The bridge to possible

Обзор FlexVPN

Апрель 2021

План сессии

- Начнем с основ – что такое FlexVPN
  - И как организована обработка трафика
- Hub & Spoke дизайн на базе IKEv2
- Hub & Spoke дизайн на базе BGP
- MPLS over FlexVPN
- Обеспечение высокой доступности
- Балансировка нагрузки
- Защита от филиалов

- Сценарии Remote Access VPN на базе Flex
  - AAA, AC-EAP
  - Clients supported
  - VPN Profiles
  - SSL/IPSec support
- Примеры использования FlexVPN:
  - FlexVPN as SD-Transit
  - WFH/COVID-19 response - Mixed Client & Branch Access
- Поддержка FlexVPN на различных платформах

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-WAN, FlexVPN, ASA and FTD

SD-WAN

FlexVPN

ASA

NG-FW/FTD

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Overview

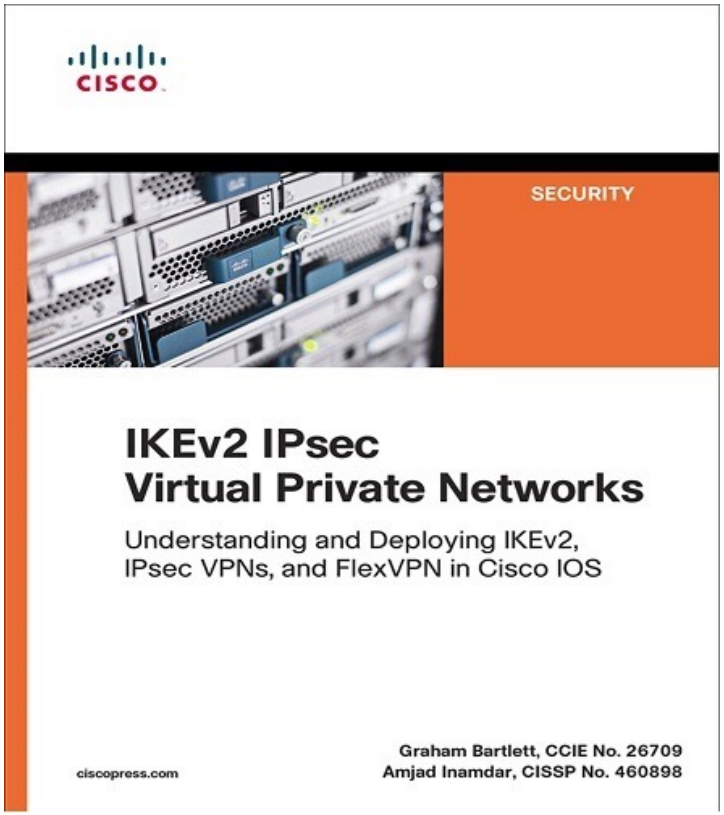
What is FlexVPN?

IKEv2-based unified VPN technology that combines site-to-site, remote-access, hub-spoke and spoke-to-spoke topologies

Highlights

- Unified CLI
- Based on and compliant to IKEv2, Interoperable with non-Cisco Implementations
- Unified features: most features available across topologies (AAA, IPv6, Routing…)
- Leverages IOS Point-to-Point tunnel interface
- Simplified configuration using smart-defaults

Cisco Press Book ‘IKEv2 IPsec VPNs’ by Amjad Inamdar & Graham Bartlett



https://www.amazon.com/IKEv2-IPsec-Virtual-PrivateNetworks/dp/1587144603/

Listed in the CCIE Security reading list
https://learningnetwork.cisco.com/community/certifications/ccie_security/written_exam/study-material

Customer Reviews

One of the best technical books I've read
This book is the IKEv2 VPN equivalent of Jeff Doyle's Routing TCP/IP Vol 1 & 2 - a must read for any network security engineer wanting to design and build secure VPN's. One of the best technical books I've read.

Superb book and well worth the money for anyone even thinking about Cisco crypto
This book is the most comprehensive book on IKEv2 for Cisco network engineers that you will find and is all about real-world scenarios.

Definitive guide on modern IPsec VPN theory and practice
Many times I wish I had a book like this to help distill many complex IETF RFCs into “plain English” and provide practical and actionable security best practices.

Brilliant
I bought the Kindle version of this on a bit of an impulse. I'm really glad I did, it's well worth the money. Not only can I establish secure IKEv2 tunnels, I also feel like I know the subject thoroughly now. Even in respect to non-Cisco equipment. The book is a great reference too. I don't usually leave reviews but was motivated to in this instance. Good job, highly recommended.

The best book on IKEv2 IPsec VPNs
The book is awesome! I appreciate authors' work on presenting deeply technical topics in extremely easy to understand manner.

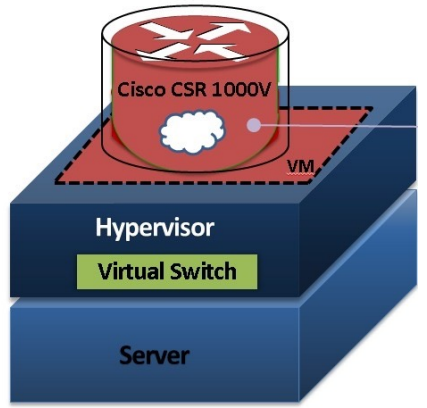
Finally, all you need to know about FLEX in one place!
Well written , concise and accurate. An absolute must for anyone designing, supporting or troubleshooting IKEv2 VPNs. You too can become a FLEX expert!

Very good Book on IPsec VPN for Enterprise networks
Very well Written book, This book touches on most important topic on building Dynamic VPN for enterprise networks.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Platforms

CSR 1000v



ASR 1000 series

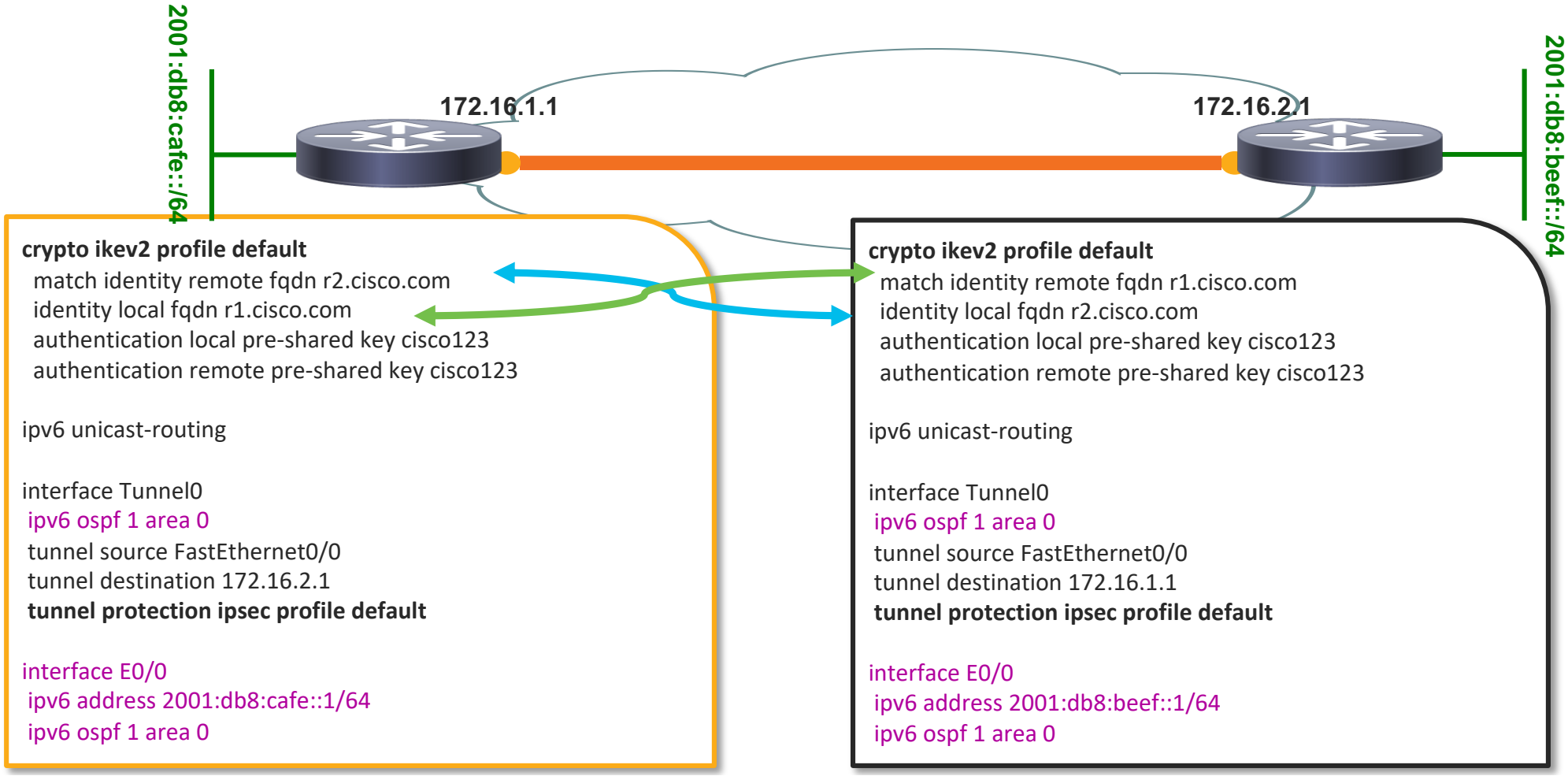
ISR 800, 1100
& 4000 Series

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Quick Recap

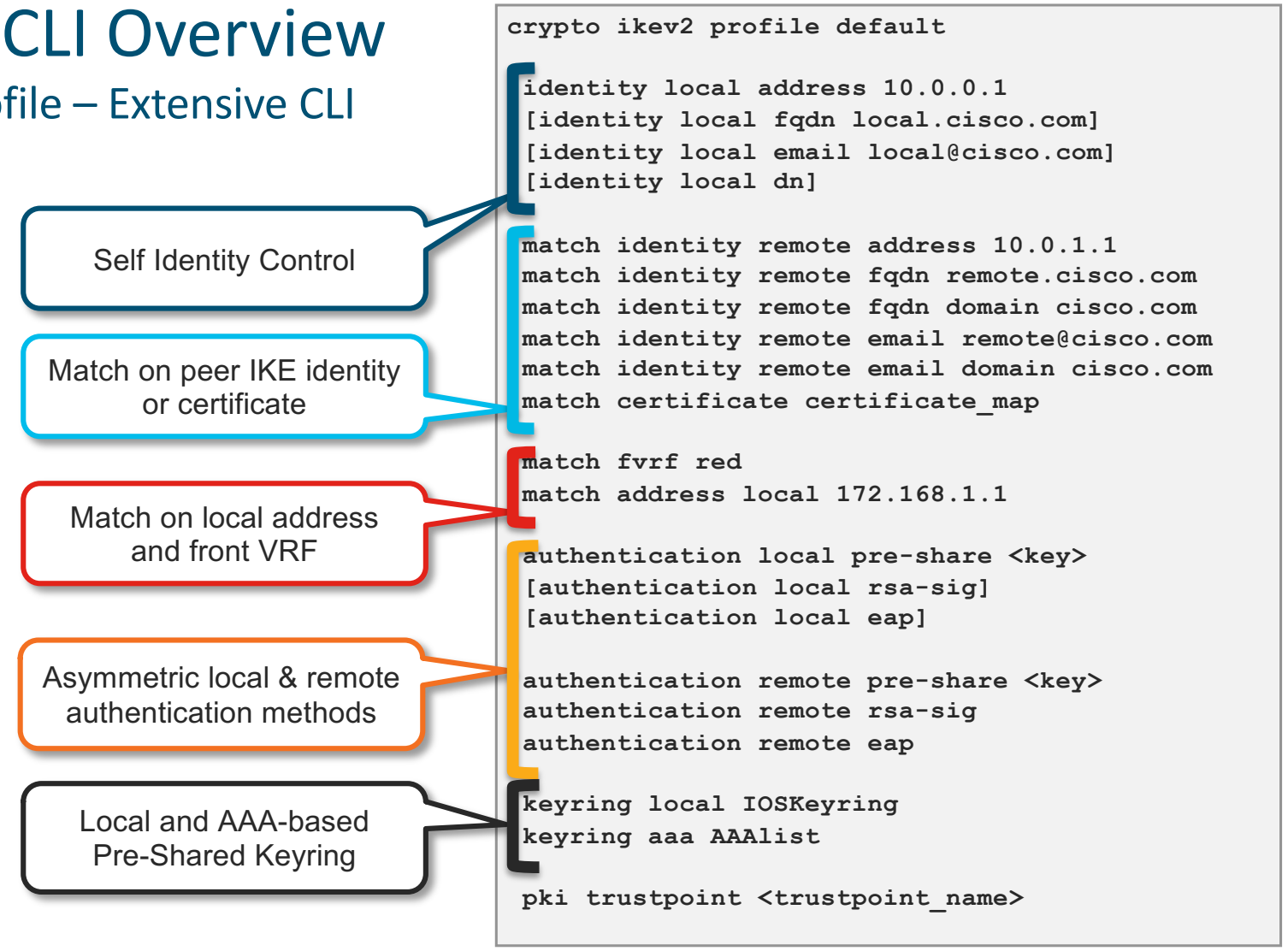
A Simple Site-to-Site Configuration

Example with IPv6 over IPv4 tunneling



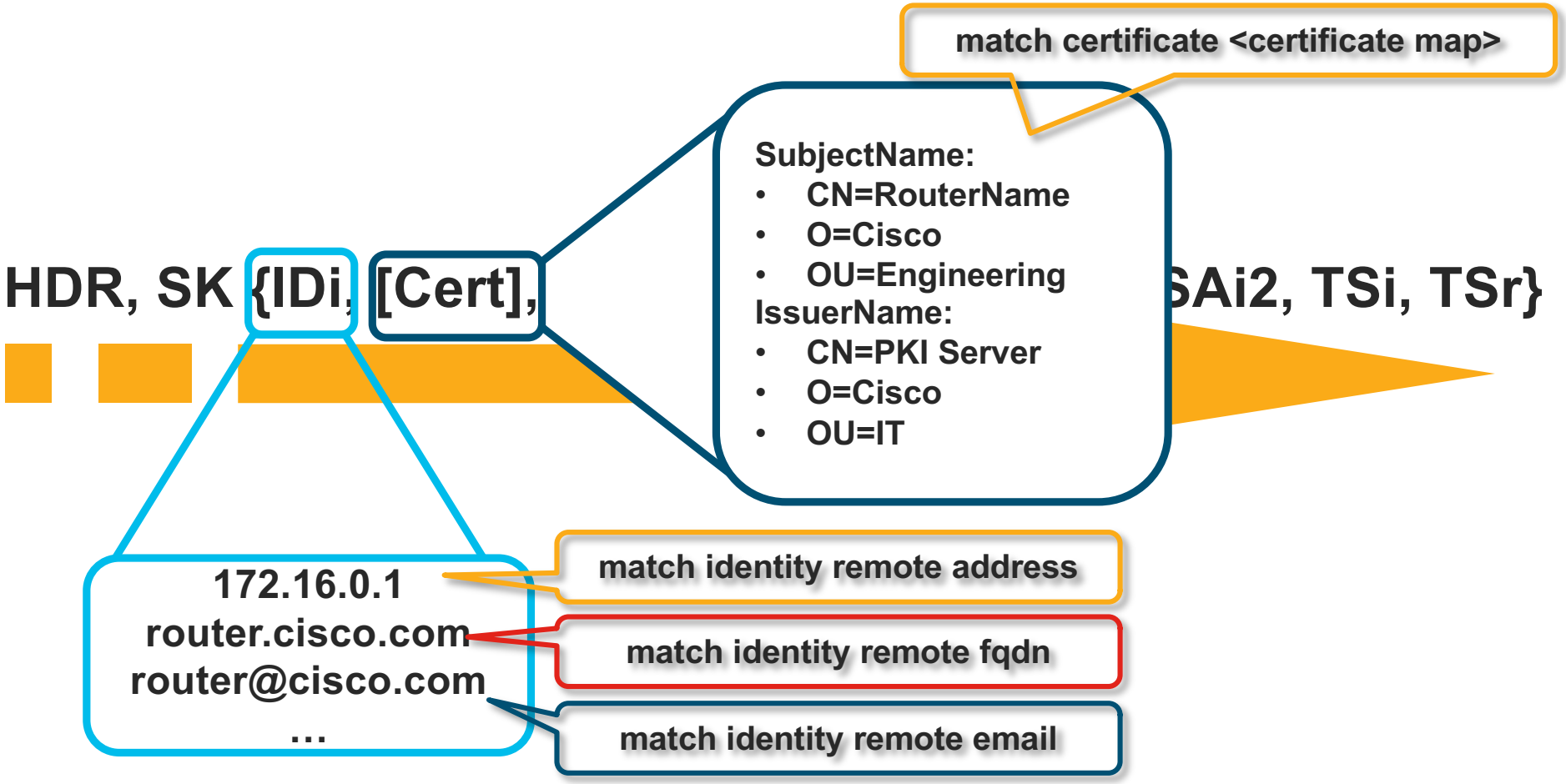
IKEv2 CLI Overview

IKEv2 Profile – Extensive CLI



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

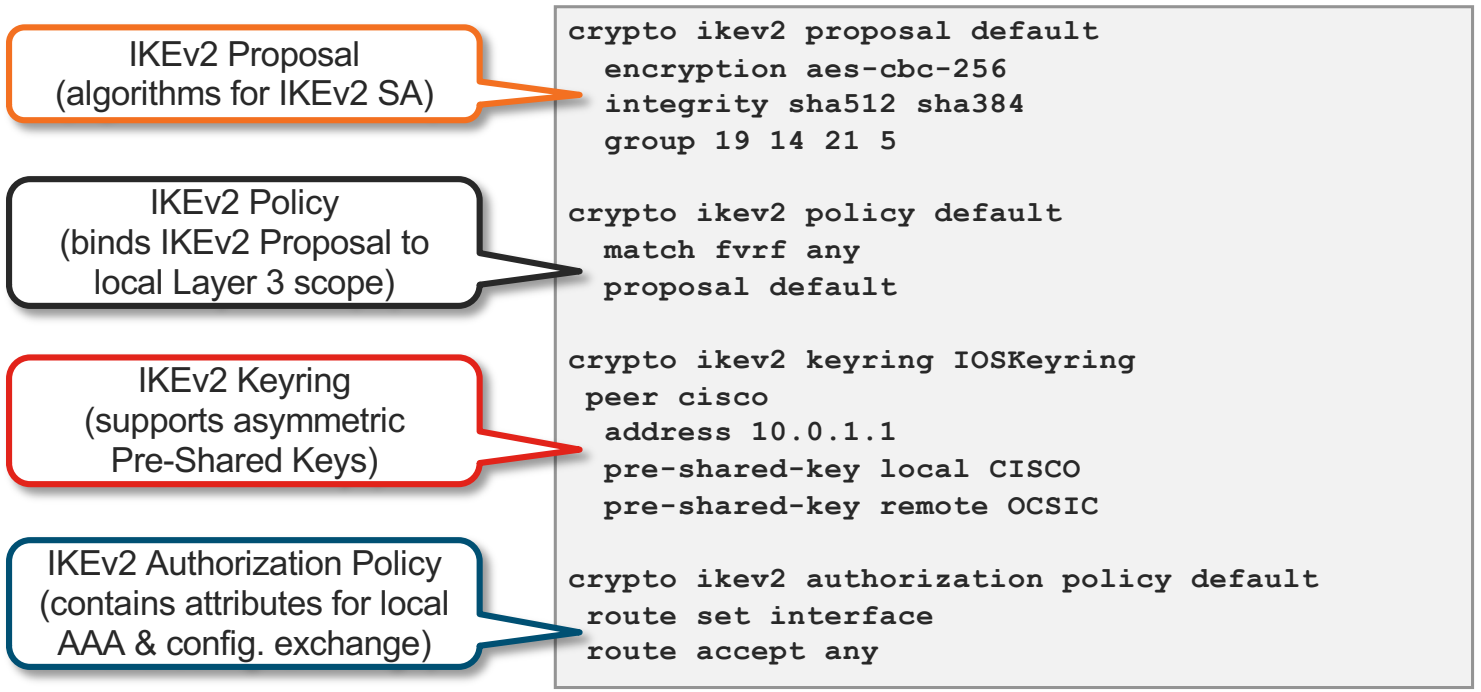
IKEv2 Profile Match Statements



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 CLI Overview

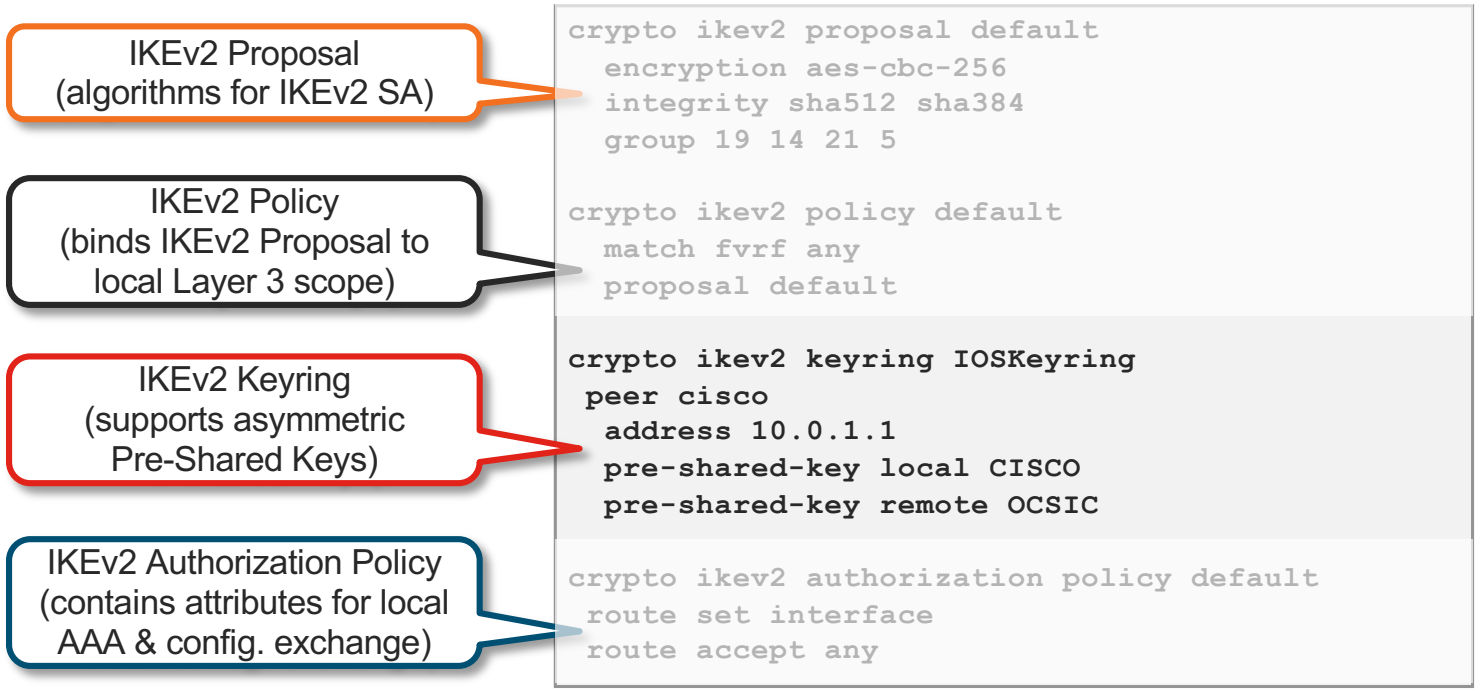
Proposal, Policy, and Keyring



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 CLI Overview - Smart Defaults

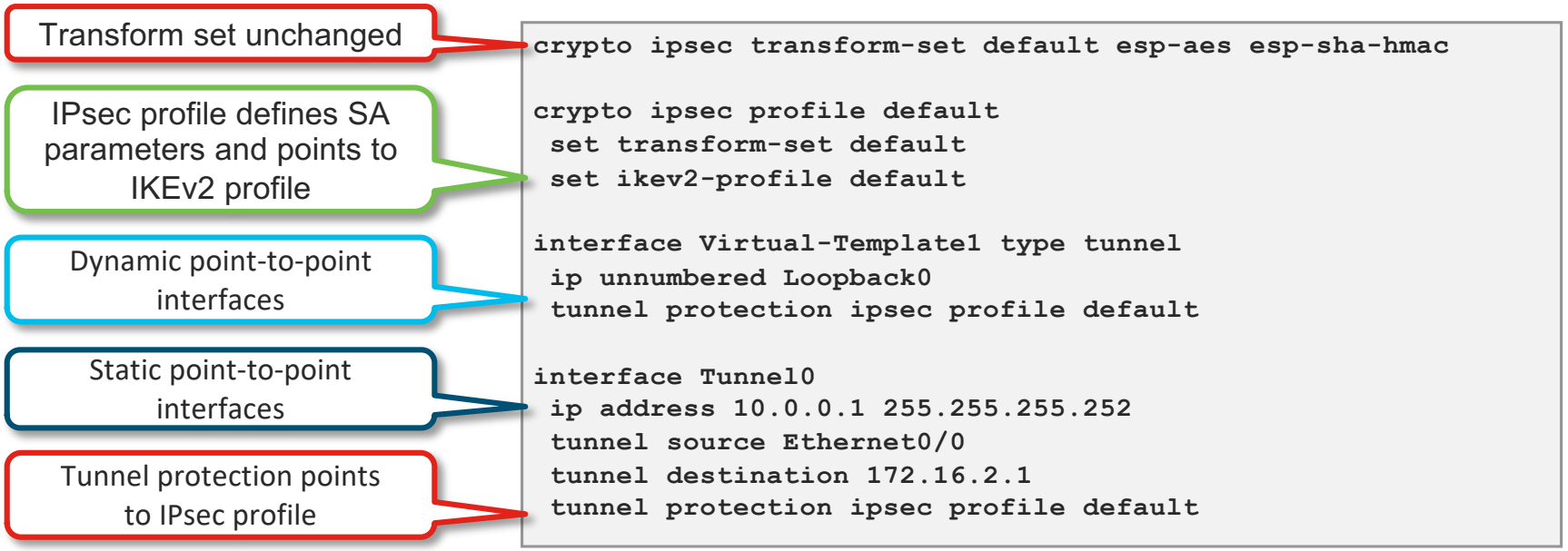
Proposal, Policy, and Keyring



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPSec CLI Overview

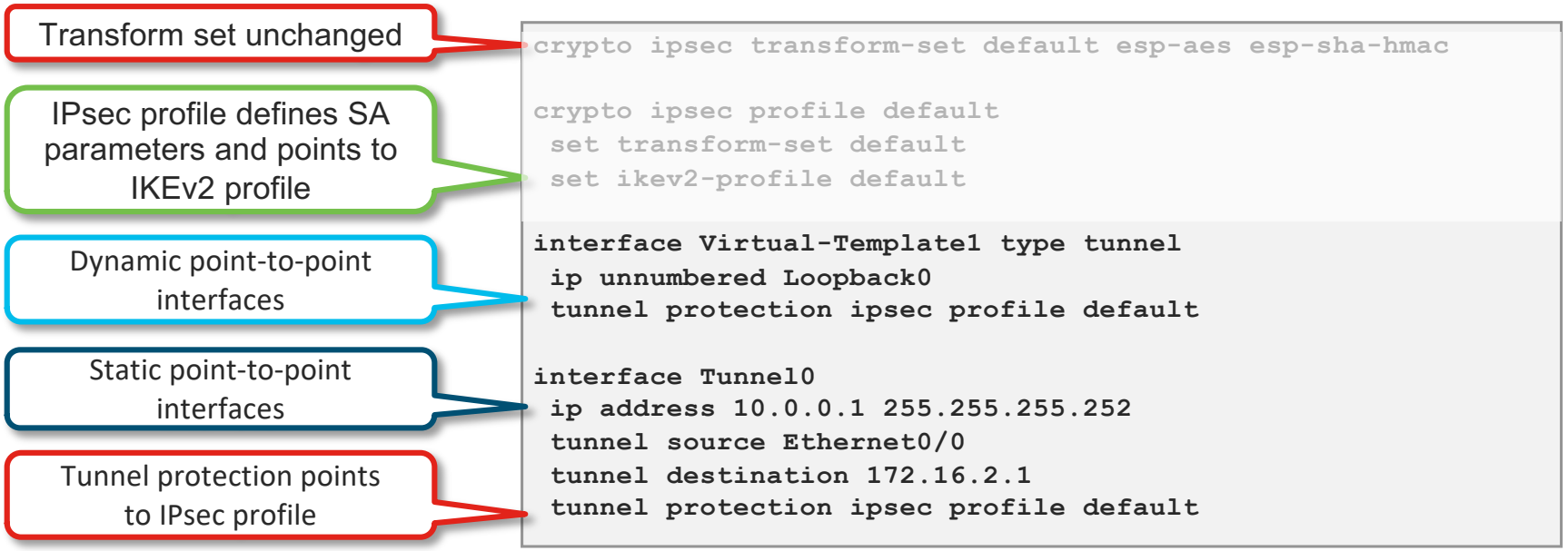
Tunnel Protection similar to DMVPN and EasyVPN



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPSec CLI Overview – Smart Defaults

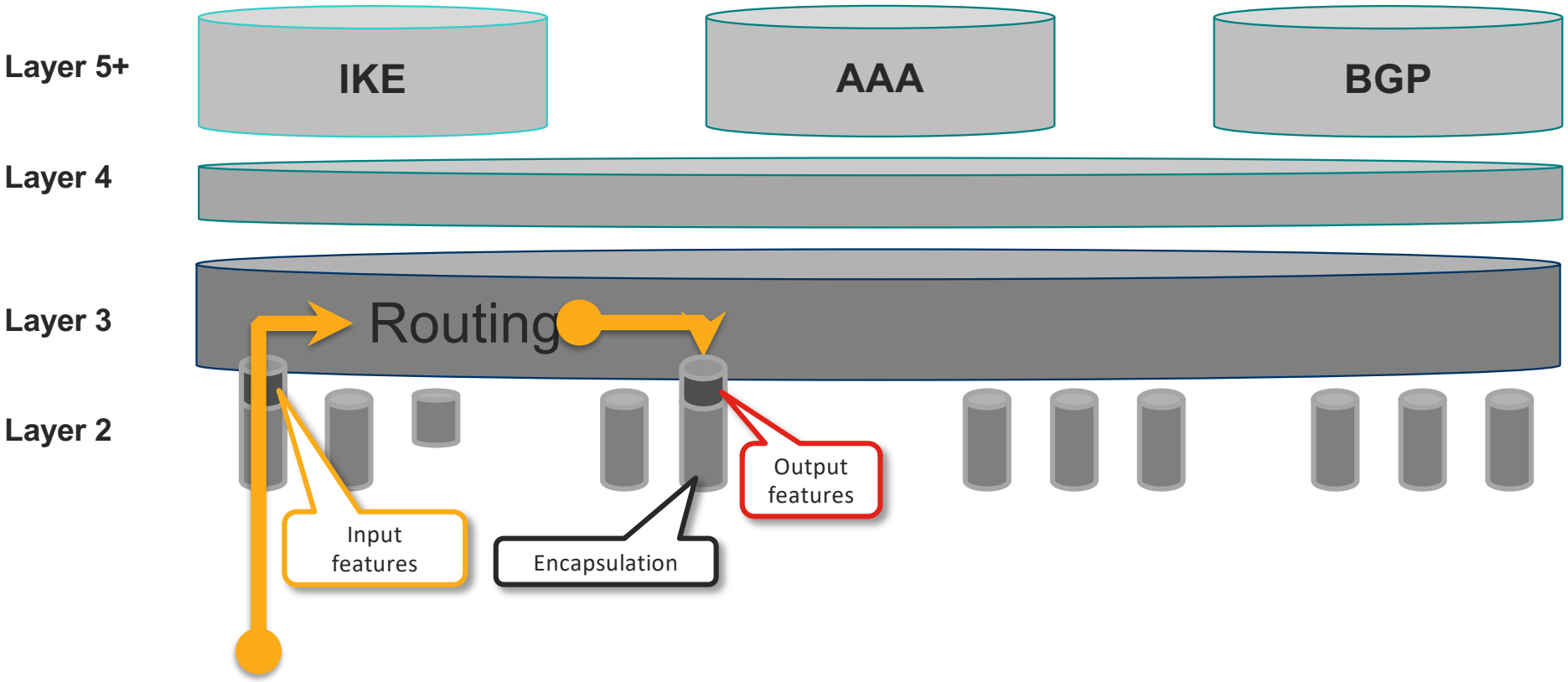
Tunnel Protection similar to DMVPN and EasyVPN



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

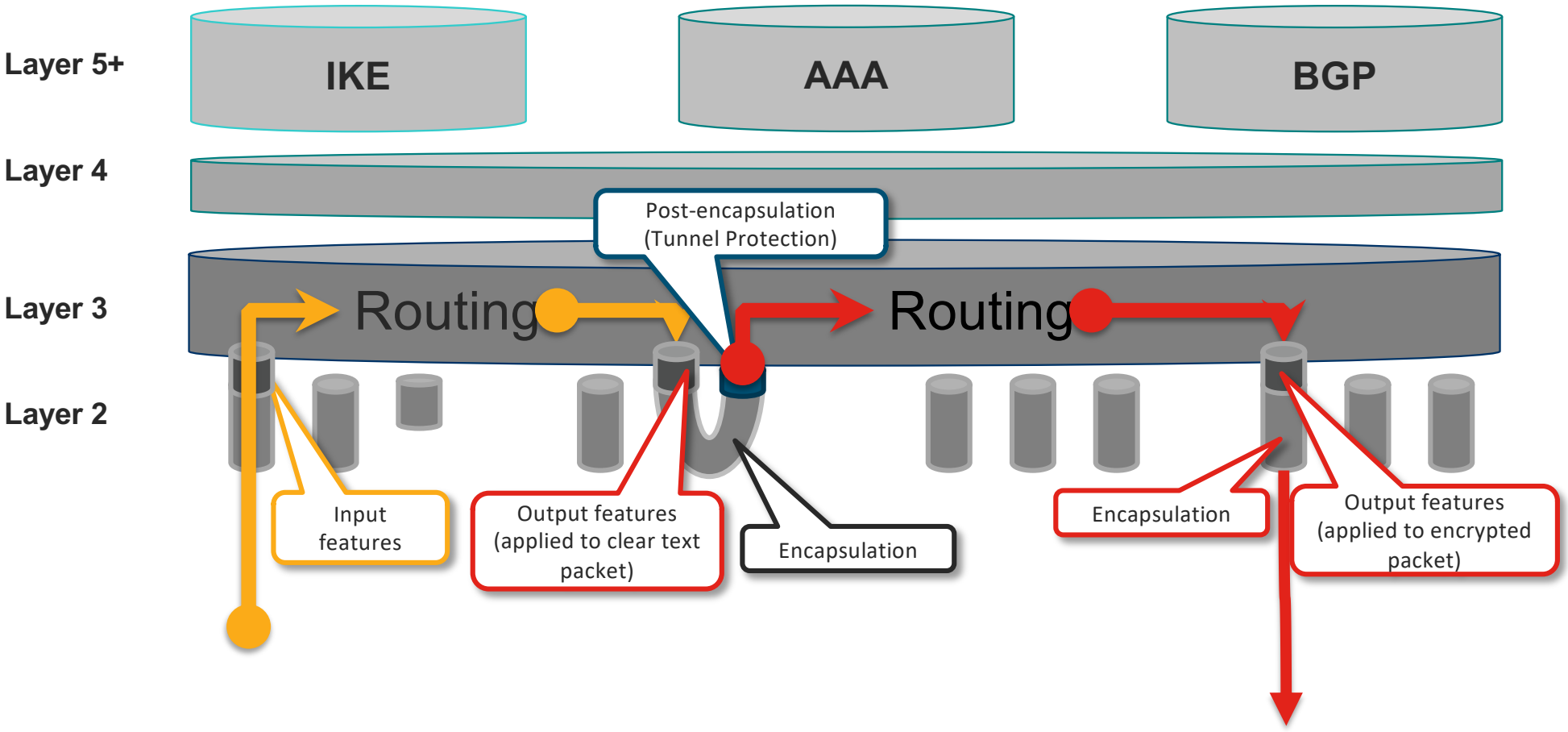
Packet Forwarding Simple Example

Basic Packet Forwarding



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Packet Forwarding – Tunnels & Features



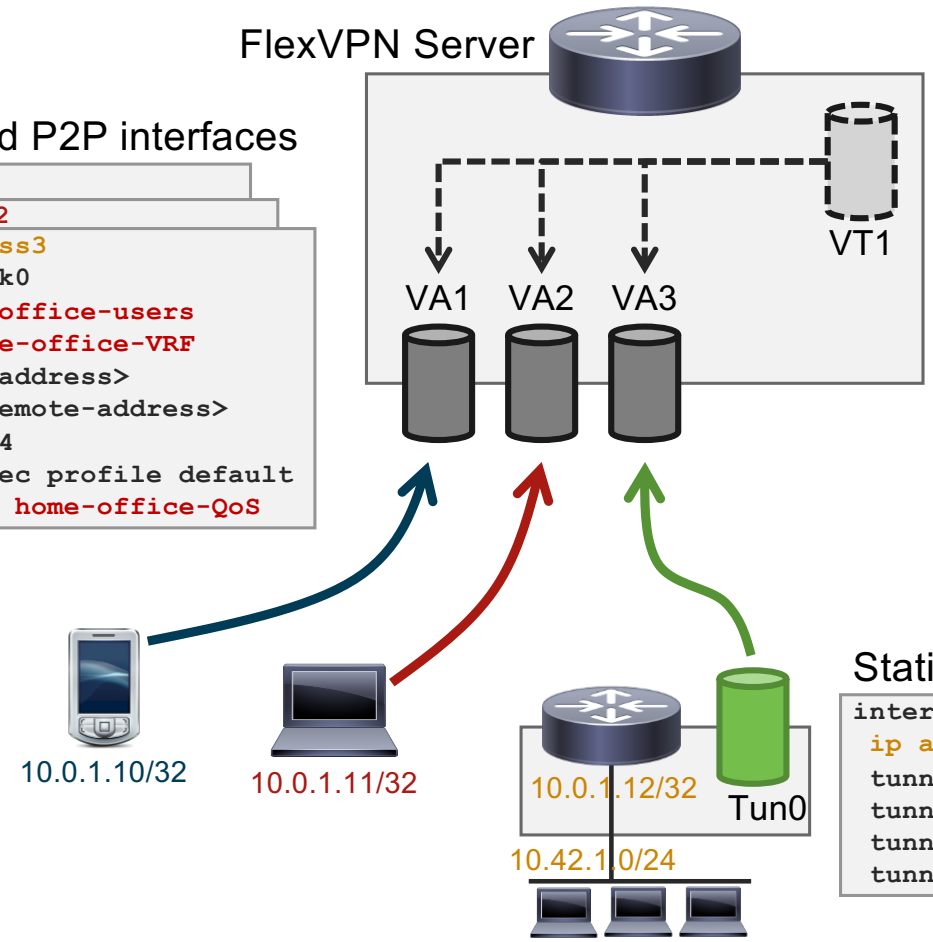
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tunnel Interfaces

Dynamic Point-to-Point Virtual Interfaces

Dynamically instantiated P2P interfaces

```
interface Virtual-Access1
interface Virtual-Access2
interface Virtual-Access3
 ip unnumbered Loopback0
 ip access-group home-office-users
 ip vrf forwarding home-office-VRF
 tunnel source <local-address>
 tunnel destination <remote-address>
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
 service-policy output home-office-QoS
```



P2P virtual interface template

```
crypto ikev2 profile default
 ...
 virtual-template 1
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Server routing table (RIB/FIB)

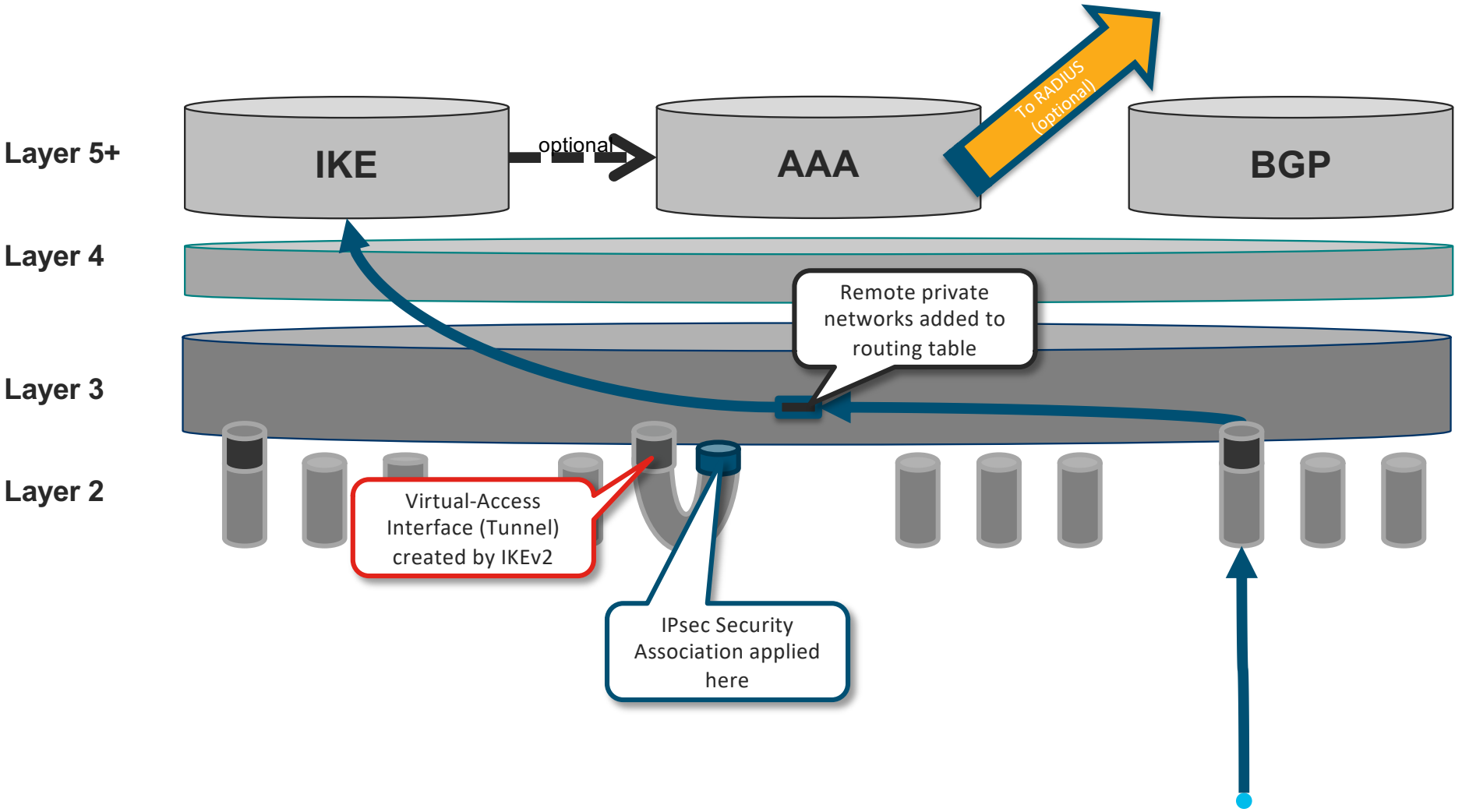
```
S default via Ethernet0/0
L 10.0.1.1/32 local Loopback0
S 10.0.1.10/32 via Virtual-Access1
S 10.0.1.11/32 via Virtual-Access2
S 10.0.1.12/32 via Virtual-Access3
S 10.42.1.0/24 via Virtual-Access3
```

Static P2P virtual interface

```
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination <server-address>
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Virtual-Access (Tunnel) Instantiation



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPv6 Support Summary

- GRE over IPSec
  - Dual-stack (IPv4 + IPv6 over IPSec) out of the box

Passenger Protocol

Transport Protocol	IPv4	IPv6
IPv4	✓	✓
IPv6	✓	✓

- IPSec Tunnel Mode
  - Dual-stack support
  - IPv4 over IPv6 mixed-mode

Passenger Protocol

Transport Protocol	IPv4	IPv6
IPv4	✓	✓
IPv6	✓ (Since XE3.10)	✓

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Tunnel modes made easy

```
crypto ikev2 profile prof1
 …
 virtual template 1
interface virtual-template 1
 …
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile prof2
 …
 virtual template 2
interface virtual-template 2
 …
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile prof3
 …
 virtual template 3
interface virtual-template 3
 …
 tunnel mode gre ip
 tunnel protection ipsec profile default
```

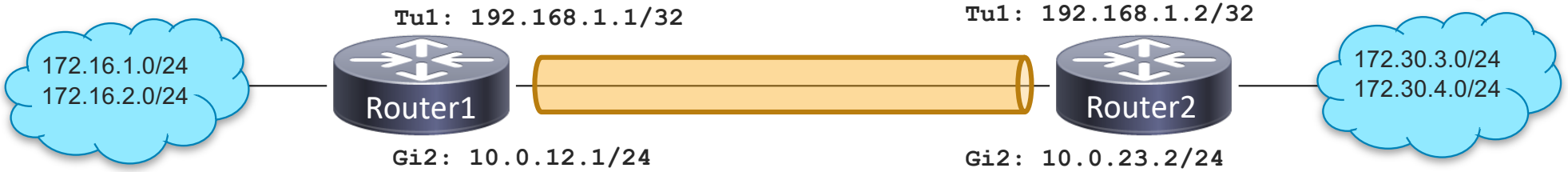
```
crypto ikev2 profile prof4
 …
 virtual template 4
interface virtual-template 4
 …
 tunnel mode gre ipv6
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile default
 …
 virtual template 1 mode auto

interface virtual-template 1
 …
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 Multi-SA SVTI - Configuration

IOS XE 16.12.1



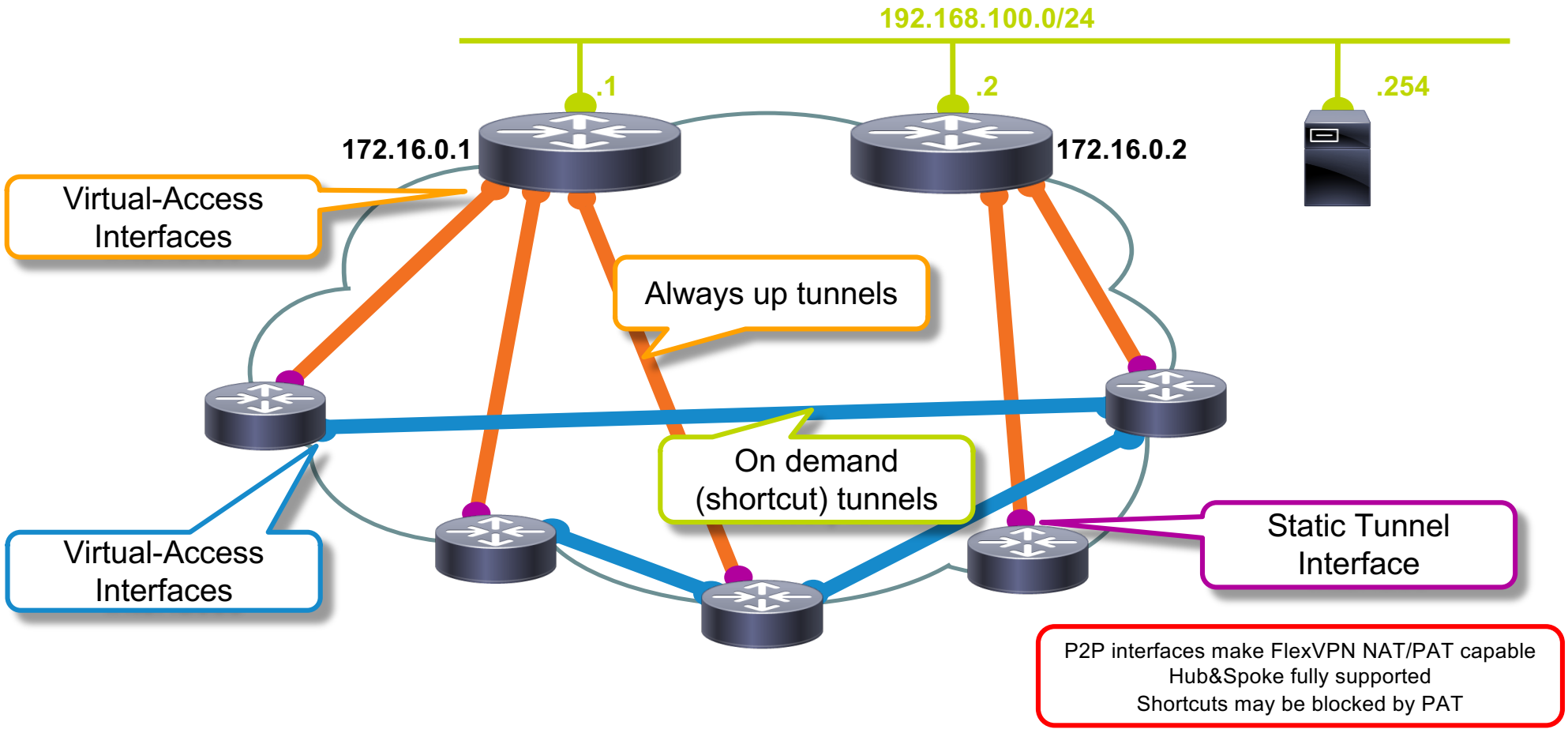

```
crypto ikev2 profile default
 match identity remote 10.0.23.2
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
!
crypto ipsec profile default
 reverse-route
!
ip access-list extended SVTI_ACL
 permit ip 172.16.1.0 0.0.0.255 172.30.3.0 0.0.0.255
 permit ip 172.16.2.0 0.0.0.255 172.30.4.0 0.0.0.255
!
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 10.0.23.2
 tunnel protection ipsec policy ipv4 SVTI_ACL
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile default
 match identity remote 10.0.12.1
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
!
crypto ipsec profile default
 reverse-route
!
ip access-list extended SVTI_ACL
 permit ip 172.30.3.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 172.30.4.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface Tunnel1
 ip address 192.168.1.2 255.255.255.252
 tunnel source GigabitEthernet2
 tunnel mode ipsec ipv4
 tunnel destination 10.0.12.1
 tunnel protection ipsec policy ipv4 SVTI_ACL
 tunnel protection ipsec profile default
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

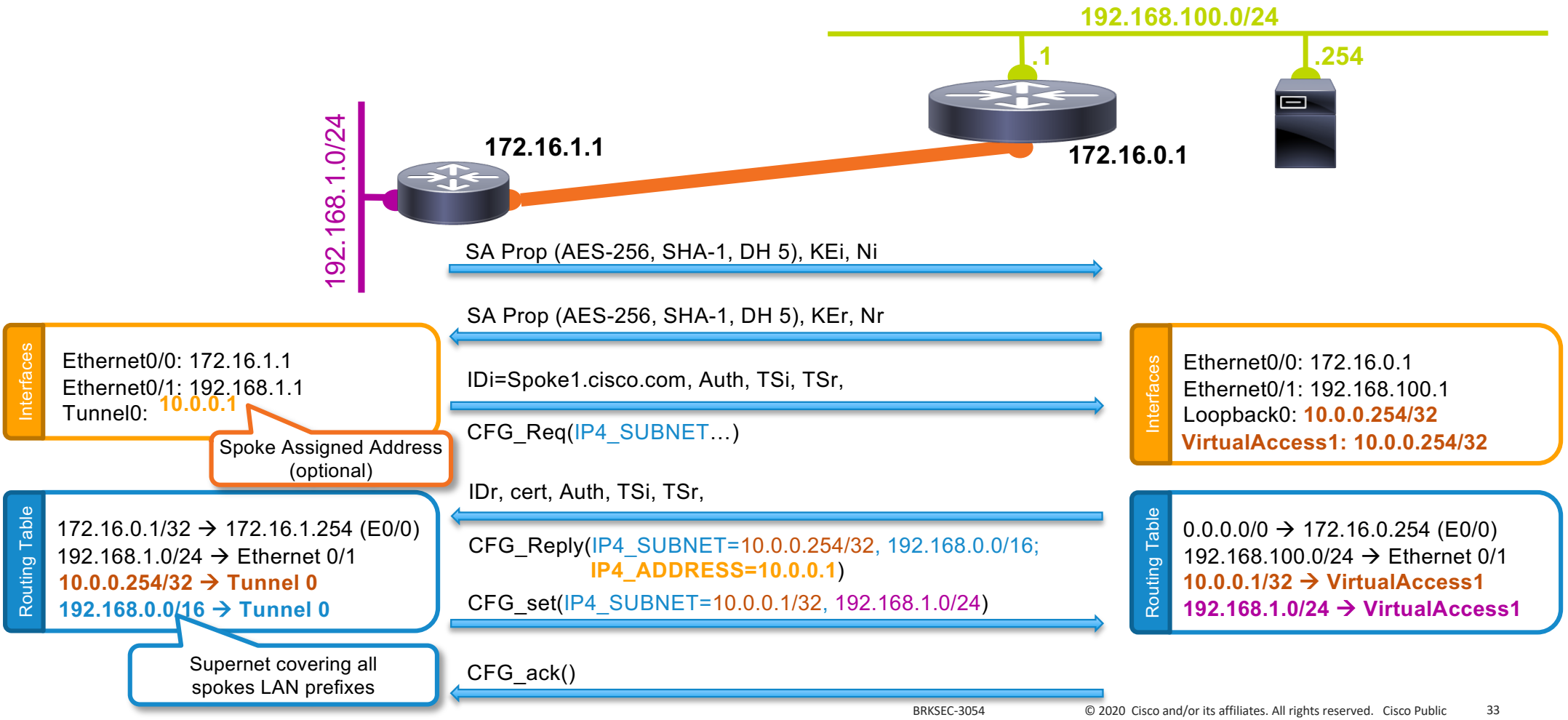
Hub & Spoke and Shortcut Switching with IKEv2 Routing

FlexVPN Mesh – Scalable Network Diagram



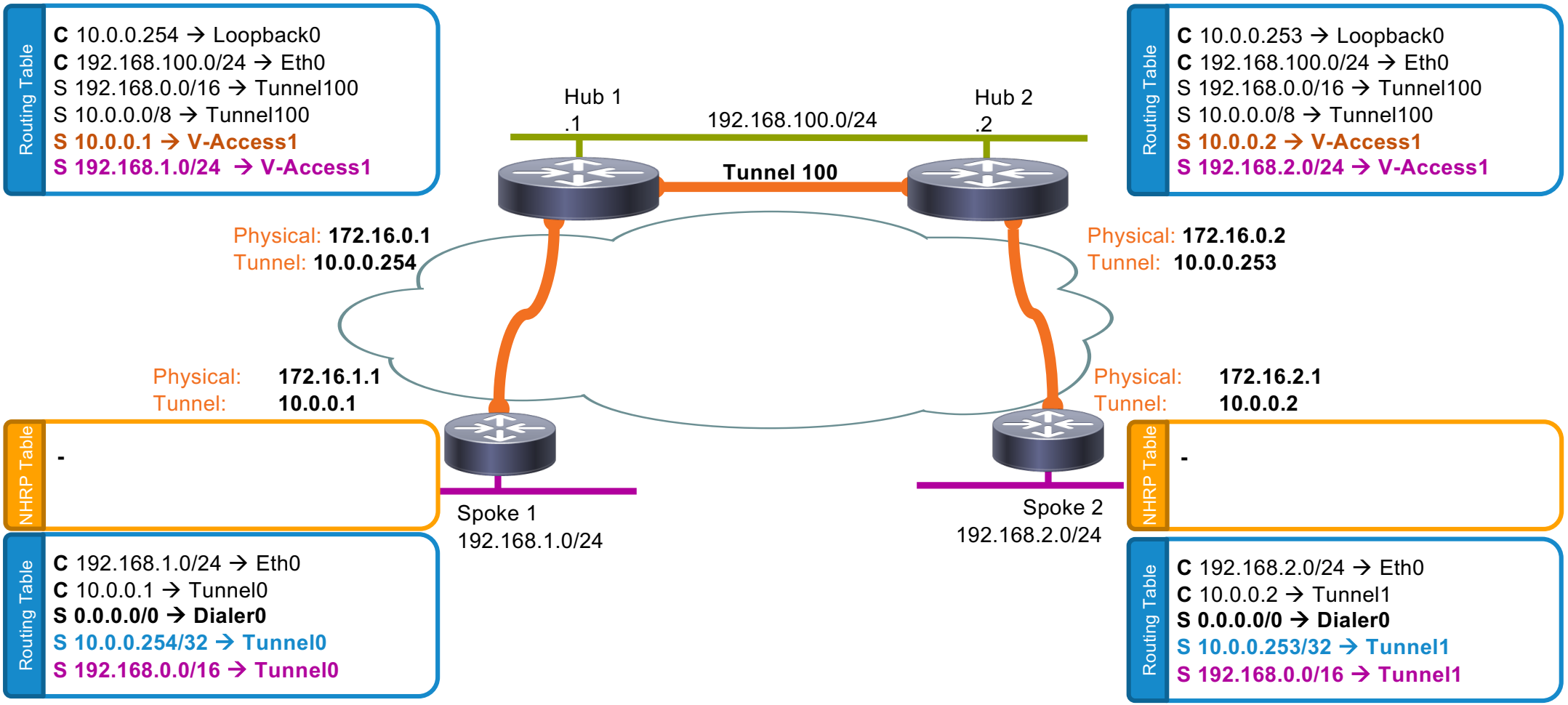
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hub & Spoke Bootstrap – Config Exchange



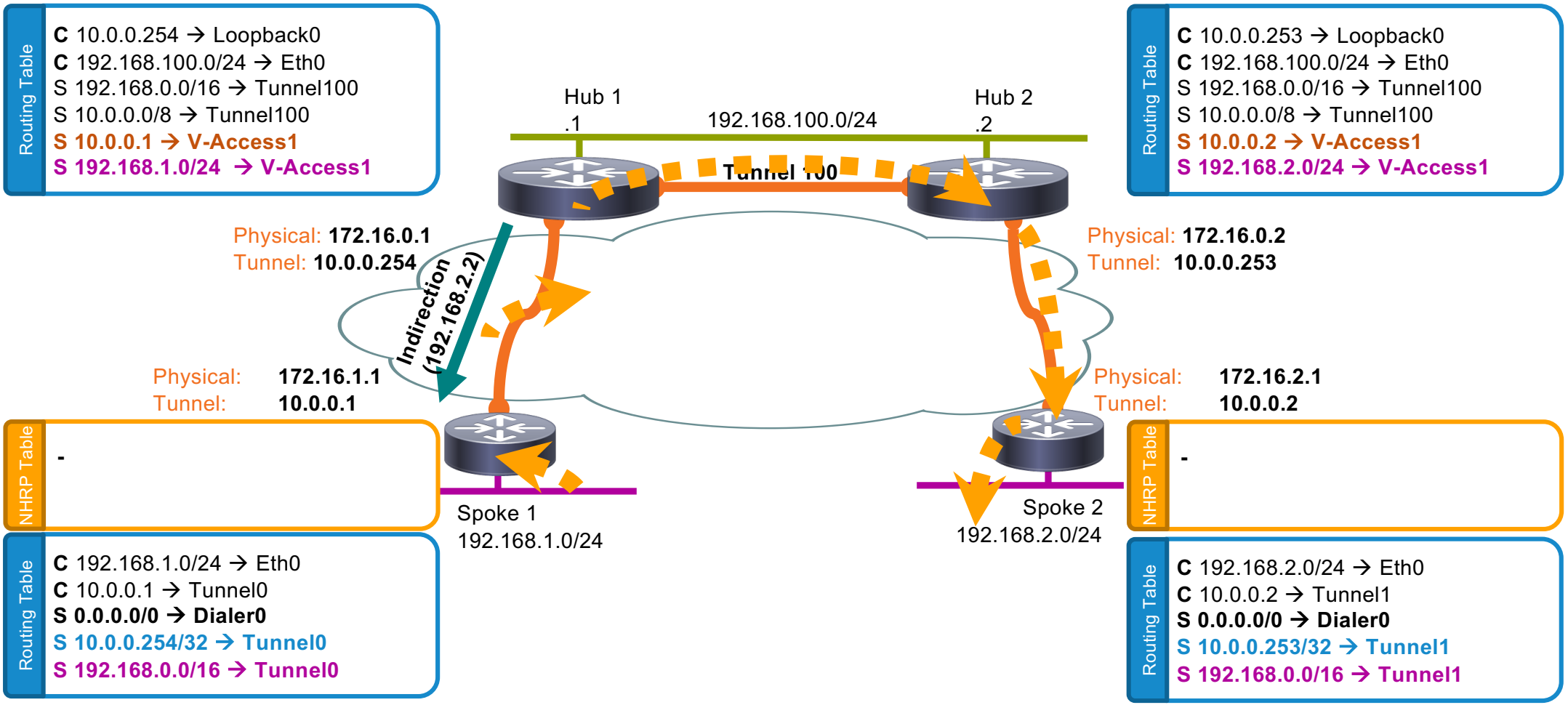
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Hub and Spoke – IKE Route Exchange



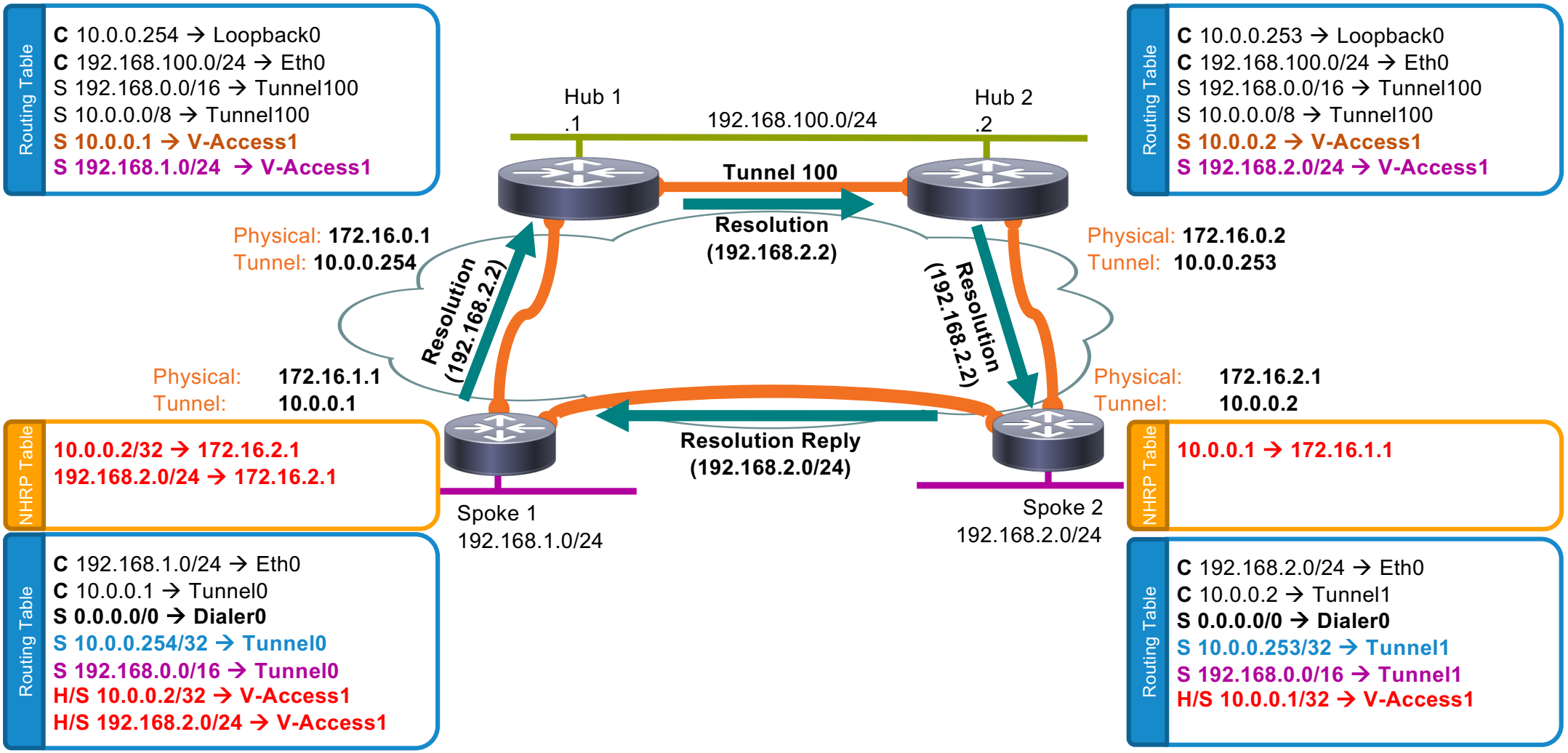
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Mesh – Indirection

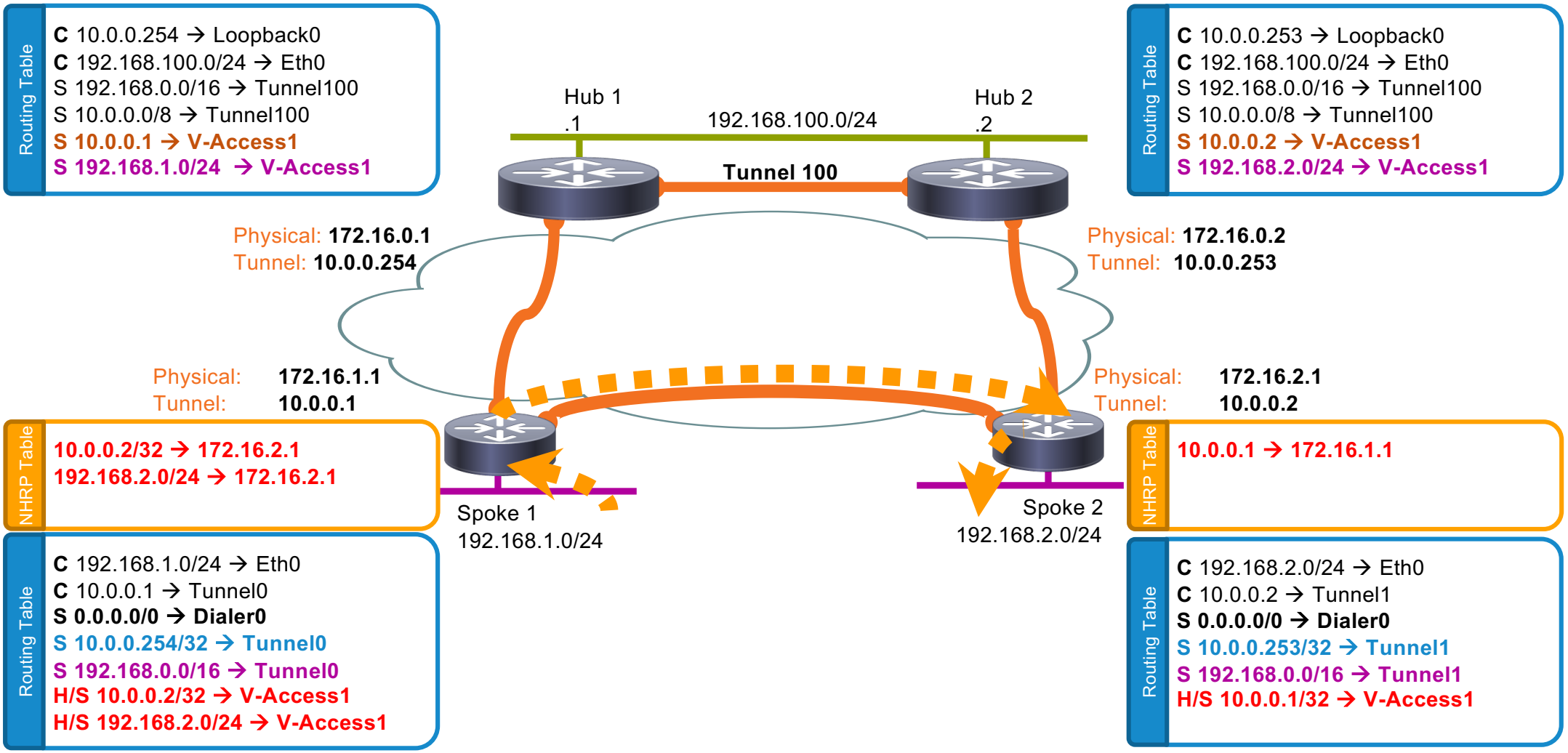


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Mesh – Resolution



FlexVPN Mesh – Shortcut Forwarding



FlexVPN Mesh (IKEv2 Routing)

Hub 1 Configuration

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub1.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
 !
crypto ikev2 authorization policy default
 route set remote 10.0.0.0 255.0.0.0
 route set remote 192.168.0.0 255.255.0.0
```

Accept connections from Spokes

Local spoke profile

These prefixes can also be set by RADIUS

Defines which prefixes should be protected

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 ip access-group AllowMyBGP in
 tunnel protection ipsec profile default
!
interface Loopback0
 ip address 10.0.0.254 255.255.255.255
!
interface Tunnel100
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source Ethernet0/1
 tunnel destination 192.168.100.2
```

Static per-spoke features applied here

All V-Access will be in the same network-id

Hub 1 dedicated overlay address

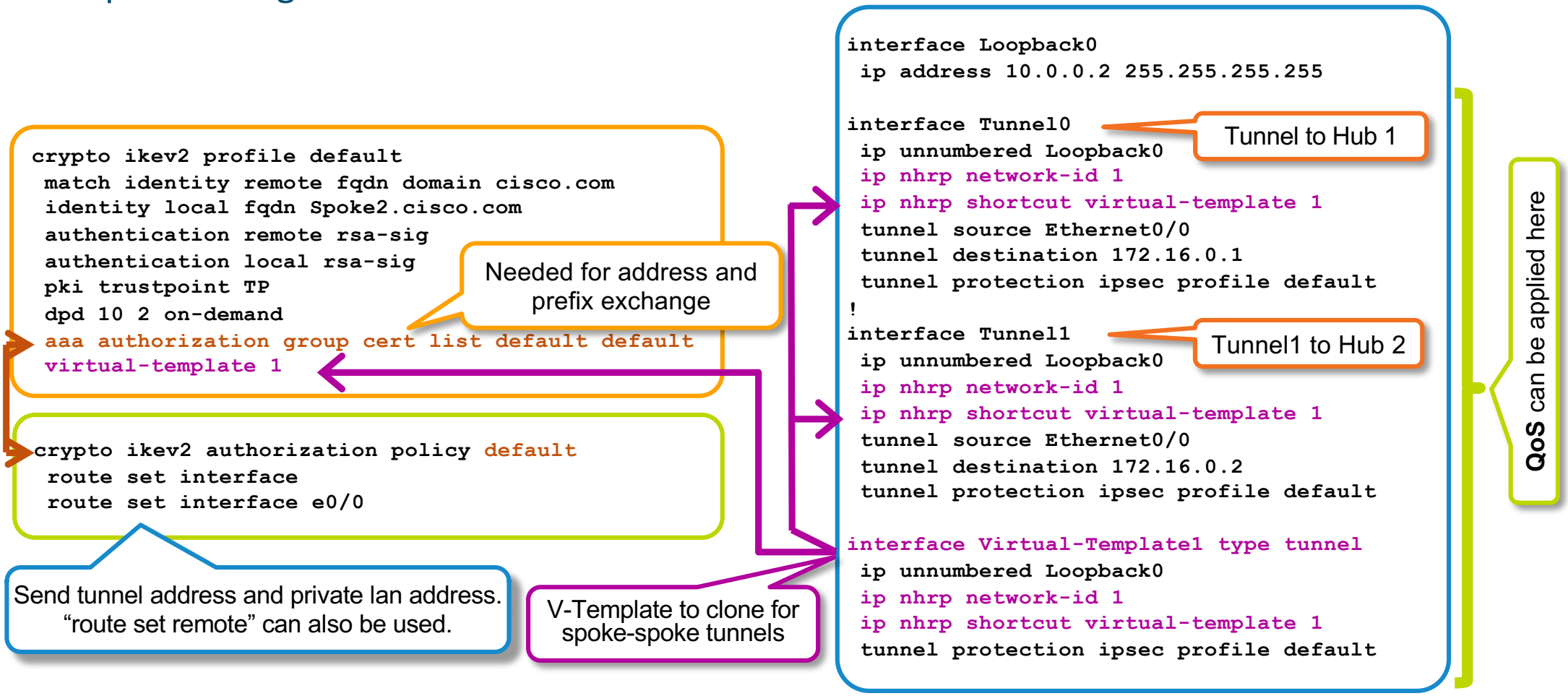
Inter-Hub link (not encrypted)

Same network-id on V-Access and inter-hub link

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Mesh (IKEv2 Routing)

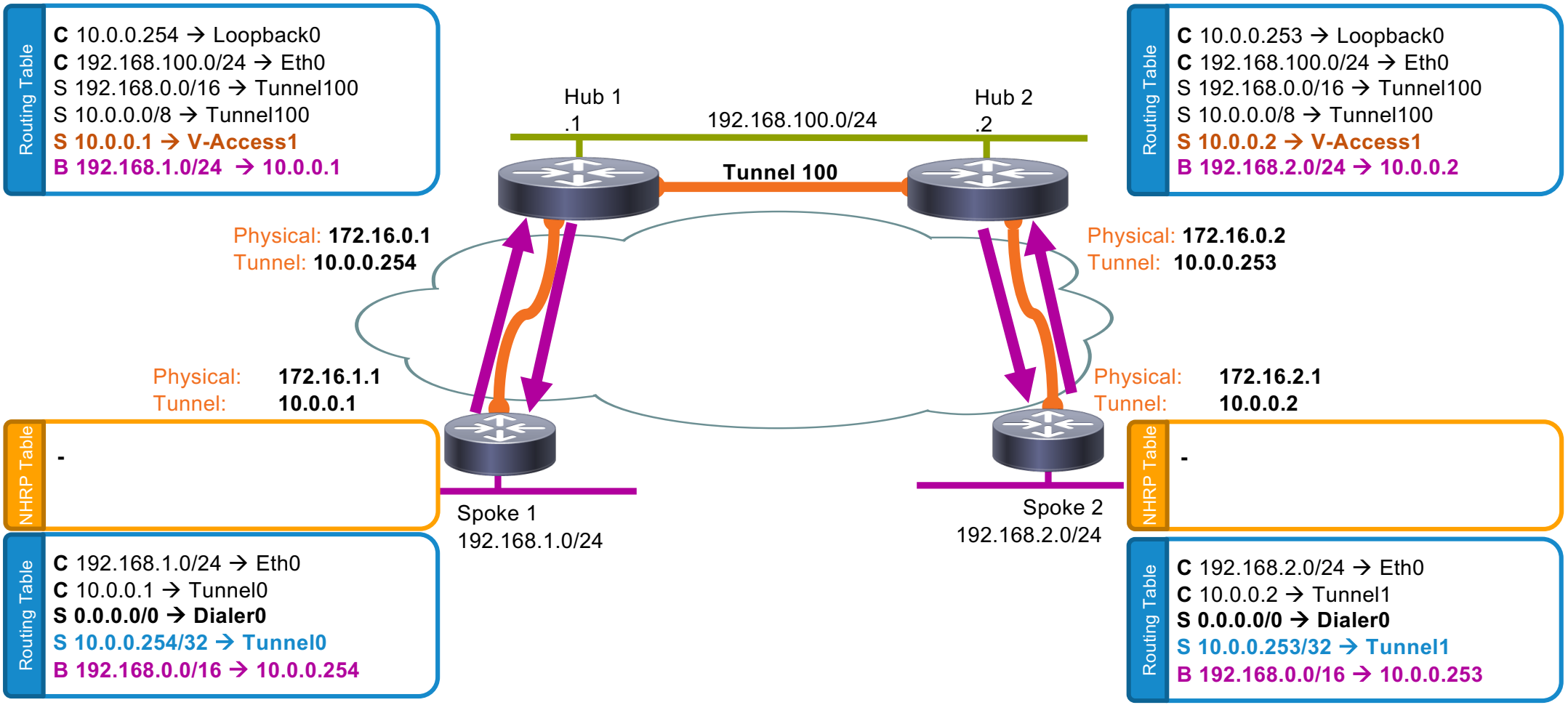
Spoke Configuration



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Shortcut Switching With a routing protocol (BGP)

FlexVPN Mesh with BGP Routing



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

BGP complex ? Not really…

Spoke Configuration

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 10.0.0.253 remote-as 1
 neighbor 10.0.0.254 remote-as 1

 address-family ipv4
  network 192.168.2.0
  neighbor 10.0.0.253 activate
  neighbor 10.0.0.254 activate
  maximum-paths ibgp 2
```

Spoke prefix to advertise

Any other routing protocol will do but mind the scalability and resiliency against packet losses.

All protocols were not created equal.

BGP shown in this presentation as a “no brainer”.

Hub Configuration

Summary prefixes to advertise to all spokes

```
ip route 10.0.0.0 255.0.0.0 Tunnel100 tag 2
ip route 192.168.0.0 255.255.0.0 Tunnel100 tag 2

router bgp 1
 bgp log-neighbor-changes
 bgp listen range 10.0.0.0/24 peer-group Flex

 address-family ipv4
  neighbor Flex peer-group
  neighbor Flex remote-as 1
  redistribute static route-map rm
 exit-address-family
!
route-map rm permit 10
 match tag 2
```

Dynamically accept spoke BGP peering!

route-map filters static routes to redistribute in BGP

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Routing IPv6 with IKEv2 or BGP

With IKEv2 routing

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub1.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 …
 virtual-template 1
 !
crypto ikev2 authorization policy default
 route set remote ipv6 2001::/64
 route set remote ipv6 2002::/64
```

Same as v4… just specify ipv6 ☺

With BGP

One peering, for both IPv4 and IPv6

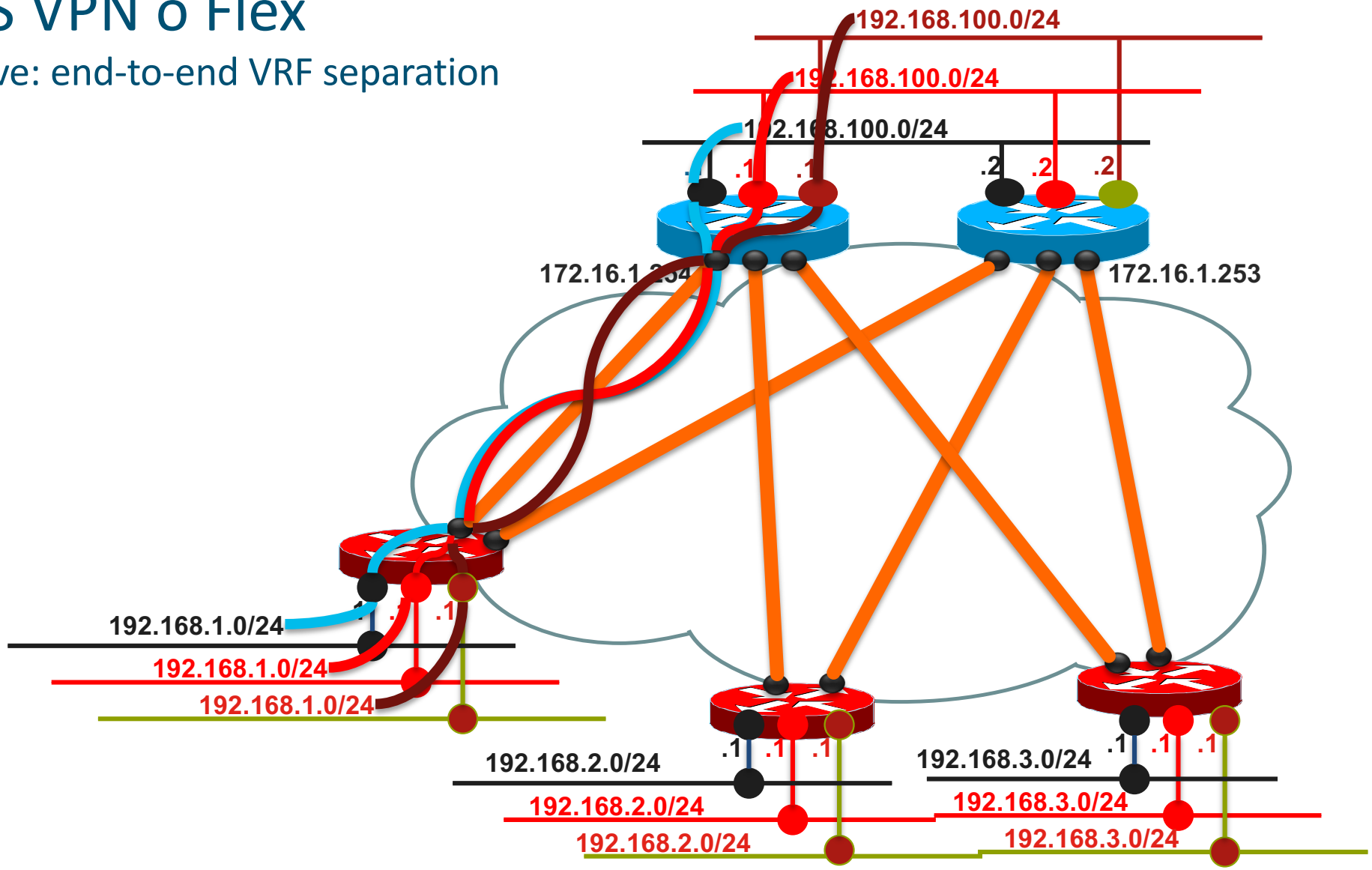
```
router bgp 1
 bgp log-neighbor-changes
 bgp listen range 10.0.0.0/16 peer-group Flex
 neighbor Flex peer-group
 neighbor Flex remote-as 1
 !
 address-family ipv4
  redistribute static route-map rm
  neighbor Flex activate
 exit-address-family
 !
 address-family ipv6
  redistribute static route-map rm
  neighbor Flex activate
 exit-address-family
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

MPLS over FlexVPN with Shortcut Switching

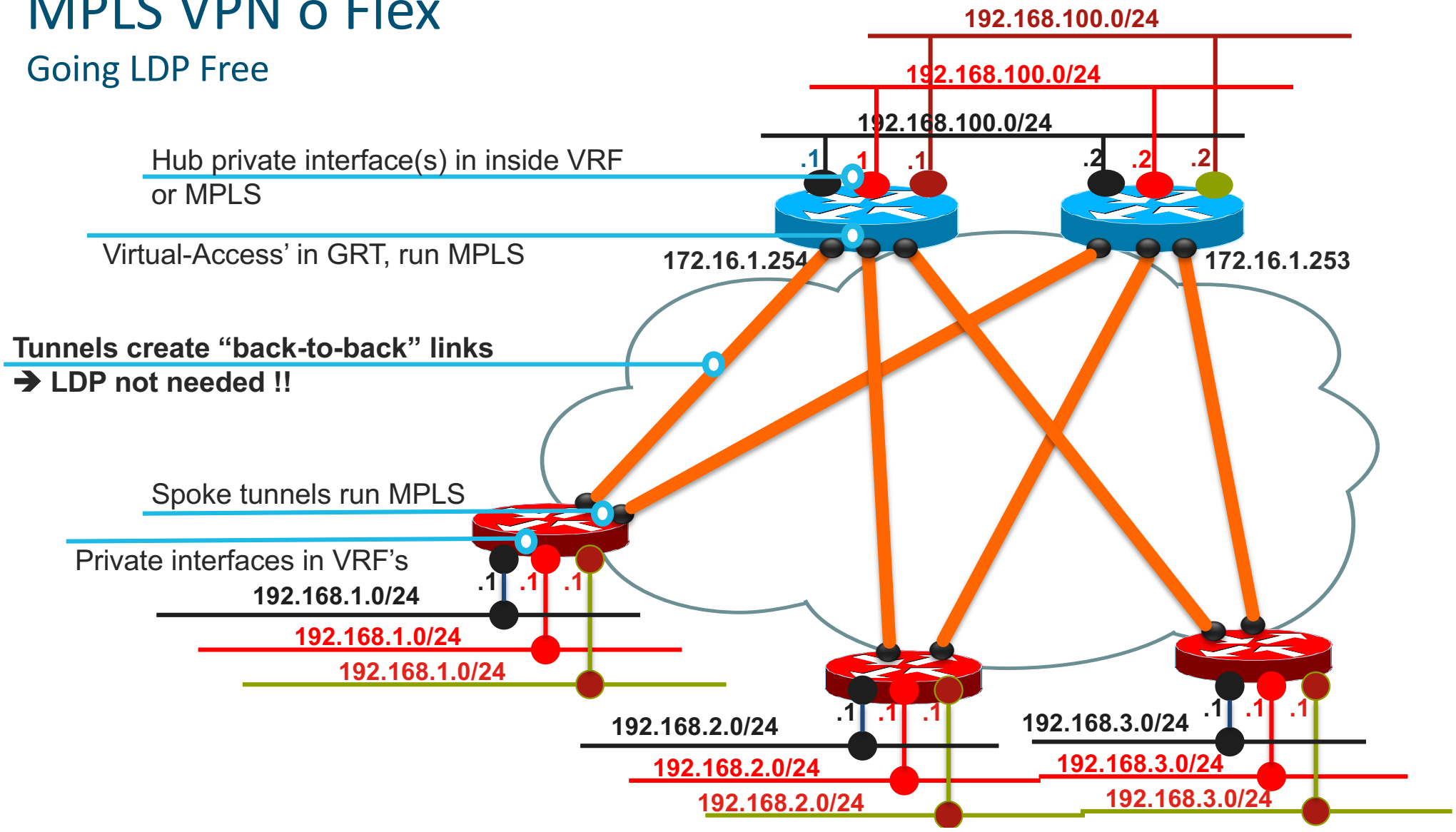
MPLS VPN o Flex

Objective: end-to-end VRF separation



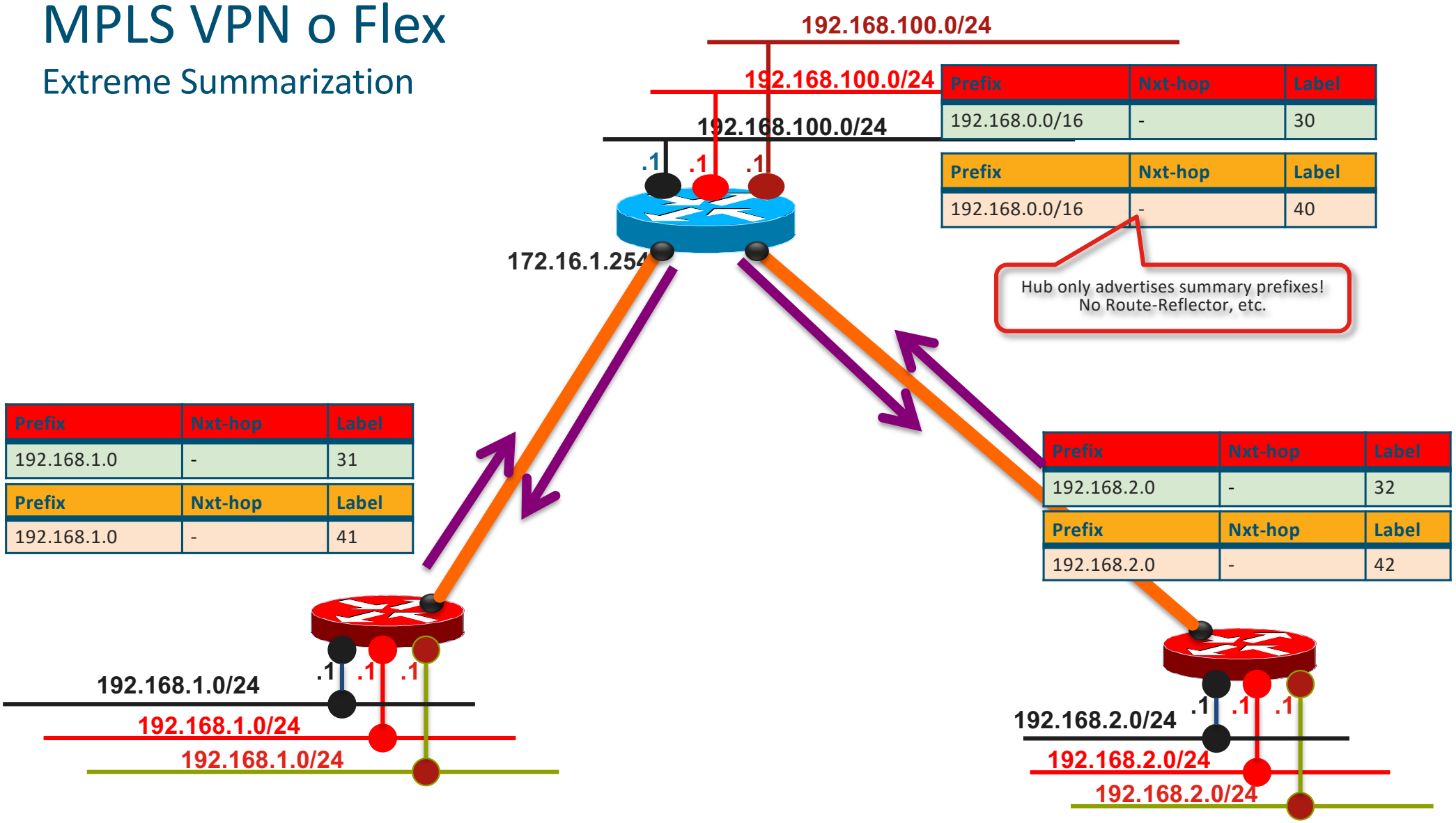
MPLS VPN o Flex

Going LDP Free



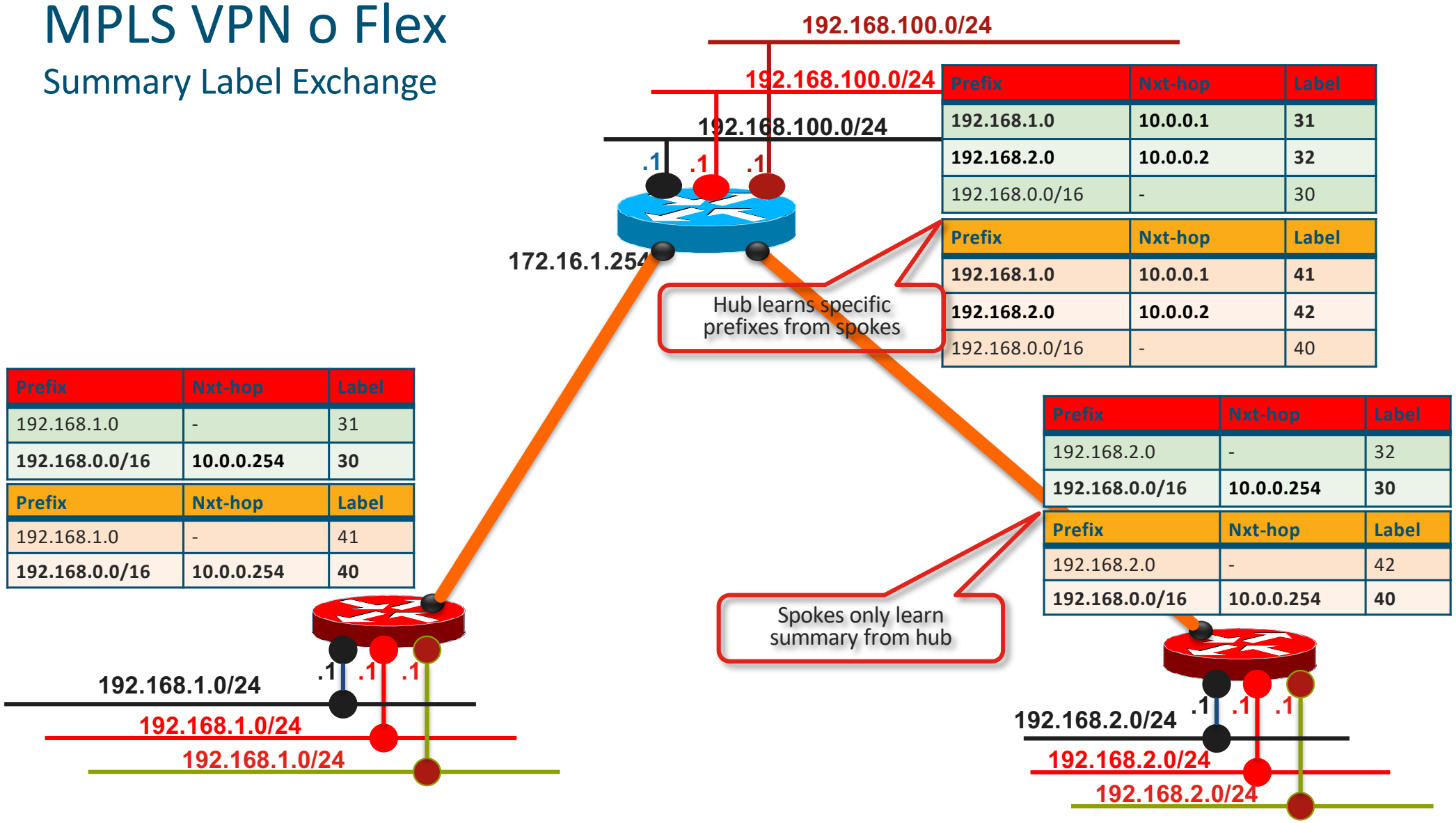
MPLS VPN o Flex

Extreme Summarization



MPLS VPN o Flex

Summary Label Exchange



Prefix	Nxt-hop	Label
192.168.1.0	10.0.0.1	31
192.168.2.0	10.0.0.2	32
192.168.0.0/16	-	30

Prefix	Nxt-hop	Label
192.168.1.0	10.0.0.1	41
192.168.2.0	10.0.0.2	42
192.168.0.0/16	-	40

Prefix	Nxt-hop	Label
192.168.1.0	-	31
192.168.0.0/16	10.0.0.254	30

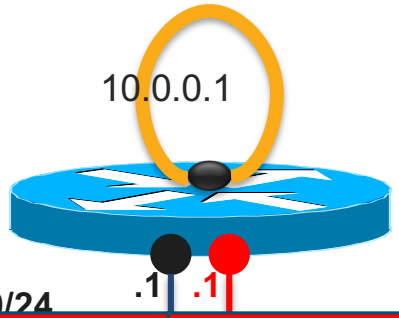
Prefix	Nxt-hop	Label
192.168.1.0	-	41
192.168.0.0/16	10.0.0.254	40

Prefix	Nxt-hop	Label
192.168.2.0	-	32
192.168.0.0/16	10.0.0.254	30

Prefix	Nxt-hop	Label
192.168.2.0	-	42
192.168.0.0/16	10.0.0.254	40

MPLS VPN o Flex

Hub & Spoke FIB's and LFIB's



192.168.1.0/24

VRF FIBs

Prefix	Adjacency
192.168.1.0/24	Glean (e0)
192.168.0.0/16	10.0.0.254 **30**

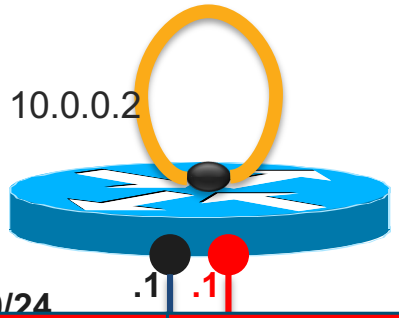
Prefix	Adjacency
192.168.1.0/24	Glean (e1)
192.168.0.0/16	10.0.0.254 **40**

FIB

Prefix	Adjacency
10.0.0.254	Tunnel0 (**Null**)
0.0.0.0/0	Dialer0

LFIB

Loc.	Out	I/F
31	POP	VRF RED
41	POP	VRF BLUE



192.168.2.0/24

VRF FIBs

Prefix	Adjacency
192.168.2.0/24	Glean (e0)
192.168.0.0/16	10.0.0.254 **30**

Prefix	Adjacency
192.168.2.0/24	Glean (e1)
192.168.0.0/16	10.0.0.254 **40**

FIB

Prefix	Adjacency
10.0.0.254	Tunnel0 (**Null**)
0.0.0.0/0	Dialer0

LFIB

Loc.	Out	I/F
32	POP	VRF RED
42	POP	VRF BLUE

192.168.100.0/24

VRF FIBs

Prefix	Adjacency
192.168.1.0/24	10.0.0.1 **31**
192.168.2.0/24	10.0.0.2 **32**

Prefix	Adjacency
192.168.1.0/24	10.0.0.1 **41**
192.168.2.0/24	10.0.0.2 **42**

FIB

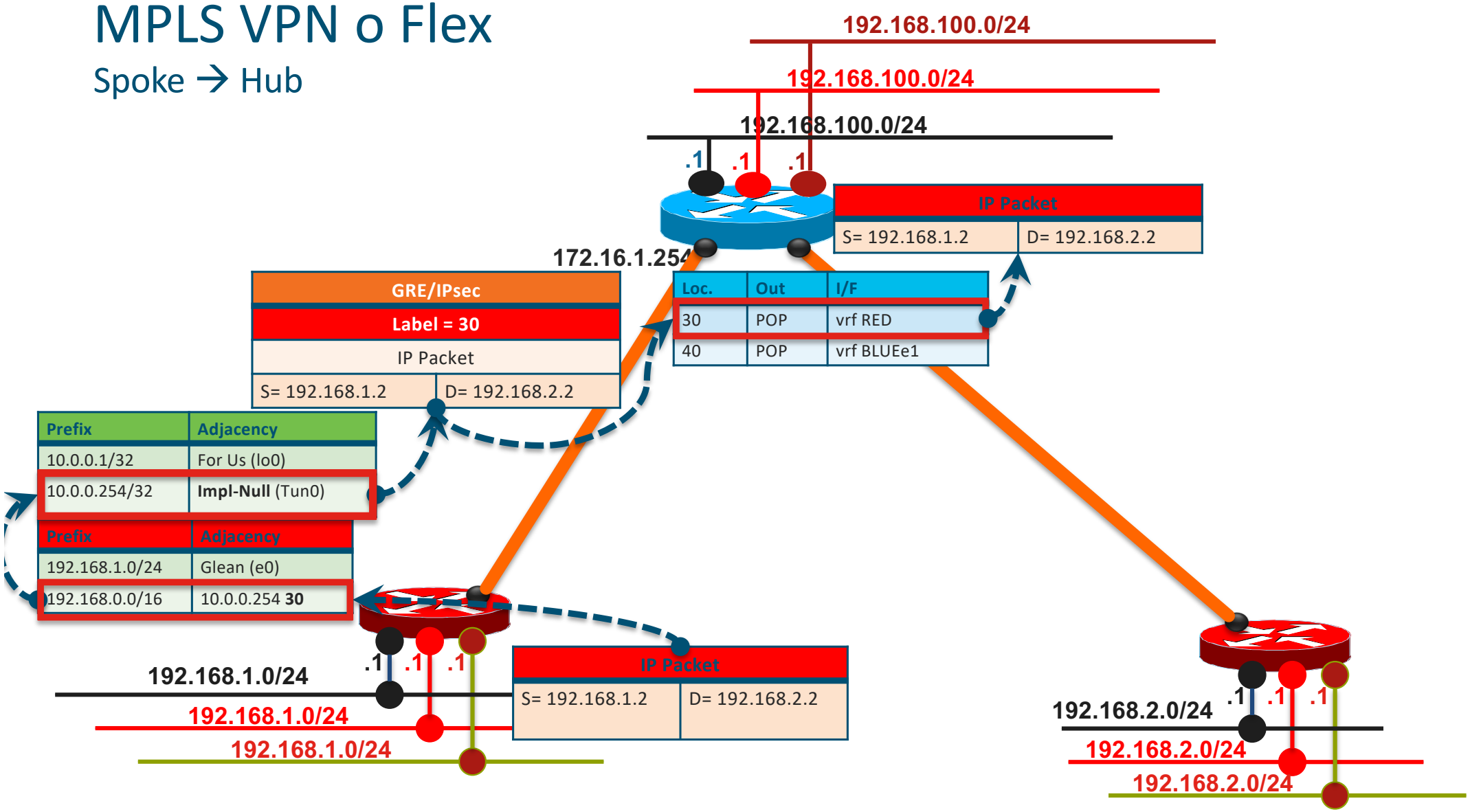
Prefix	Adjacency
10.0.0.1	VA-1 (**Null**)
10.0.0.2	VA-2 (**Null**)
0.0.0.0	Dialer0

LFIB

Loc.	Out	I/F
30	POP	VRF RED
40	POP	VRF BLUE

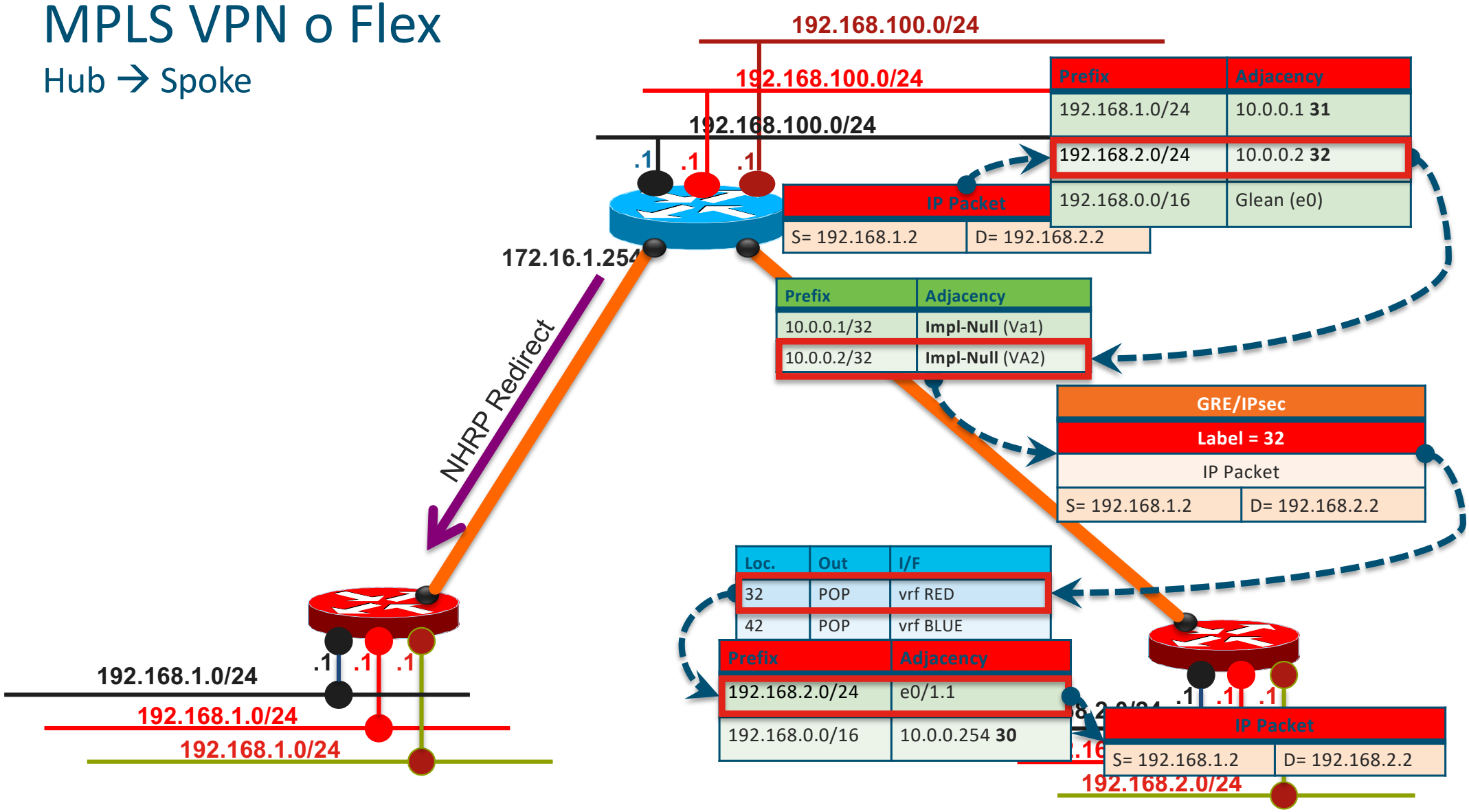
MPLS VPN o Flex

Spoke → Hub



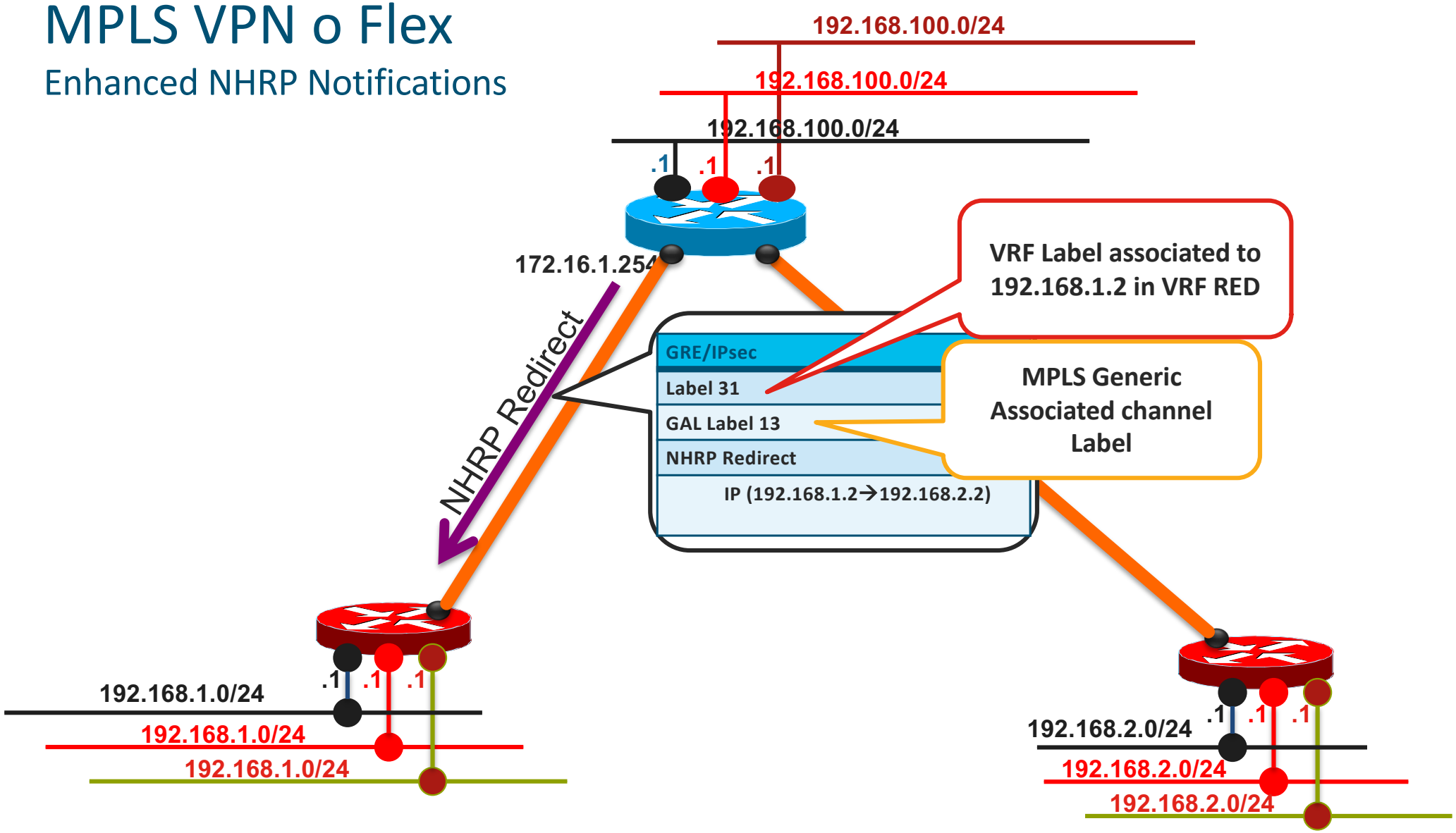
MPLS VPN o Flex

Hub → Spoke



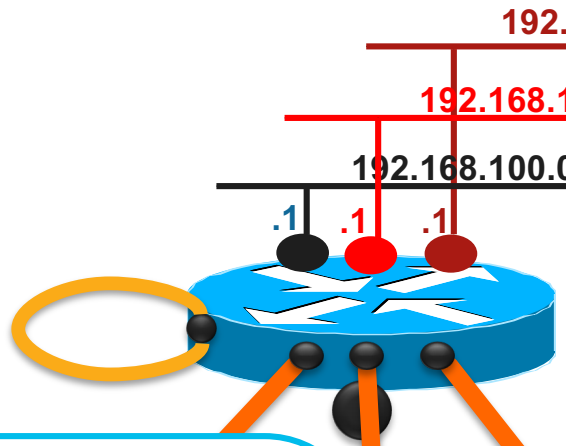
MPLS VPN o Flex

Enhanced NHRP Notifications



Hub Routing

BGP and Interfaces




```
ip route 0.0.0.0 0.0.0.0 172.16.1.2
ip route vrf Blue 192.168.0.0 255.255.0.0 Null0
ip route vrf Red 192.168.0.0 255.255.0.0 Null0

router bgp 1
 bgp log-neighbor-changes
 bgp listen range 10.0.0.0/16 peer-group Flex
 neighbor Flex peer-group
 neighbor Flex remote-as 1
 neighbor Flex timers 5 15

 address-family vpnv4
  neighbor Flex activate
  neighbor Flex send-community extended

 address-family ipv4 vrf Blue
  network 192.168.0.0 mask 255.255.0.0

 address-family ipv4 vrf Red
  network 192.168.0.0 mask 255.255.0.0
```

Activate VPNv4

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 mpls nhrp
 tunnel protection ipsec profile default
```

Activate NHRP redirects and give NHRP control over MPLS

```
interface Ethernet0/0
 ip address 172.16.1.254 255.255.255.0
```

WAN Interface can be in Front VRF

```
interface Loopback0
 ip address 10.0.0.254 255.255.255.255
```

Tunnels and Loopback in Global Routing Table

Advertise each VRF

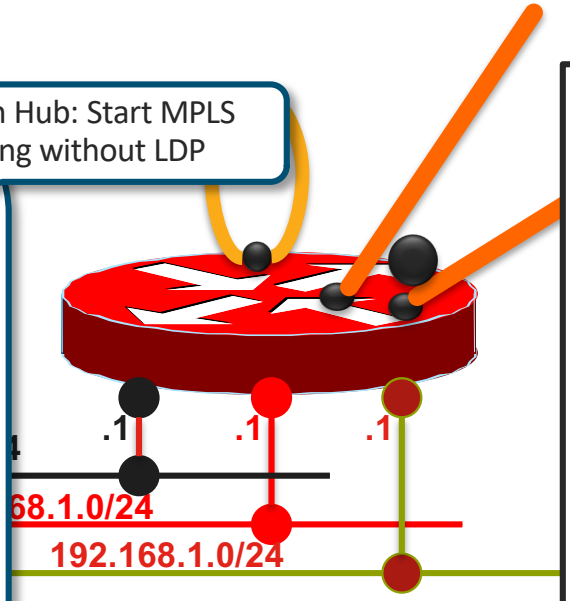
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Spoke Routing Configuration

BGP and Static Routes

```
interface Tunnel0
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 mpls nhrp
 tunnel source Ethernet0/0
 tunnel destination 172.16.1.254
 tunnel protection ipsec profile default

interface Tunnel1
 (same as Tunnel0 – points to hub 2)

interface Virtual-Template 1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 mpls nhrp
 tunnel protection ipsec profile default

interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.0

interface Loopback0
 ip address 10.0.0.2 255.255.255.255
```

Same as on Hub: Start MPLS forwarding without LDP




```
ip route 0.0.0.0 0.0.0.0 172.16.2.2

router bgp 1
 bgp log-neighbor-changes
 neighbor Flex peer-group
 neighbor Flex remote-as 1
 neighbor Flex timers 5 15
 neighbor 10.0.0.253 peer-group Flex
 neighbor 10.0.0.254 peer-group Flex

 address-family vpnv4
  neighbor Flex send-community extended
  neighbor 10.0.0.253 activate
  neighbor 10.0.0.254 activate

 address-family ipv4 vrf Blue
  redistribute connected
  maximum-paths ibgp 2

 address-family ipv4 vrf Red
  redistribute connected
  maximum-paths ibgp 2
```

Activate VPNv4

Advertise each VRF

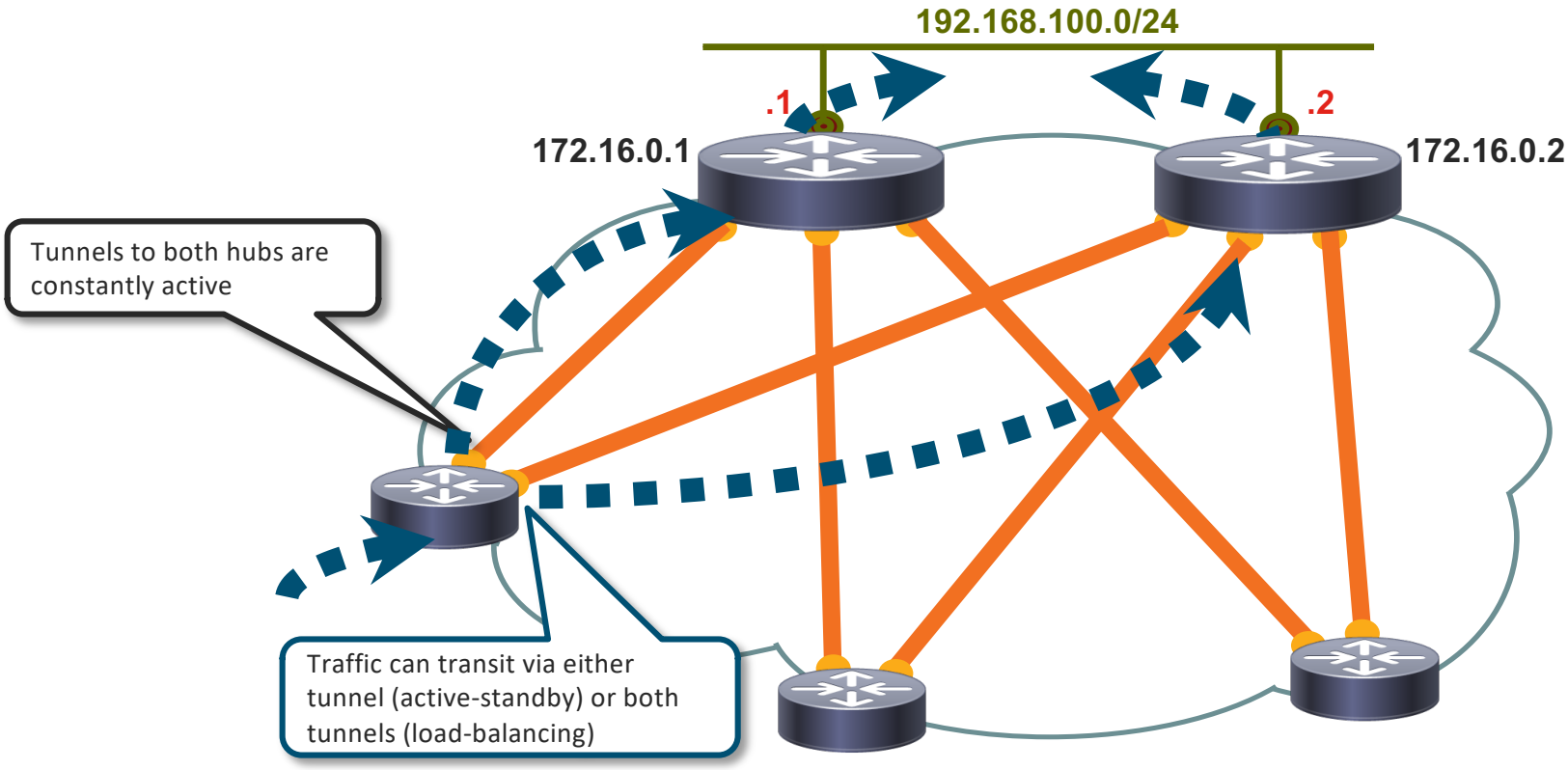
WAN Interface can be in Front VRF

Tunnels and Loopback in Global Routing Table

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

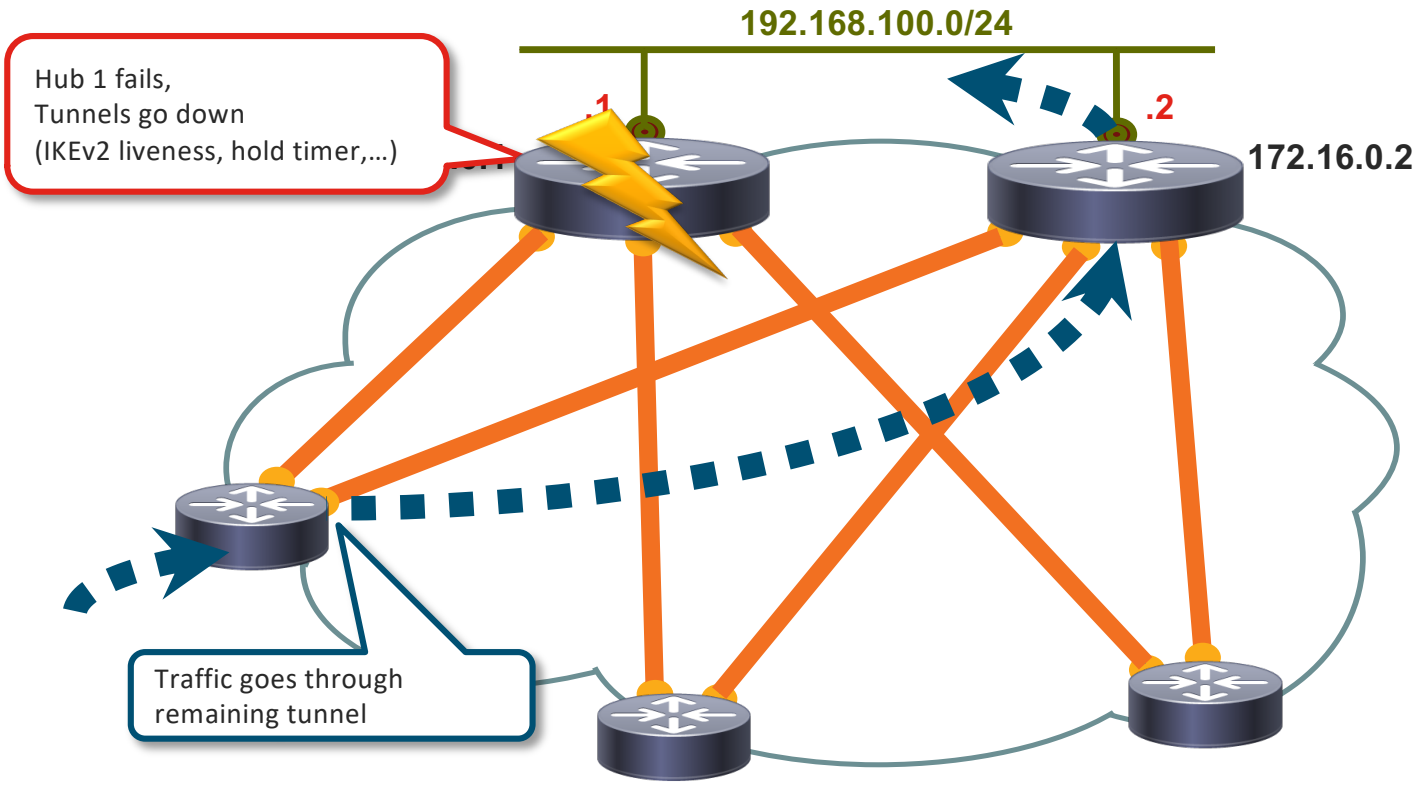
Routing Based Resiliency

FlexVPN Backup
Routing Based Multi-Hub Resiliency (1)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

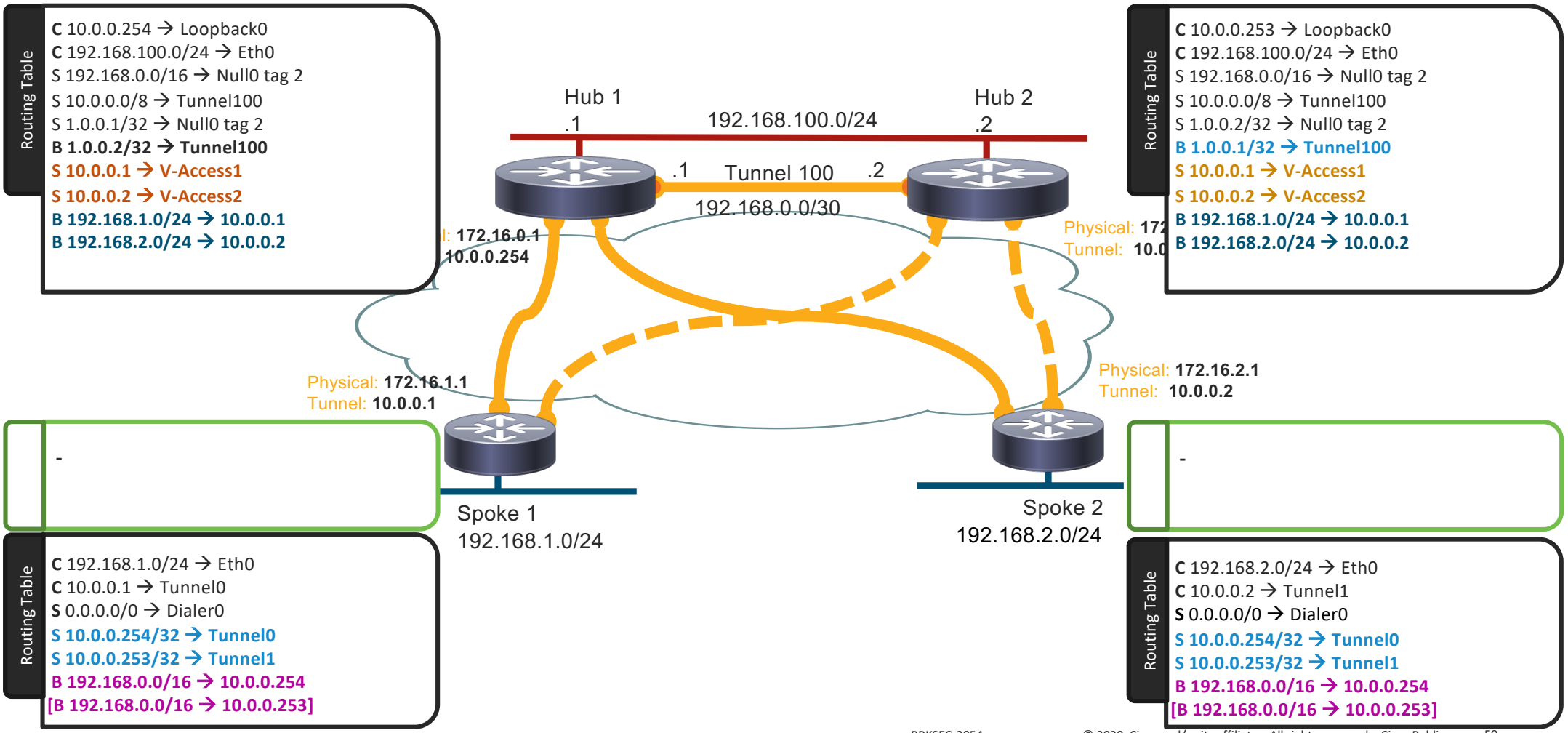
FlexVPN Backup
Routing Based Multi-Hub Resiliency (2)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Routing Based Resiliency
Faster Convergency

A simple setup…



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Method #1: Faster Hello's

Hub Configuration

```
router bgp 1
 bgp log-neighbor-changes
 bgp listen range 10.0.0.0/8 peer-group SPOKES
 neighbor SPOKES peer-group
 neighbor SPOKES remote-as 1
 neighbor SPOKES timers 1 3
 address-family ipv4
  neighbor SPOKES activate
```

Spoke Configuration

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 10.0.0.254 remote-as 1
 neighbor 10.0.0.254 timers 1 3
 neighbor 10.0.0.253 remote-as 1
 neighbor 10.0.0.253 timers 1 3
```

BGP can go as fast as 1 second hello's with a 3 seconds Hold Timer ➔ Failover in 3 seconds

Monitor IOS CPU level – expect about 10% CPU background load at 500 spokes (RP2)

Convergence (massive reconnect) may be affected by process starvation. Test –test –test –test.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Method #2: BFD between hub and spokes

Hub Configuration

```
bfd map ipv4  10.0.0.0/8  10.0.0.0/8 mh1
bfd-template multi-hop mh1
 interval min-tx 200 min-rx 200 multiplier 3

router bgp 1
 bgp log-neighbor-changes
 bgp listen range 10.0.0.0/8 peer-group SPOKES
 neighbor SPOKES peer-group
 neighbor SPOKES remote-as 1
 neighbor SPOKES ebgp-multihop 2
 neighbor SPOKES fall-over bfd multi-hop
 address-family ipv4
 neighbor SPOKES activate
```

Spoke Configuration

```
bfd map ipv4  10.0.0.0/8  10.0.0.0/8 mh1
bfd-template multi-hop mh1
 interval min-tx 200 min-rx 200 multiplier 3

router bgp 1
 bgp log-neighbor-changes
 neighbor 10.0.0.254 remote-as 1
 neighbor 10.0.0.254 fall-over bfd multi-hop
 neighbor 10.0.0.253 remote-as 1
 neighbor 10.0.0.253 fall-over bfd multi-hop
```

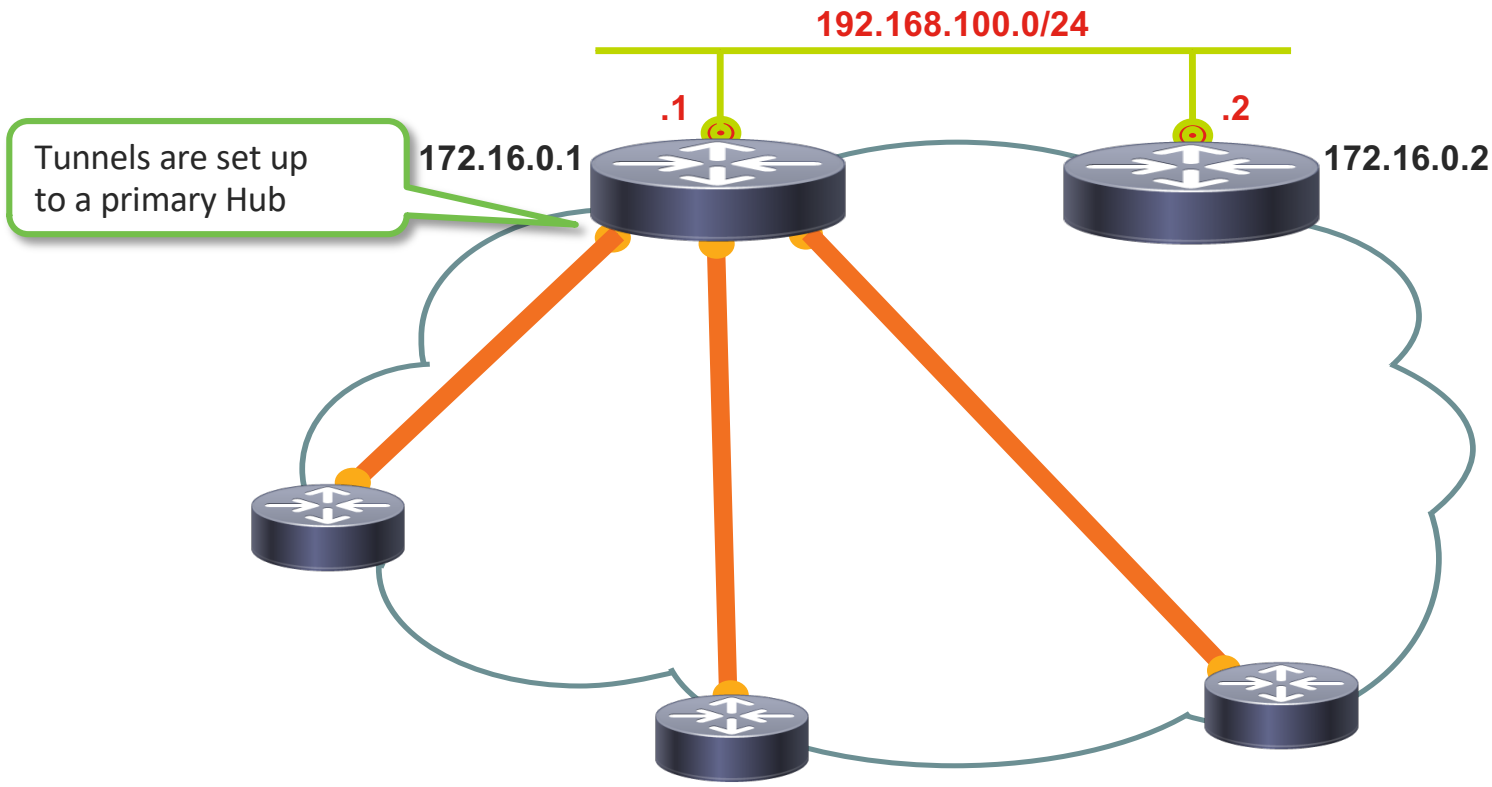
On ASR1K, ESP CPU will offload BFD; IOS unaffected
problem moved, not fully solved

Microbursts can cause false positives; very hard to monitor

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

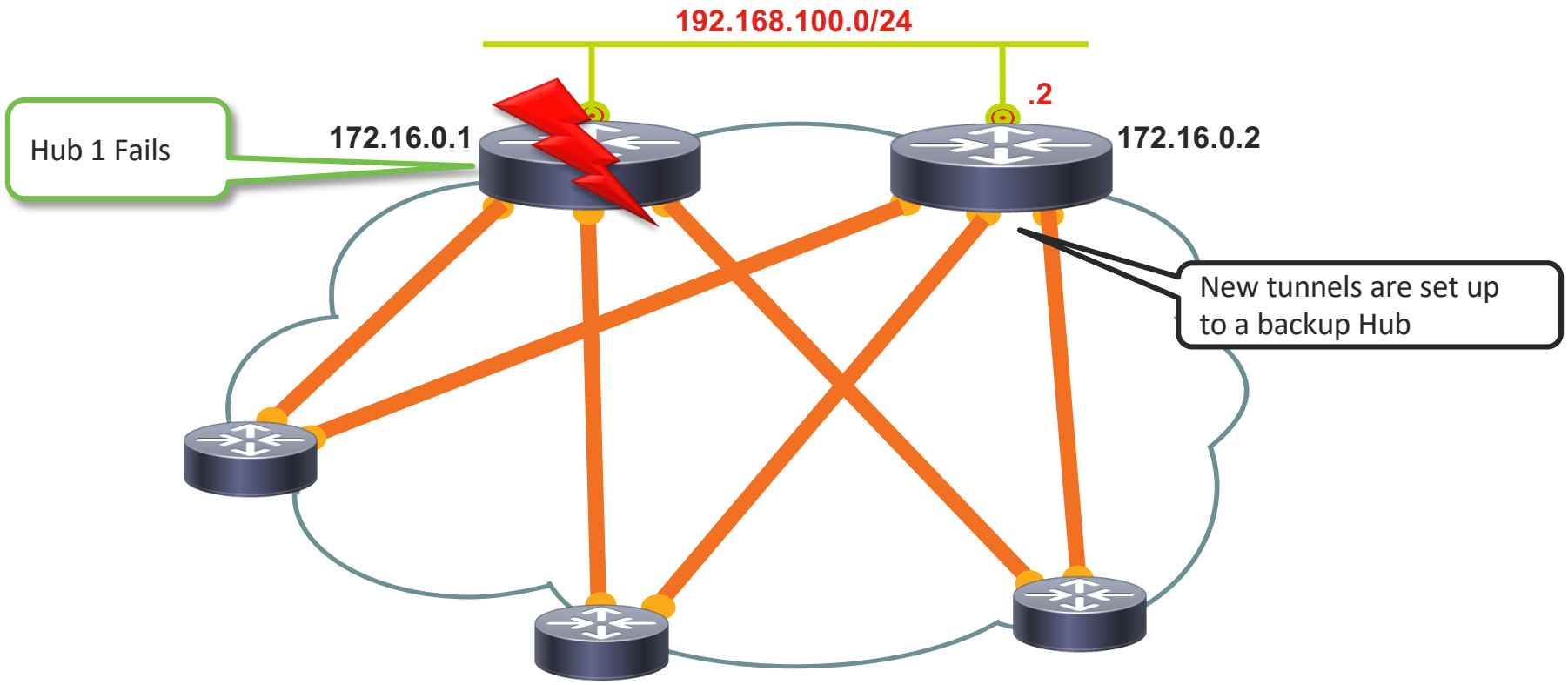
FlexVPN Backup Mechanisms

FlexVPN Backup Peers (1)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Backup Peers (2)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Backup Peers (3) – Spoke Config.


```
aaa authorization network default local

crypto ikev2 profile default
 match certificate HUBMAP
 identity local fqdn Spoke1.cisco.com
 authentication remote rsa-sig
 authentication local pre-shared
 keyring local
 pki trustpoint CA
 aaa authorization group cert list default default
 dpd 30 2 on-demand

crypto ikev2 client flexvpn default
 client connect tunnel 0
 peer 1 172.16.1.254
 peer 2 172.16.1.253

interface Tunnel0
 ip address negotiated
 tunnel source FastEthernet0/0
 tunnel destination dynamic
 tunnel protection ipsec profile default
```

Detect Hub Failure

To Primary Hub

To Secondary Hub

Destination managed by FlexVPN

Powerful Peer Syntax

```
peer reactivate
peer <n> <ip>
peer <n> <ip> track <x>
peer <n> <fqdn> [dynamic [ipv6]]
peer <n> <fqdn> [dynamic …] track <x>
```

Switch back

N^{th} source selected only if corresponding track object is up

RADIUS Backup List Attribute

`ipsec:ipsec-backup-gateway`

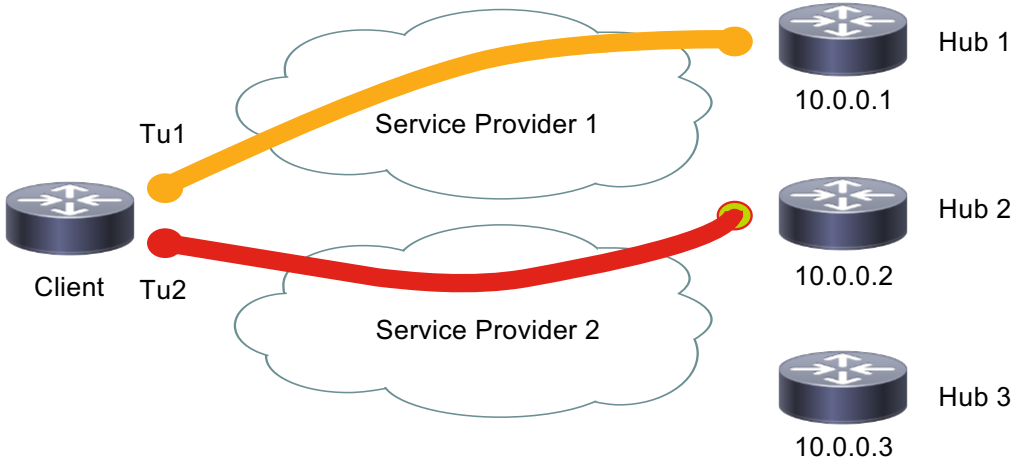
Up to 10 backup gateways pushed by config-exchange

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 99
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Backup Groups

Warrant that a peer, belonging to different peer-lists in the same backup gro



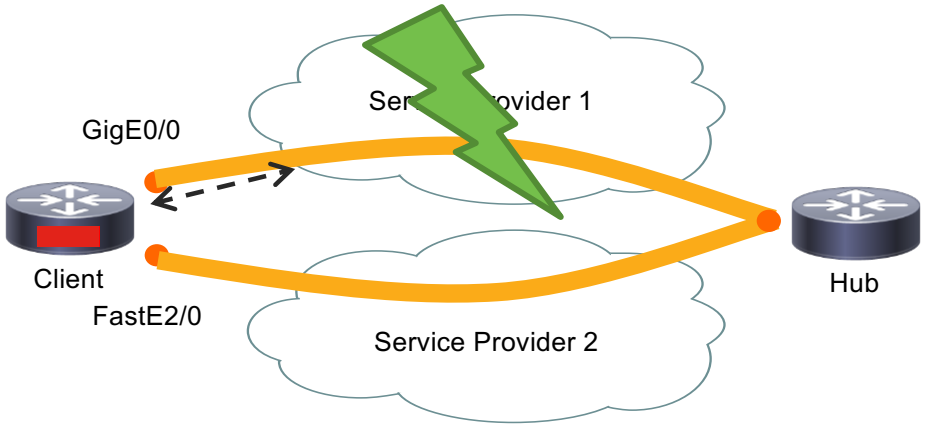

```
crypto ikev2 flexvpn client remote1
 peer 1 10.0.0.1
 peer 2 10.0.0.2
 peer 3 10.0.0.3
 backup group 1
 client connect Tunnel1
crypto ikev2 flexvpn client remote2
 peer 1 10.0.0.1
 peer 2 10.0.0.2
 peer 3 10.0.0.3
 backup group 1
 client connect Tunnel2
!
interface Tunnel1
 ip address negotiated
 …
 tunnel destination dynamic
 …
interface Tunnel2
 ip address negotiated
 …
 tunnel destination dynamic
 …
```

10.0.0.1 cannot be used as already active in remote1 peer-list from same group

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Tunnel Pivot

- Use when different Service Providers are used to connect to remote host

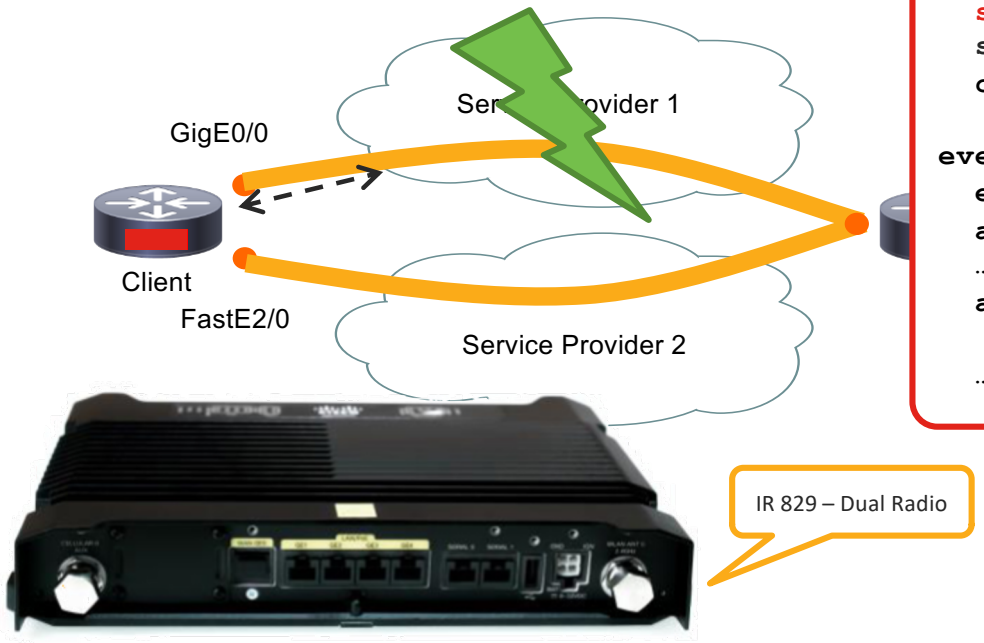



```
track 1 ip sla 1 reachability

crypto ikev2 flexvpn client remote1
  peer 10.0.0.1
  source 1 interface GigabitEthernet0/0 track 1
  source 2 interface FastEthernet2/0
  client connect tunnel 0

interface Tunnel0
   ip address negotiated
   …
   tunnel source dynamic
   tunnel destination dynamic
   …
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Associating Tunnel Pivot to RSSI of LTE ?

- Use Cellular which currently has better RSSI




```
track 1 ip sla 1 reachability

crypto ikev2 flexvpn client remote1
  peer 10.0.0.1
  source 1 Cellular0/0 track 106
  source 2 Cellular1/0 track 105
  client connect tunnel 0

event manager applet watch-signal
  event timer watchdog time 60 maxrun 120
  action 020 cli command "show cellular 0/0 all| inc Current RSSI"
  …
  action 100 if LTE1 gt "$LTE2" ! Prefer Cellular0/0
   action 110  track set 106 state up
  …
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Associating track to … RSSI of LTE - EEM

```
event manager environment rssiTolerance -3
event manager environment rssiRange 10
event manager applet watch-signal authorization bypass
 event timer watchdog time 60 maxrun 120
 action 010 cli command "enable"
 action 020 cli command "show cellular 0/0 all | inc Current RSSI"
 action 030 set LTE1 "$_cli_result"
 action 040 regexp "Current RSSI\(RSCP\) = (-[0-9]+) dBm" "$_cli_result" match LTE1
 action 041 regexp "Current RSSI = (-[0-9]+) dBm" "$_cli_result" match LTE1
 action 050 puts "Cellular0/0 RSSI = $LTE1"
 action 060 cli command "show cellular 1/0 all | inc Current RSSI"
 action 070 set LTE2 "$_cli_result"
 action 080 regexp "Current RSSI\(RSCP\) = (-[0-9]+) dBm" "$_cli_result" match LTE2
 action 081 regexp "Current RSSI = (-[0-9]+) dBm" "$_cli_result" match LTE2
 action 089 puts "Cellular1/0 RSSI = $LTE2"
 action 090 if $LTE1 eq "-0"
 action 091  set LTE1 "-999"
 action 092  syslog msg "Cellular0/0 is down, setting RSSI to -999"
 action 093 end
 action 094 if $LTE2 eq "-0"
 action 095  set LTE2 "-999"
 action 096  syslog msg "Cellular1/0 is down, setting RSSI to -999"
 action 097 end
 action 098 add $LTE1 $rssiRange
 action 099 set adjLTE1 "$_result"
 action 105 if $adjLTE1 gt "$LTE2"
 action 106  divide $LTE2 $adjLTE1
 action 107  set differenceLTE1 "$_remainder"
 action 108  if $rssiTolerance gt "$differenceLTE1"
 action 109   track set 100 state up
 action 110   syslog msg "Cellular0/0 is preferred because of bigger difference ($differenceLTE1) than configured tolerance ($rssiTolerance)"
 action 111  else
 action 112   syslog msg "No change, because RSSI difference ($differenceLTE1) is smaller than configured tolerance ($rssiTolerance)"
 action 113  end
 action 120 else
 action 121  divide $adjLTE1 $LTE2
 action 122  set differenceLTE2 "$_remainder"
 action 123  if $rssiTolerance gt "$differenceLTE2"
 action 130   track set 100 state down
 action 131   syslog msg "Cellular1/0 is preferred because of bigger difference ($differenceLTE2) than configured tolerance ($rssiTolerance)"
 action 132  else
 action 133   syslog msg "No change, because RSSI difference ($differenceLTE2) is smaller than configured tolerance ($rssiTolerance)"
 action 134  end
 action 135 end
!
end
```

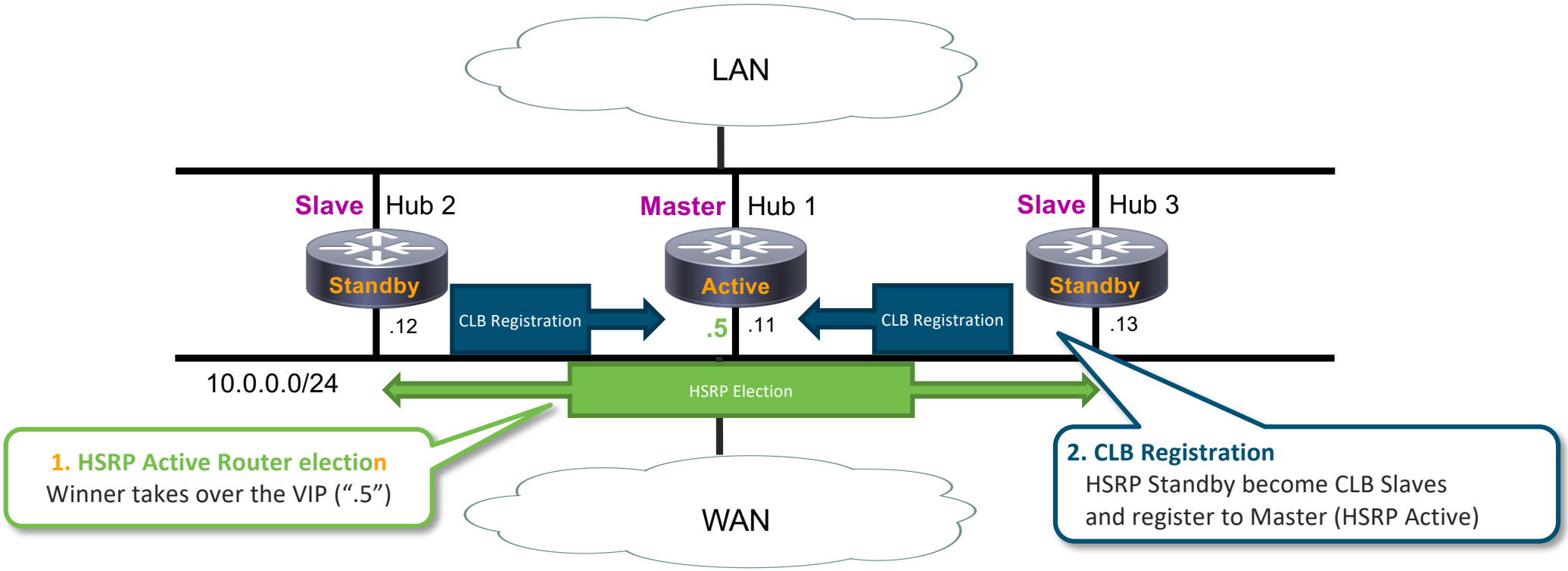

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Load Balancer

FlexVPN Backup
IKEv2 Load Balancer

- Redirects inbound IKEv2 negotiation to Least Loaded Gateway (LLG)
- Implements **RFC 5685**
- Redirect is performed during IKEv2 SA_INIT, IKE_AUTH
- Rely on **HSRP** for device failure detection and master selection
- Rely on **Cisco Load Balancing (CLB)** protocol (TCP/2012) to report load to cluster master
- Available since 15.2(4)M
- Cluster Auto-reconnect: Tight integration with Anyconnect
  - Allows reconnect to occur on any hub [without any stateful replication]

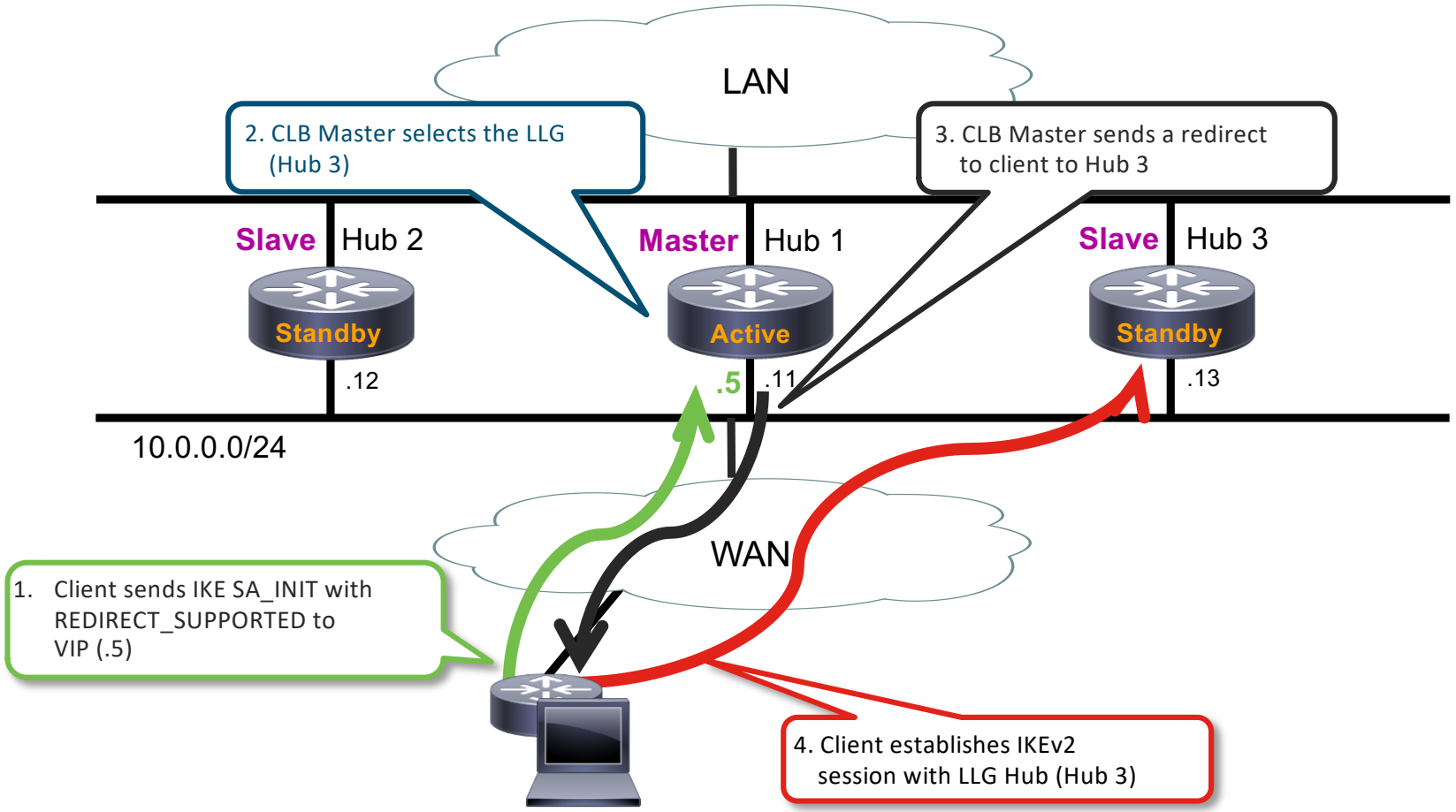
FlexVPN Load-Balancer Bootstrap




```
On Hub 1:
*Nov 20 12:43:58.488: %CLB-6-CLB_SLAVE_CONNECTED: Slave 10.0.0.13 connected.
*Nov 20 12:43:58.493: %CLB-6-CLB_SLAVE_CONNECTED: Slave 10.0.0.12 connected.
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Load-Balancer Client Connection



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Load-Balancer – Hub 1 Configuration

For Your Reference

```
crypto ikev2 redirect gateway init
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub1.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 cluster
 standby-group vpngw
 slave max-session 10
 no shutdown
```

Activates the sending of IKEv2 redirects during SA_INIT

```
!
interface Ethernet0/0
 ip address 10.0.0.11 255.
 standby 1 ip 10.0.0.5
 standby 1 name vpngw
!
interface Loopback0
 ip address 172.16.1.11 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip mtu 1400
tunnel source Ethernet1/0
tunnel protection ipsec profile default
```

HSRP Group Name must match IKEv2 Cluster configuration

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Load-Balancer – Client Configuration

For Your Reference

```
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 redirect client max-redirects 10
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Spoke2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ikev2 client flexvpn VPN_LB
 peer 1 10.0.0.5
 client connect Tunnel0
```

Activates IKEv2 redirection support and limit redirect count (DoS prevention)

```
interface Tunnel0
  ip address 172.16.1.100 255.255.255.0
  ip mtu 1400
  tunnel source Ethernet0/0
  tunnel destination dynamic
  tunnel protection ipsec profile default
```

FlexVPN Peer configured with the VIP address **only**

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Spokes Zero Touch Provisioning

ZTD – SUDI enhancement

```
crypto pki server CA
   grant auto
```

Insecure!!!

```
crypto pki server CA
   grant manual
```

Administrative burden
Need to confirm manually

```
crypto pki server CA
   grant auto trustpoint TP
```

Automatically grant requests signed by another CA

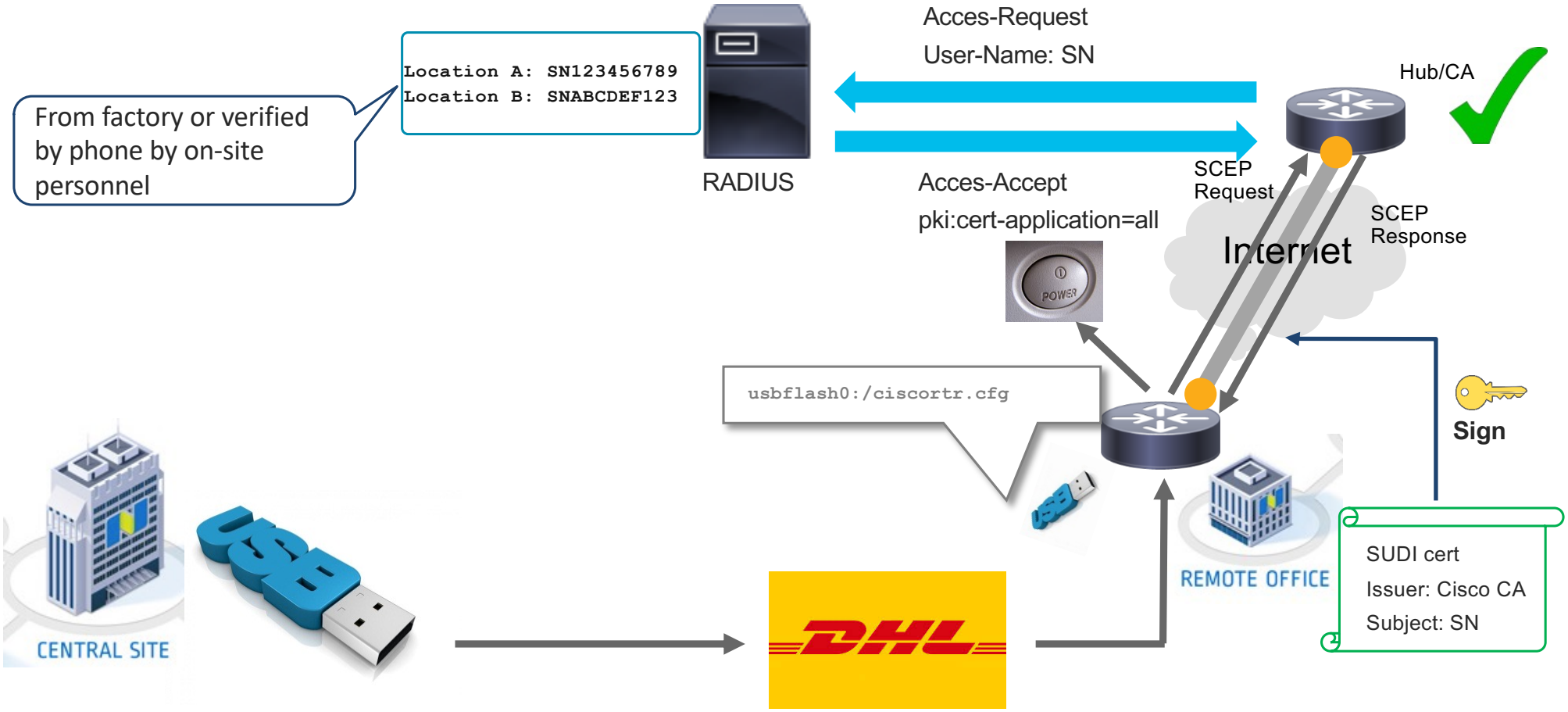
SUDI certificate (Secure Unique Device Identification)

- Factory built-in certificate signed by Cisco CA
- Stored in secure ACT2 chip or in software (hardware dependent)
- Contains Serial Number information

```
Certificate
  Status: Available
  Certificate Serial Number (hex): 0086530E
  Certificate Usage: General Purpose
  Issuer:
    cn=ACT2 SUDI CA
    o=Cisco
  Subject:
    Name: C891FW-E-K9
    Serial Number: PID:C891FW-E-K9 SN:FOC19244JNQ
    cn=C891FW-E-K9
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:C891FW-E-K9 SN:FOC19244JNQ
  Validity Date:
    start date: 02:53:14 CEST Oct 9 2015
    end   date: 02:53:14 CEST Oct 9 2025
  Associated Trustpoints: CISCO_IDEVID_SUDI
```


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

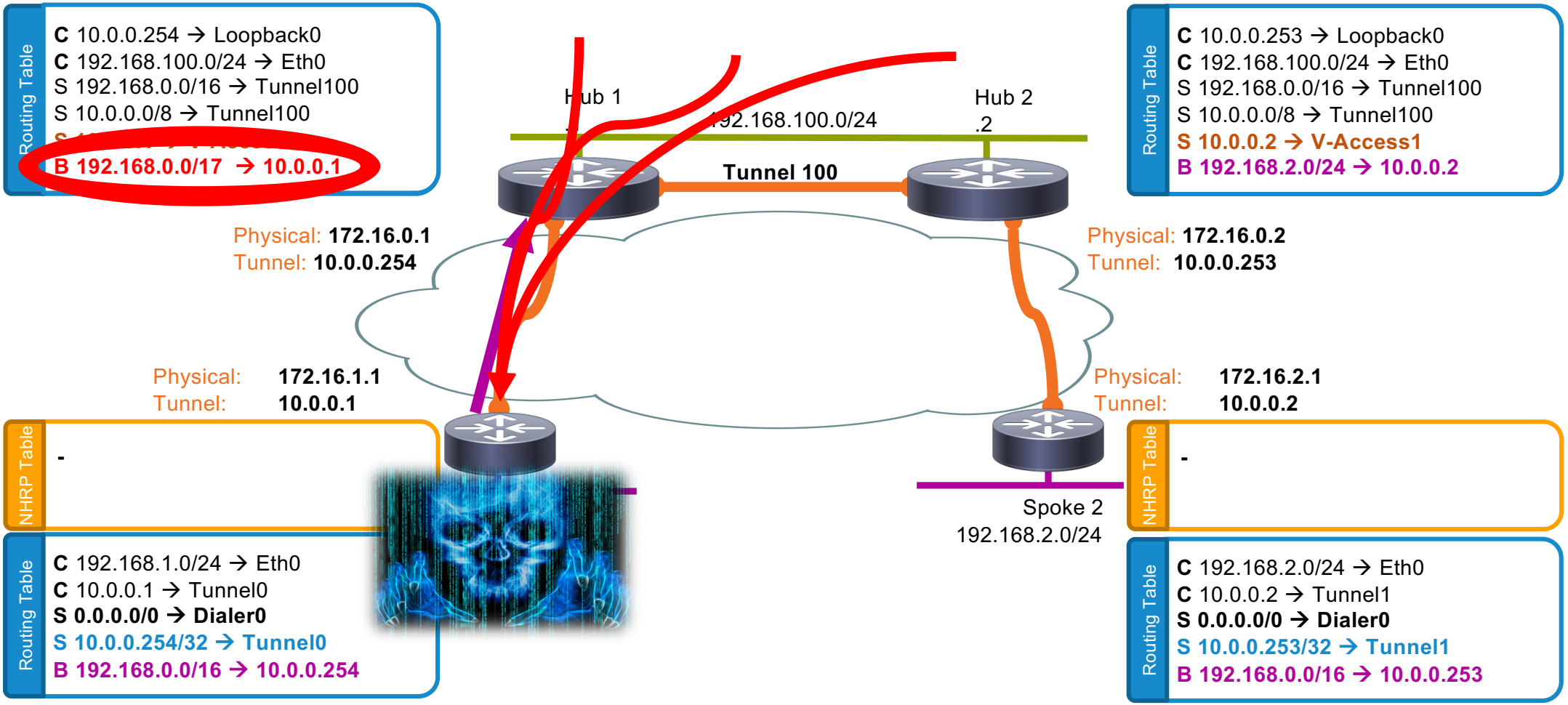
ZTD – SUDI enhancement



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

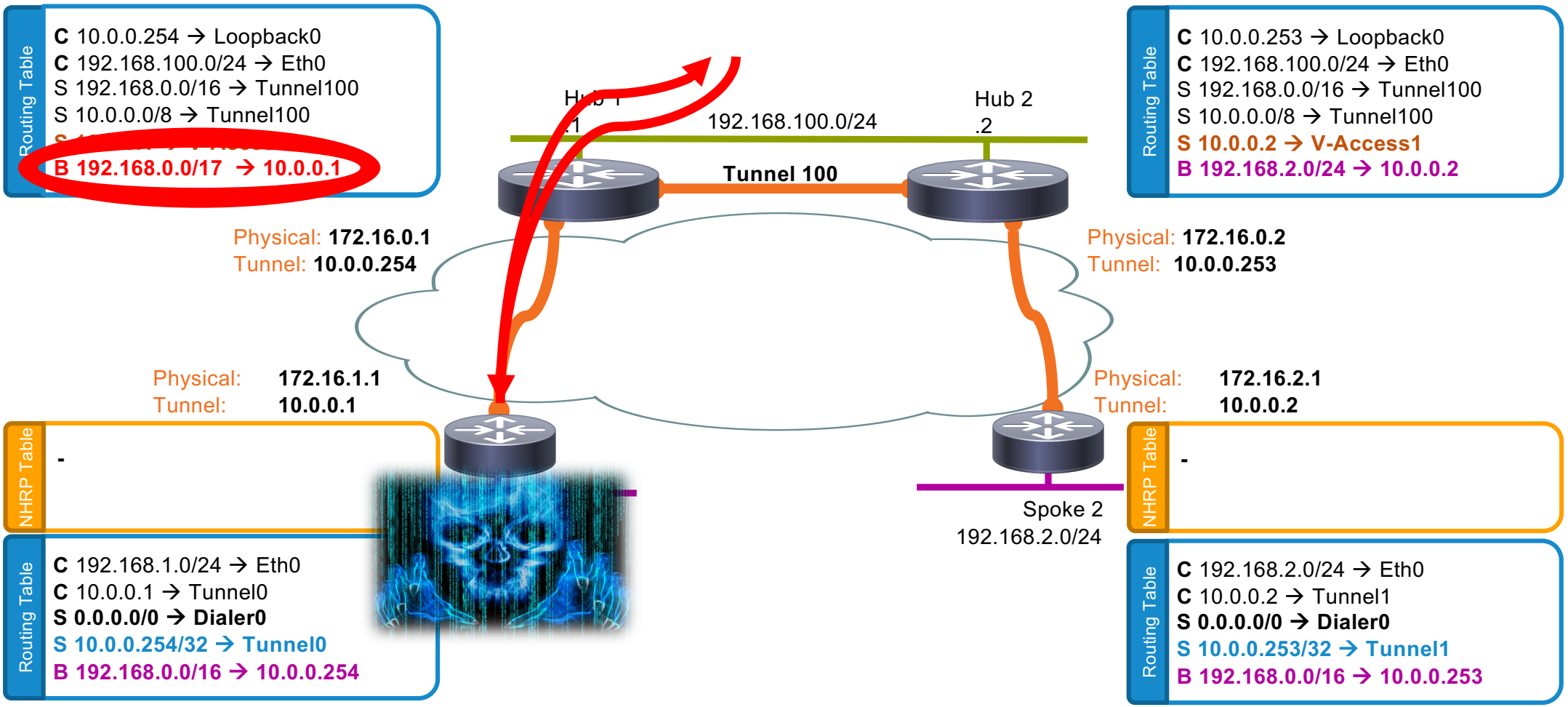
Limited trust to the Spokes

Risk: Route Injection



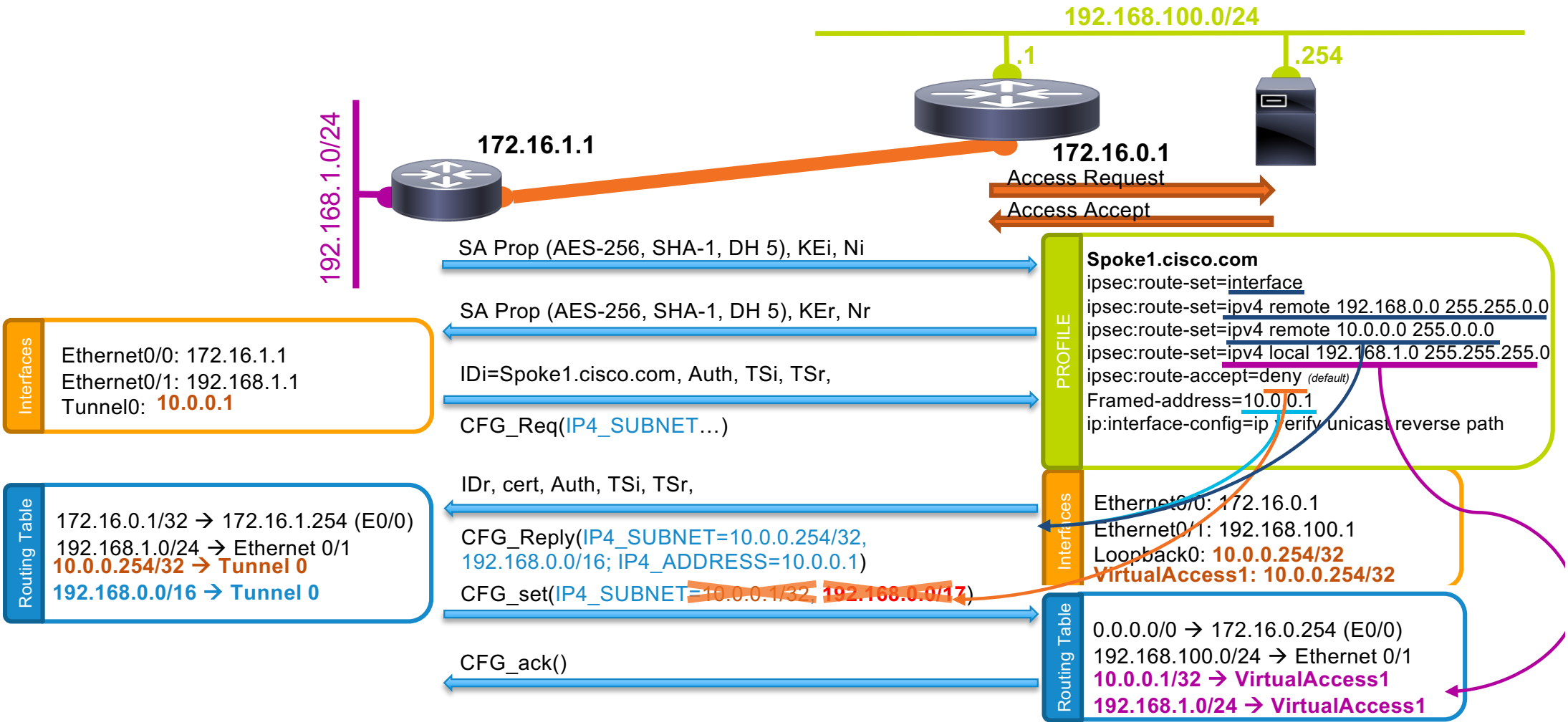
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Risk: Traffic Injection

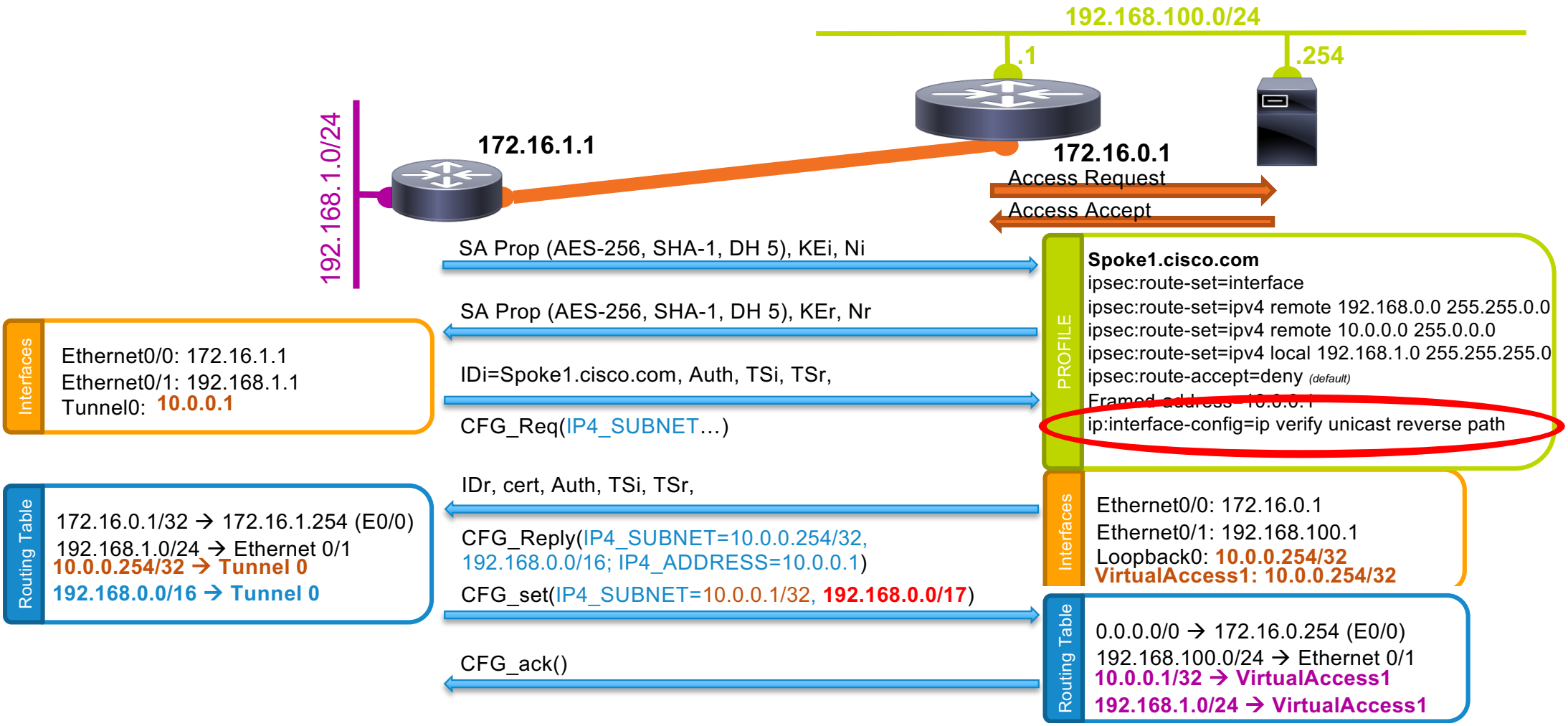


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

AAA local & remote routes



AAA local & remote routes



Before we part…

Route Exchange Protocol Selection

Branch-Hub		Use case				
IKEv2 Recommended	Simple, large scale	Static (No redistribution IGP→IKE)	Simple branches (< 20 prefixes)	Identity-based route filtering	Lossy networks	High density hubs
BGP Recommended	Simple to complex, large scale	Dynamic (Redistribution IGP → BGP)	Complex branches (> 20 prefixes)	Powerful route filtering – not identity based	Lossy networks	High density hubs up to 350K routes
EIGRP not recommended at large scale	Simple to complex	Dynamic (Redistribution IGP → IGP)	Semi-complex branches (> 20 prefixes)	Intermediate route filtering – not identity based	Lossless networks (very rare)	< 5000 prefixes at hub

Hub-Hub	Use case		
BGP Recommended	Large amount of prefixes (up to 1M)	Road to scalability	Powerful route filtering
IGP (EIGRP, OSPF)	< 5000 prefixes total	Perceived simplicity	

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

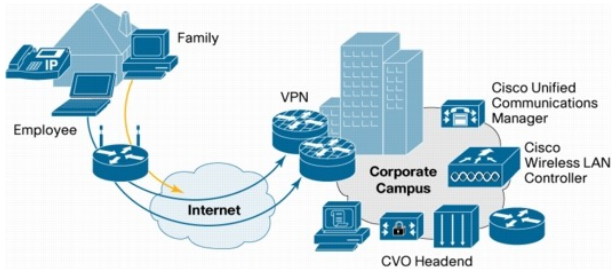
Ideal for M2M, IoT, Field, B2B, Managed Svc,…

Connected Vehicle

ISP & Managed Service

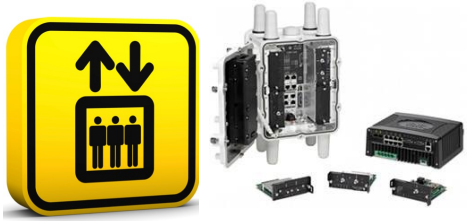
ATM's

Fleet Connectivity



Virtual Office, Retails,…

SmartGrid and all Utilities



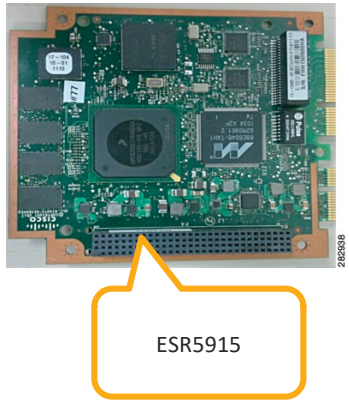
Elevators and IoT via Field Area Routers

Construction, Oil, and field deployments

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Spotlight on ESR & IR platforms

- ESR – Embedder Services Routers
- Regular IOS
- Mobile networks in vehicles, mobile users, harsh environments
- 3 ESR models – 5915, **5921** (runs on Linux!) and 5940
- 3 IR models – IR 809, IR819 & IR 829 – ruggedized fog-computing platforms



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public