid MTU issues with the following best practices
  - ***ip mtu 1400*** (WAN facing interface or tunnel)
  - ***ip tcp adjust-mss 1360*** (WAN facing interface or tunnel)

Remote-Site with 3G or 4G/LTE Wireless WAN

Best Practice Uses Dialer Interface



The dialer interface provides a consistent method of configuration regardless of the chosen wireless technology.

Wireless WAN with 3G (GSM and CDMA)

Two PPP Encapsulation Methods

CDMA Example

```
chat-script CDMA "" "ATDT#777" TIMEOUT 30 "CONNECT"

interface Cellular0/0/0
 bandwidth 1800
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 no peer default ip address
 async mode interactive
 no ppp lcp fast-start
!
interface Dialer1
 bandwidth 1800
 ip vrf forwarding INET-PUBLIC
 ip address negotiated
 ip access-group ACL-INET-PUBLIC in
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer string CDMA
 dialer persistent
 ppp ipcp address accept
!
line 0/0/0
 script dialer CDMA
 modem InOut
 no exec
```

GSM Example

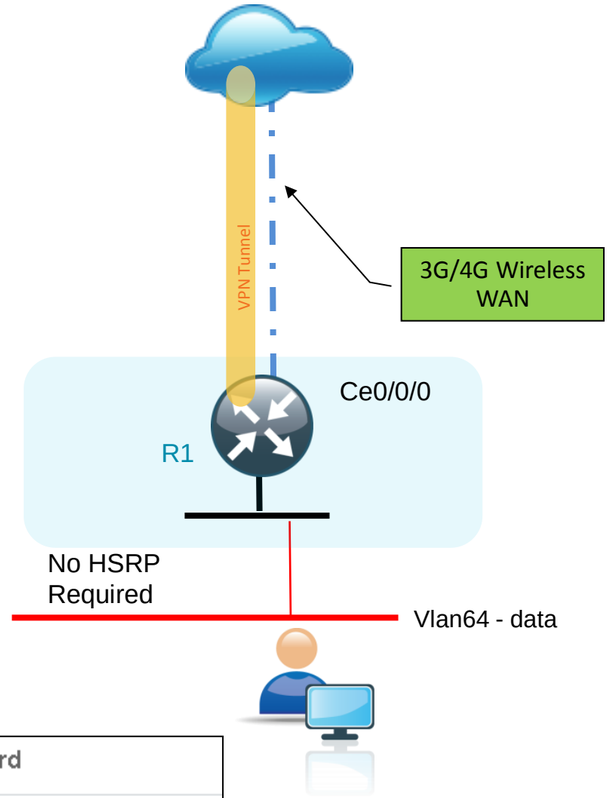
```
chat-script GSM "" "ATDT*98*1#" TIMEOUT 30 "CONNECT“
!
interface Cellular0/0/0
 bandwidth 384
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 no peer default ip address
 async mode interactive
 no ppp lcp fast-start
!
interface Dialer1
 bandwidth 384
 ip vrf forwarding INET-PUBLIC
 ip address negotiated
 ip access-group ACL-INET-PUBLIC in
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer string GSM
 dialer persistent
 no ppp lcp fast-start
 ppp chap hostname ISP@CINGULARGPRS.COM
 ppp chap password 7 02252D752C3323007E1F
 ppp ipcp address accept
 ppp timeout retry 120
 ppp timeout ncp 30
!
line 0/0/0
 script dialer GSM
 modem InOut
 no exec
```

Router with GSM must also create a profile

```
R1# cellular 0/0/0 gsm profile create 1 isp.cingular chap ISP@CINGULARGPRS.COM CINGULAR1
```

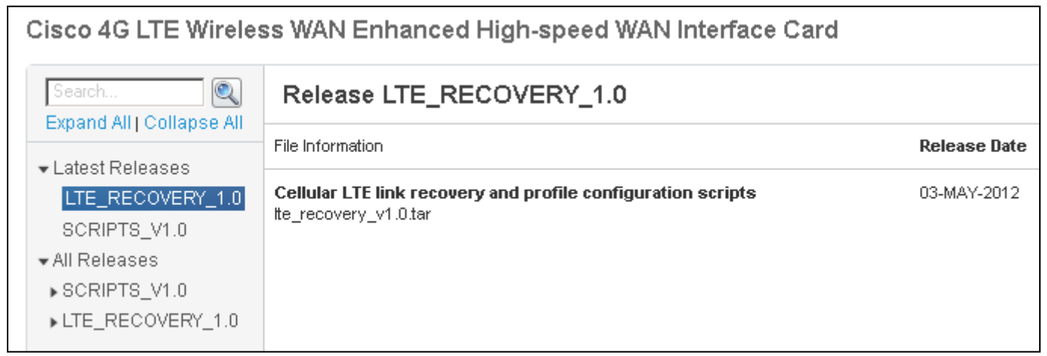
Wireless WAN with 4G/LTE

Direct IP Encapsulation Instead of PPP




```
R1#
chat-script LTE "" "AT!CALL1" TIMEOUT 20 "OK"

interface Cellular0/0/0
 bandwidth 2000
 no ip address
 encapsulation slip
 dialer in-band
 dialer pool-member 1
 no peer default ip address
 async mode interactive
!
interface Dialer1
 bandwidth 2000
 ip vrf forwarding INET-PUBLIC
 ip address negotiated
 ip access-group ACL-INET-PUBLIC in
 encapsulation slip
 dialer pool 1
 dialer idle-timeout 0
 dialer string LTE
 dialer persistent
!
line 0/0/0
 script dialer LTE
 modem InOut
 no exec
```

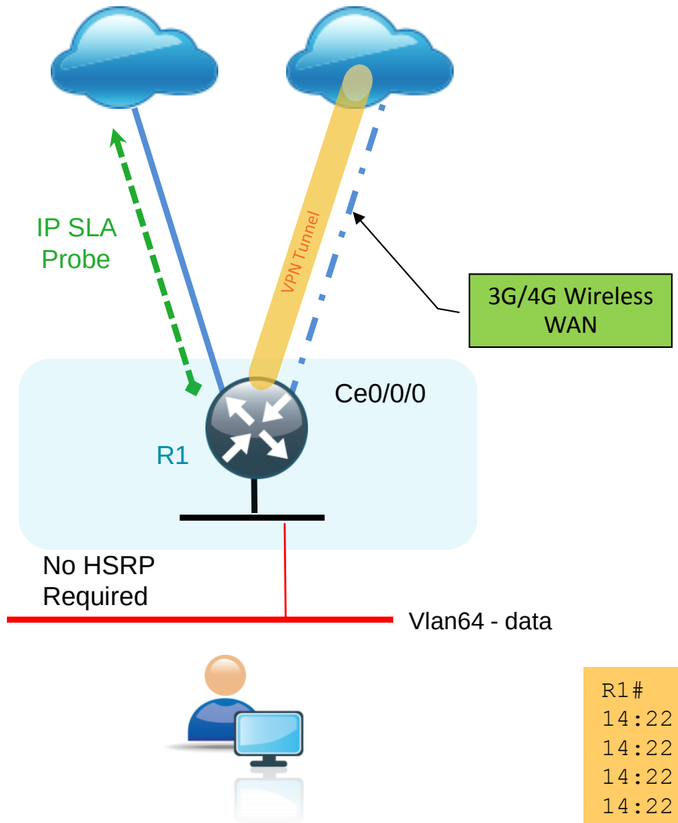
LTE recovery script recommended



- Direct IP requires SLIP encapsulation keyword
- No PPP authentication parameters required
- No profile required

Wireless WAN with 3G/4G Backup

Enhanced Object Tracking (EOT) with EEM Scripts



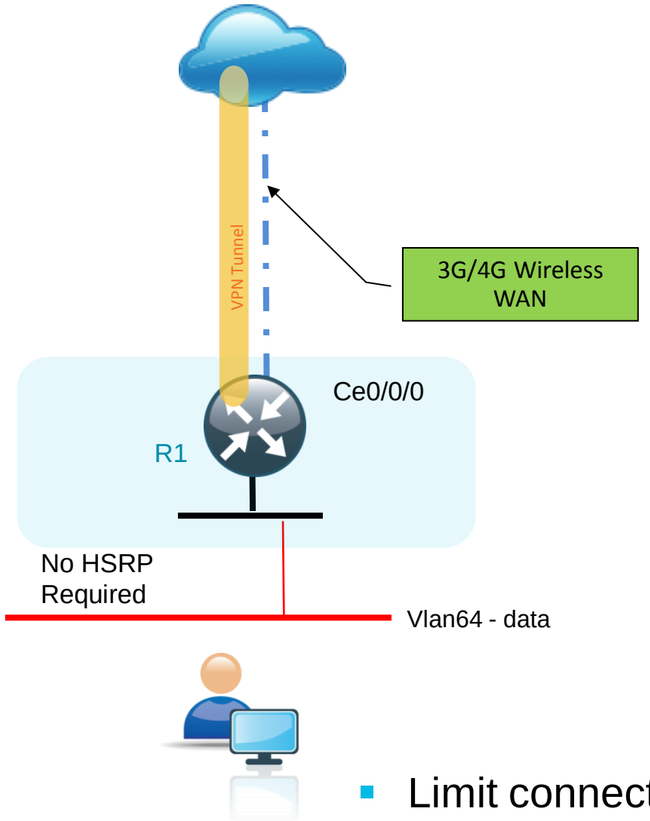

```
R1#
ip sla 100
 icmp-echo 192.168.3.26 source-interface
GigabitEthernet0/0
 timeout 1000
 threshold 1000
 frequency 15
ip sla schedule 100 life forever start-time now

track 60 ip sla 100 reachability

event manager applet ACTIVATE-3G
 event track 60 state down
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface cellular0/0/0"
 action 4  cli command "no shutdown"
 action 5  cli command "end"
 action 99 syslog msg "Activating 3G interface"
```

Note: This method is also compatible with a dual router design (probes are sent from R2)

```
R1#
14:22:14: %TRACKING-5-STATE: 60 ip sla 100 reachability Up->Down
14:22:14: %SYS-5-CONFIG_I: Configured from console by  on vty0(EEM:ACTIVATE-3G)
14:22:14: %HA_EM-6-LOG: ACTIVATE-3G: Activating 3G interface
14:22:34: %LINK-3-UPDOWN: Interface Cellular0/0/0, changed state to up
14:22:34: %DIALER-6-BIND: Interface Ce0/0/0 bound to profile Di1
14:22:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0/0/0, changed state to up
14:22:40: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state to up
14:22:40: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
14:22:42: %DUAL-5-NBRCHANGE: EIGRP-IPv4 200: Neighbor 10.4.34.1 (Tunnel11) is up: new adjacency
```

Wireless WAN with 3G/4G Only Link

Time Based Connection with EEM Scripts




```
R1#
event manager applet TIME-OF-DAY-ACTIVATE-3G
 event timer cron cron-entry "45 4 * * 1-5"
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface cellular0/0/0"
 action 4  cli command "no shutdown"
 action 5  cli command "end"
 action 99 syslog msg "M-F @ 4:45AM Activating 3G interface"

event manager applet TIME-OF-DAY-DEACTIVATE-3G
 event timer cron cron-entry "15 18 * * 1-5"
 action 1  cli command "enable"
 action 2  cli command "configure terminal"
 action 3  cli command "interface cellular0/0/0"
 action 4  cli command "shutdown"
 action 5  cli command "end"
 action 99 syslog msg "M-F @ 6:15PM Deactivating 3G interface"
```

- Limit connection time to reduce usage charges
- EEM scripts leverage CRON
- Additional scripting or enhancements can allow for manual override for weekend or after hours use.

WAN Quality of Service

Defining SBA QoS Classes of Services

Class of Service	Traffic Type	DSCP Value(s)	Bandwidth (%)	Congestion Avoidance
VOICE	Voice traffic	ef	10 (PQ)	
INTERACTIVE-VIDEO	Interactive video (video conferencing)	cs4 af41	23 (PQ)	
CRITICAL-DATA	Highly interactive (such as Telnet, Citrix, and Oracle thin clients)	cs3 af31	15	DSCP based
DATA	Data	af21	19	DSCP based
SCAVENGER	Scavenger	cs1 af11	5	
NETWORK-CRITICAL	Routing protocols. Operations, administration and maintenance (OAM) traffic.	cs2 cs6	3	
class-default	Best effort	other	25	random

All WAN routers:

```
class-map match-any VOICE
 match dscp ef
class-map match-any INTERACTIVE-VIDEO
 match dscp cs4  af41
class-map match-any CRITICAL-DATA
 match dscp cs3  af31
class-map match-any DATA
 match dscp af21
class-map match-any SCAVENGER
 match dscp cs1  af11
class-map match-any NETWORK-CRITICAL
 match dscp cs2  cs6
```

For MPLS CE routers:

```
class-map match-any BGP-ROUTING
 match protocol bgp
policy-map MARK-BGP
 class BGP-ROUTING
  set dscp cs6
```

For DMVPN routers:

```
ip access-list extended ISAKMP
 permit udp any eq isakmp any eq isakmp
class-map match-any NETWORK-CRITICAL
 match access-group name ISAKMP
```

WAN Design and Deployment Using SBA

Agenda

- SBA WAN Overview
- SBA WAN Design Methodology
- Key Aspects of the Design
- Summary

Summary

- The SBA WAN design methodology allows for either a small or large scale initial deployment.

- Flexibility is built into the WAN and remote-site design. Adding additional scale, resiliency or capabilities is straightforward.

- The SBA WAN design uses advanced features and capabilities. Each is documented in a prescriptive manner.
  - Route-maps ensure routing stability
  - F-VRF DMVPN permits spoke-spoke with central tunneling
  - WAAS GRE negotiated return enables shared clusters
  - EEM scripts extend capabilities of EOT


CISCO