
TOMORROW starts here.
cisco
Cisco live!

Advanced IPSec with FlexVPN

BRKSEC-3013

Tom Alexander
Technical Leader

Cisco live!

Objectives & Prerequisites

- Session objectives:
  - Understand IKEv2 & FlexVPN Building blocks
  - Demonstrate the value-add of FlexVPN
  - Knowledge of complex FlexVPN Designs
- Basic understanding of the following topics is required:
  - IPsec, IKEv1, PKI, AAA, RADIUS, AnyConnect
- Experience with the following features is a plus:
  - DMVPN, EzVPN, Routing protocols
- More FlexVPN
  - Walk-In Self-Paced Labs (FlexVPN in practice)

Agenda

- FlexVPN Introduction
  - Why FlexVPN
  - FlexVPN Positioning
- FlexVPN Building Blocks
- Shortcut Switching (FlexMesh)
- FlexVPN dVTI, AAA
  - Per peer features
  - AAA integration
- FlexVPN Redundancy
  - Backup Mechanisms
  - Load Balancing
- Remote Access
  - Overview
  - AnyConnect 3.0 Mobile
- Wrap-up

Before We Begin...

For Your Reference

Additional info

"For your Reference" slides:

- Just for your reference when back at work.
- Will not be covered in detail

"Additional info" slides:

- Rendered in the presentation PDF (download it through the Cisco Live portal)
- Not shown during the live presentation
- Cover extra details or small additional topics




FlexVPN Introduction

Why FlexVPN, IKEv2

EasyVPN, DMVPN and Crypto Maps

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client confi
 key cisco123
 pool dvti
 acl 100
crypto isakmp profile dvti
   match identity group ci
   client authentication l
   isakmp authorization li
   client configuration ad
   virtual-template 1
crypto ipsec transform-set
crypto ipsec profile dvti
 set transform-set dvti
 set isakmp-profile dvti
interface Virtual-Template
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec p
ip local pool dvti 192.168
ip route 0.0.0.0 0.0.0.0 10
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
```

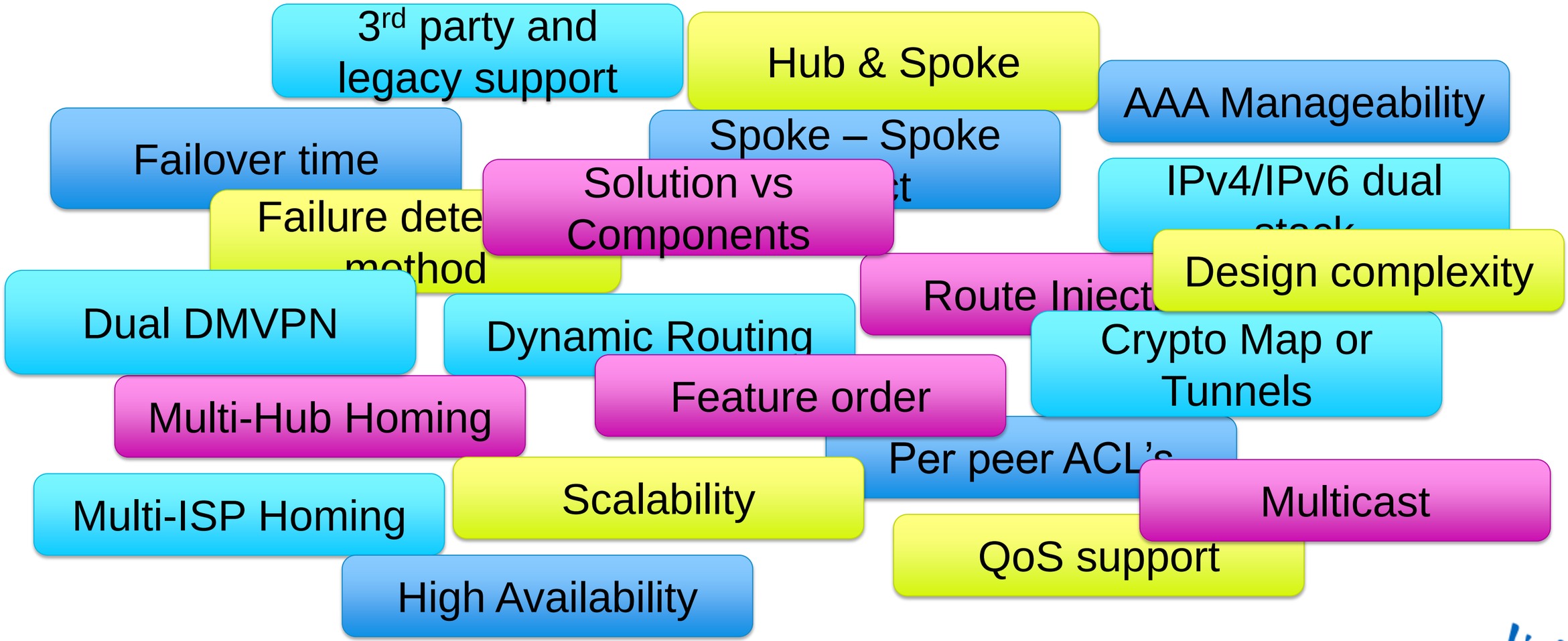
```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto ipsec transform-set vpn-ts-set es
 mode transport
crypto ipsec profile vpnprofile
 set transform-set vpn-ts-set
interface Tunnel0
 ip address 10.0.0.254 255.255.255.0
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpnprof

ip route 192.168.0.0 255.255.0.0 Null0rc
bgp log-neighbor-changes
redistribute static
 neighbor DMVPN peer-group
 bgp listen range 10.0.0.0/24 peer-group
 neighbor DMVPN remote-as 1
 no auto-summary
```

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client configuration group cisco
 key pr3sh@r3dk3y
 pool vpnpool
 acl 110
crypto ipsec transform-set vpn-ts-set esp-3des esp-sha-hmac
crypto dynamic-map dynamicmap 10
 set transform-set vpn-ts-set
 reverse-route
crypto map client-vpn-map client authentication list userauthen
crypto map client-vpn-map isakmp authorization list groupauthor
crypto map client-vpn-map client configuration address initiate
crypto map client-vpn-map client configuration address respond
crypto map client-vpn-map 10 ipsec-isakmp dynamic dynamicmap
interface FastEthernet0/0
 ip address 83.137.194.62 255.255.255.240
 crypto map client-vpn-map
ip local pool vpnpool 10.10.1.1 10.10.1.254
access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.1.0 0.0.0.255
```

VPN Technology Selection

Death by a thousand questions…



FlexVPN Unifies

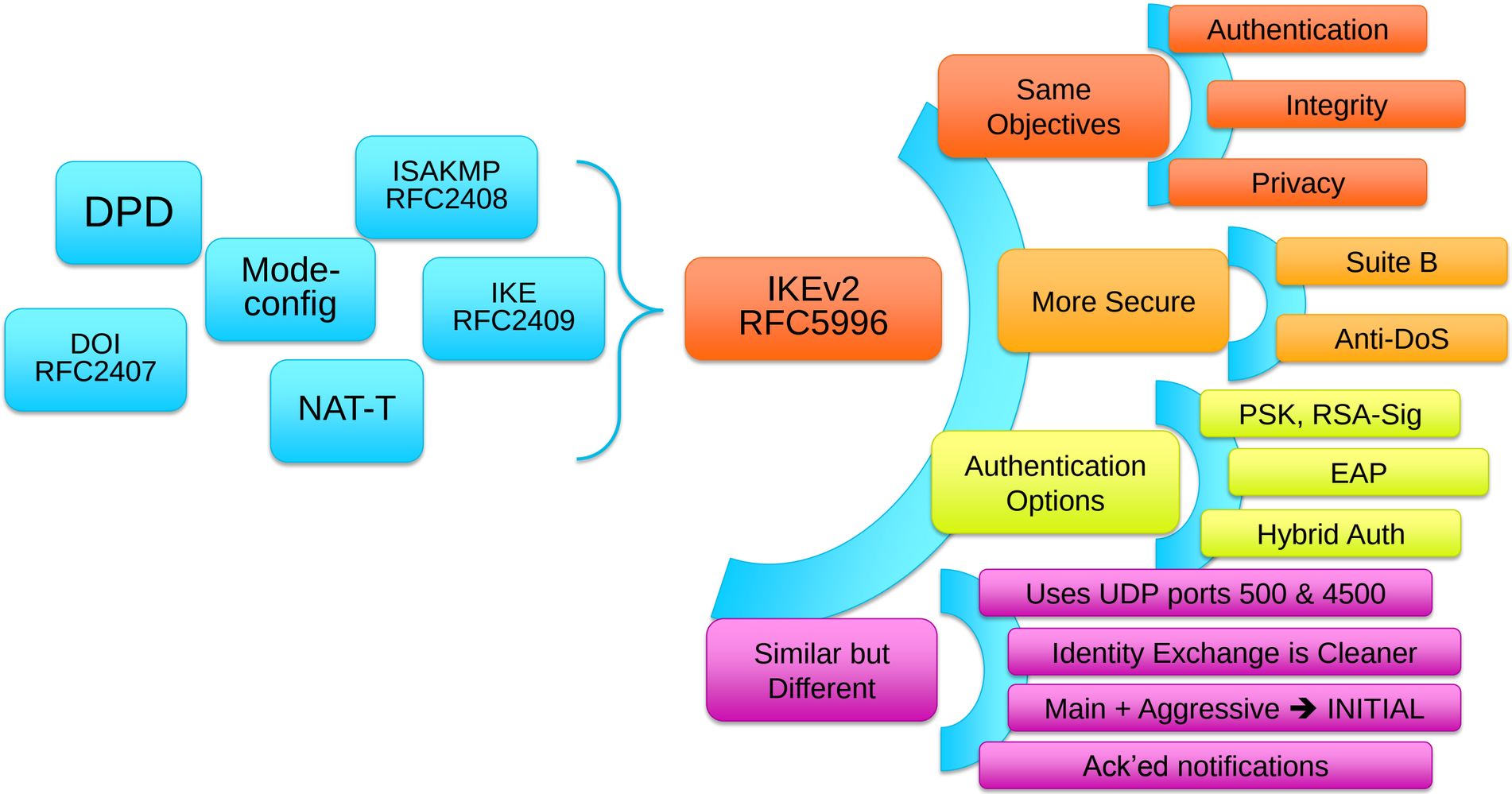
Unified Overlay VPN's

VPN	Interop	Dynamic Routing	IPsec Routing	Spoke-spoke direct (shortcut)	Remote Access	Simple Failover	Source Failover	Config push	Per-peer config	Per-Peer QoS	Full AAA Management
Easy VPN	No	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
DMVPN	No	Yes	No	Yes	No	partial	No	No	No	group	No
Crypto Map	Yes	No	Yes	No	Yes	poor	No	No	No	No	No
Flex VPN	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

- One VPN to learn and deploy
- Everything works – no questions asked

Flex is IKEv2 Only

Why Flex now?



FlexVPN Overview

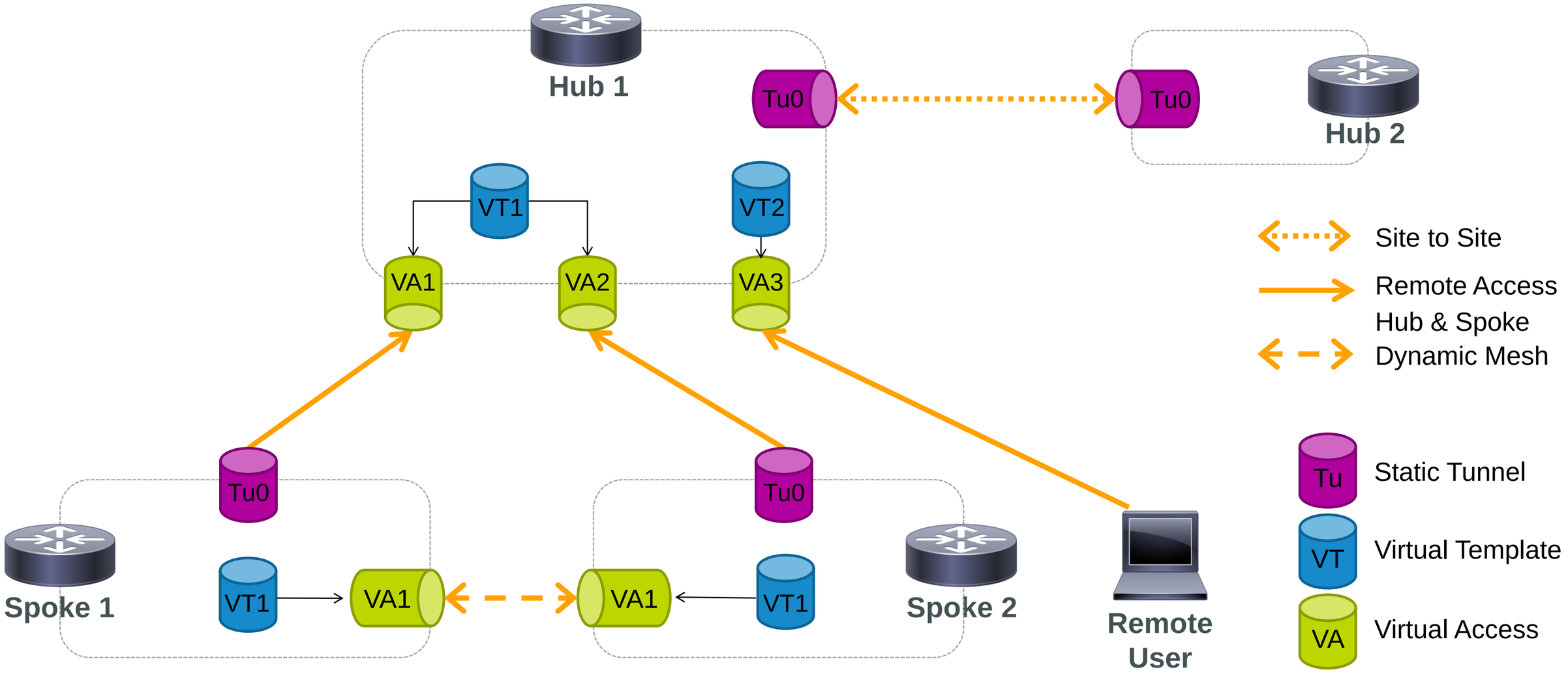
- What is FlexVPN?
  - IKEv2-based unified VPN technology that combines site-to-site, remote-access, hub-spoke and spoke-to-spoke topologies

- FlexVPN highlights
  - Unified CLI
  - Based on and compliant to IKEv2 standard
  - Unified infrastructure: leverages IOS Point-to-Point tunnel interface
  - Unified features: most features available across topologies
  - Key features: AAA, config-mode, dynamic routing, IPv6
  - Simplified config using smart-defaults
  - Interoperable with non-Cisco implementations
  - Easier to learn, market and manage




FlexVPN Building Blocks

FlexVPN and Interfaces



Sample FlexVPN Config

All parameters tunable "per-peer" via AAA

IKEv2 Parameters

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn R1.cisco.com
 authentication local rsa-sig
 authentication remote eap
 pki trustpoint TP sign
 aaa authentication eap default
 aaa authorization user eap
 virtual-template 1
```

Hub & Spoke

```
interface Virtual-Template1 type tunnel
 ip unnumbered loopback0
 tunnel protection ipsec profile default
```

Dual Stack v4/v6

Remote Access

```
 ip nhrp network-id 1
```

Interop & Legacy
crypto map peer

```
 tunnel mode ipsec ipv4
```

Spoke-Spoke
shortcut switching

IKEv2 CLI Overview

IKEv2 Profile – Extensive CLI

```
crypto ikev2 profile default

 identity local address 10.0.0.1
 identity local fqdn local.cisco.com
 identity local email local@cisco.com
 identity local dn


 match identity remote address 10.0.1.1
 match identity remote fqdn remote.cisco.com
 match identity remote fqdn domain cisco.com
 match identity remote email remote@cisco.com
 match identity remote email domain cisco.com
 match certificate certificate_map

 match fvrf red
 match address local 172.168.1.1


 authentication local pre-share
 authentication local rsa-sig
 authentication local eap

 authentication remote pre-share
 authentication remote rsa-sig
 authentication remote eap

 keyring local IOSKeyring
 keyring aaa AAAlist

 pki trustpoint <trustpoint_name>
```

Only one local identity allowed

Multiple “match identity” allowed

Only one local method allowed

Multiple remote methods allowed

Self Identity Control

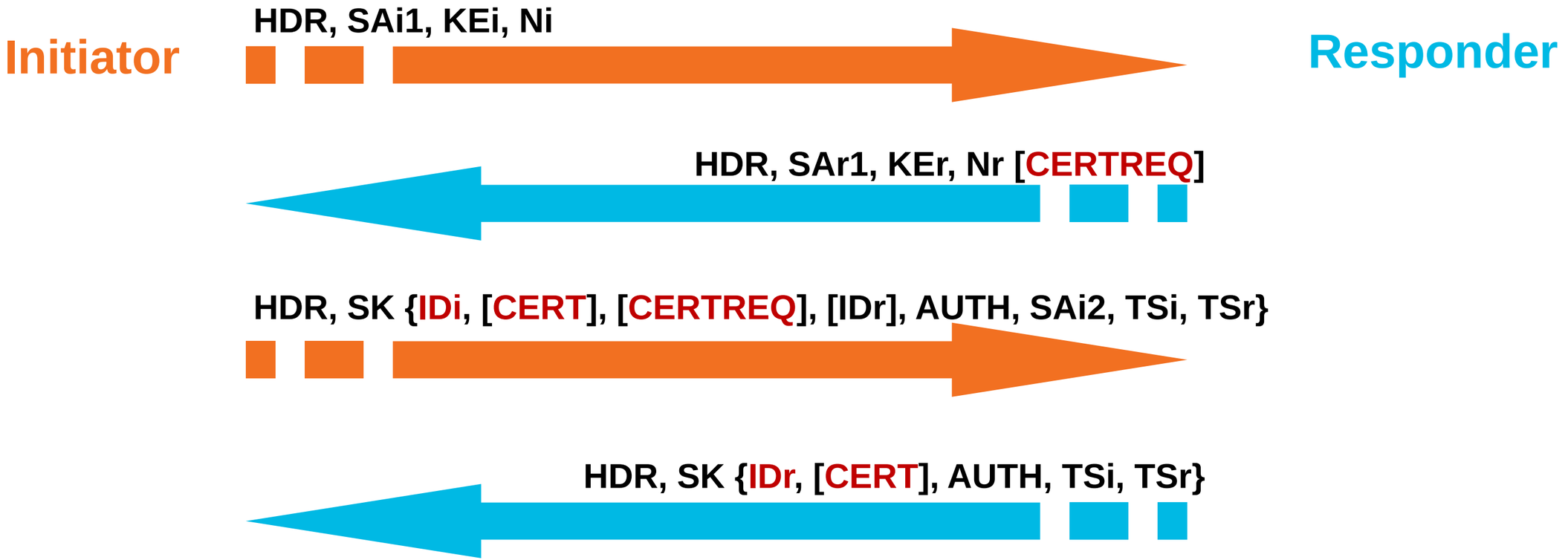
Match on peer IKE identity or certificate

Match on local address and front VRF

Asymmetric local & remote authentication methods

Local and AAA-based Pre-Shared Keyring

IKEv2 Basic Negotiation



HDR – IKE Header

SAi, SAr – Crypto algorithms proposed/accepted by the peer

KEi, KEr – Initiator Key Exchange material

Ni, Nr – Initiator/Responder Nonce

SK {...} – Payload encrypted and integrity protected

IDi, IDr – Initiator/Responder IKE Identity

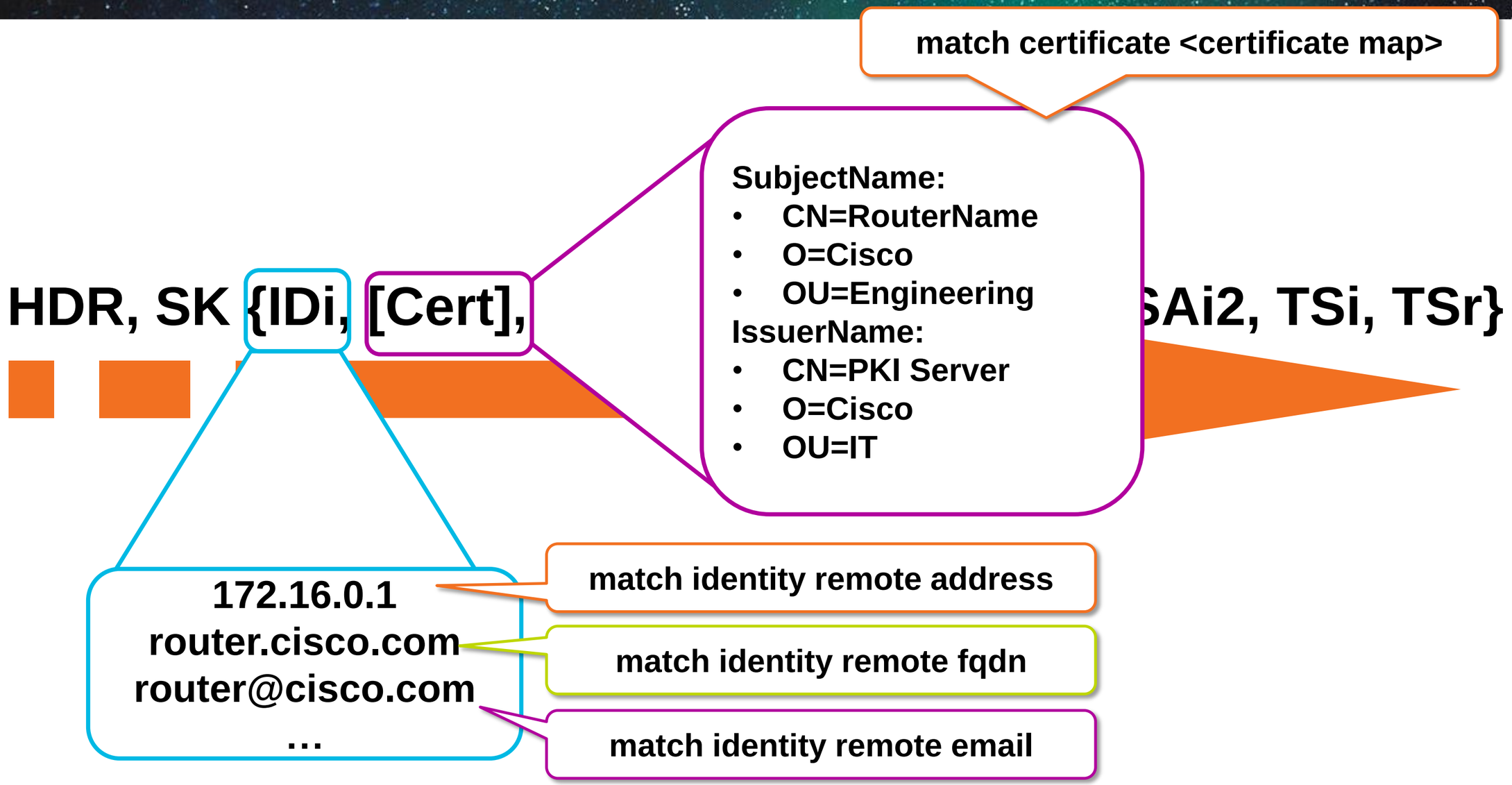
CERTREQ, CERT – Certificate Request, Certificate Payload

AUTH – Authentication data

SA – Proposal & Transform to create initial CHILD_SA

TSi, TSr – Traffic Selectors (as src/dst proxies)

IKEv2 Profile Match Statements



IPsec CLI Overview

Tunnel Protection

Transform set unchanged

IPsec profile defines SA parameters and points to IKEv2 profile

Dynamic and Static point-to-point interfaces

Static point-to-point interfaces

Tunnel protection links to to IPsec profile

```
crypto ipsec transform-set default esp-aes 128 esp-sha-hmac

crypto ipsec profile default
 set transform-set default
 set crypto ikev2 profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel protection ipsec profile default

interface Tunnel0
 ip address 10.0.0.1 255.255.255.252
 tunnel source Ethernet0/0
 tunnel destination 172.16.2.1
 tunnel protection ipsec profile default
```

Introducing Smart Defaults

Intelligent, reconfigurable defaults

```
crypto ipsec transform-set default
                esp-aes 128 esp-sha-hmac

crypto ipsec profile default
 set transform-set default
 set crypto ikev2 profile default

crypto ikev2 proposal default
  encryption aes-cbc-256 aes-cbc-128 3des
  integrity sha512 sha 256 sha1 md5
  group 5 2

crypto ikev2 policy default
  match fvrf any
  proposal default

crypto ikev2 authorization policy default
 route set interface
 route accept any
```

These constructs are the Smart Defaults

```
crypto ikev2 profile default
 match identity remote address 10.0.1.1
 authentication local rsa-sig
 authentication remote rsa-sig
 aaa authorization user cert list default default
 pki trustpoint TP
!
interface Tunnel0
 ip address 192.168.0.1 255.255.255.252
 tunnel protection ipsec profile default
```

What you need to specify

Static Site-to-Site Example

Additiona info

Router 1

Router 2

Perform IKE SA agreement & Diffie-Hellman key exchange (not shown)

My IKE ID is: **r1.cisco.com** (FQDN)
My PSK authentication payload is...
I want to protect GRE traffic between...

Map connection to IKEv2 profile “default” by matching on peer FQDN

Verify peer’s AUTH payload & produce our own based on configured PSK

Use our own FQDN as IKE ID

My IKE ID is: **r2.cisco.com** (FQDN)
My PSK authentication payload is...
I agree to protect GRE traffic between...

Finalise IPsec SAs (GRE between local & remote WAN addresses)

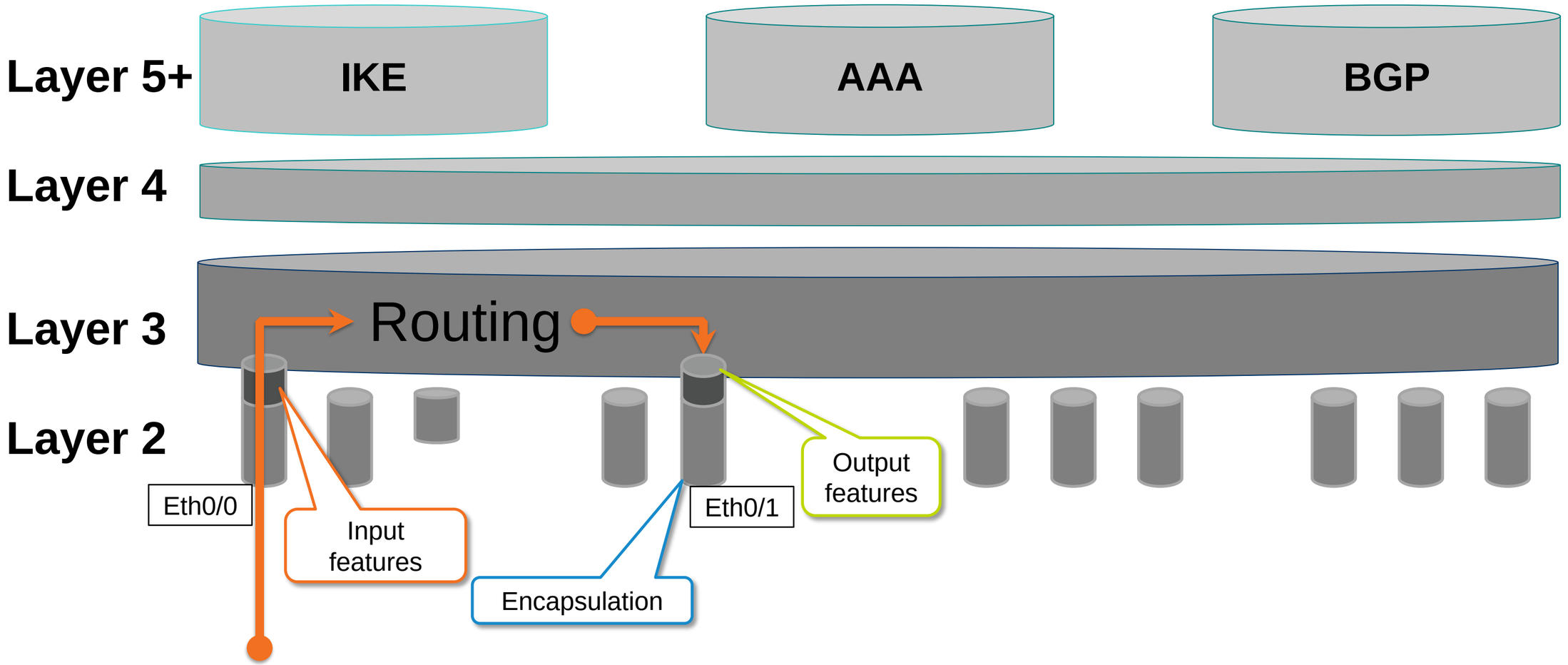
Establish routing protocol neighbourship & exchange prefixes

```
crypto ikev2 profile default
 match identity remote fqdn r1.cisco.com
 identity local fqdn r2.cisco.com
 authentication remote pre-share key r1r2!
 authentication local pre-share key !r2r1
!
interface Tunnel0
 ip address 10.0.0.2 255.255.255.252
 tunnel source Ethernet0/0
 tunnel destination 192.0.2.1
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 192.0.2.2 255.255.255.0
!
router rip
 version 2
 network 10.0.0.0
 ...
```

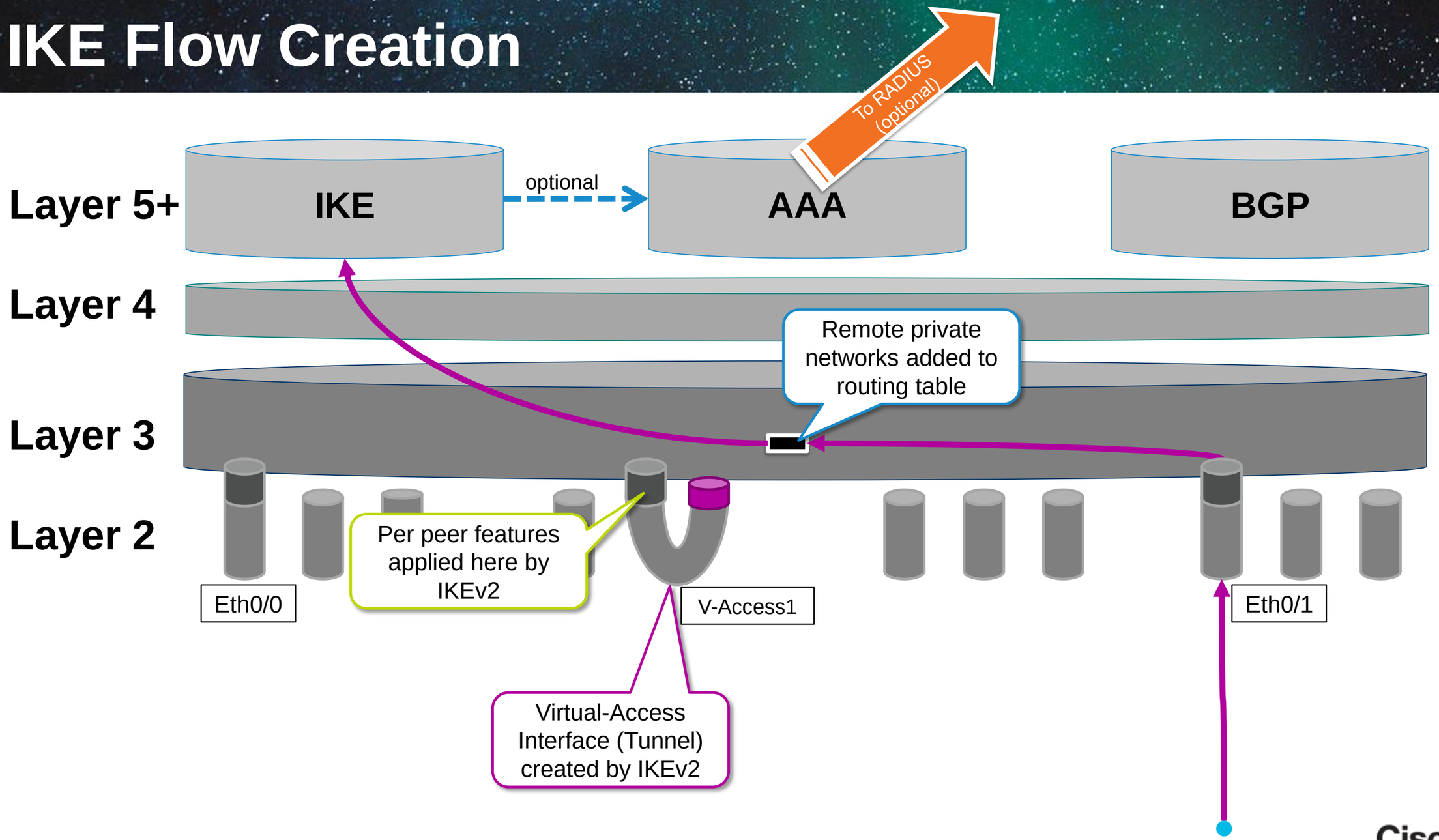



Packet Forwarding

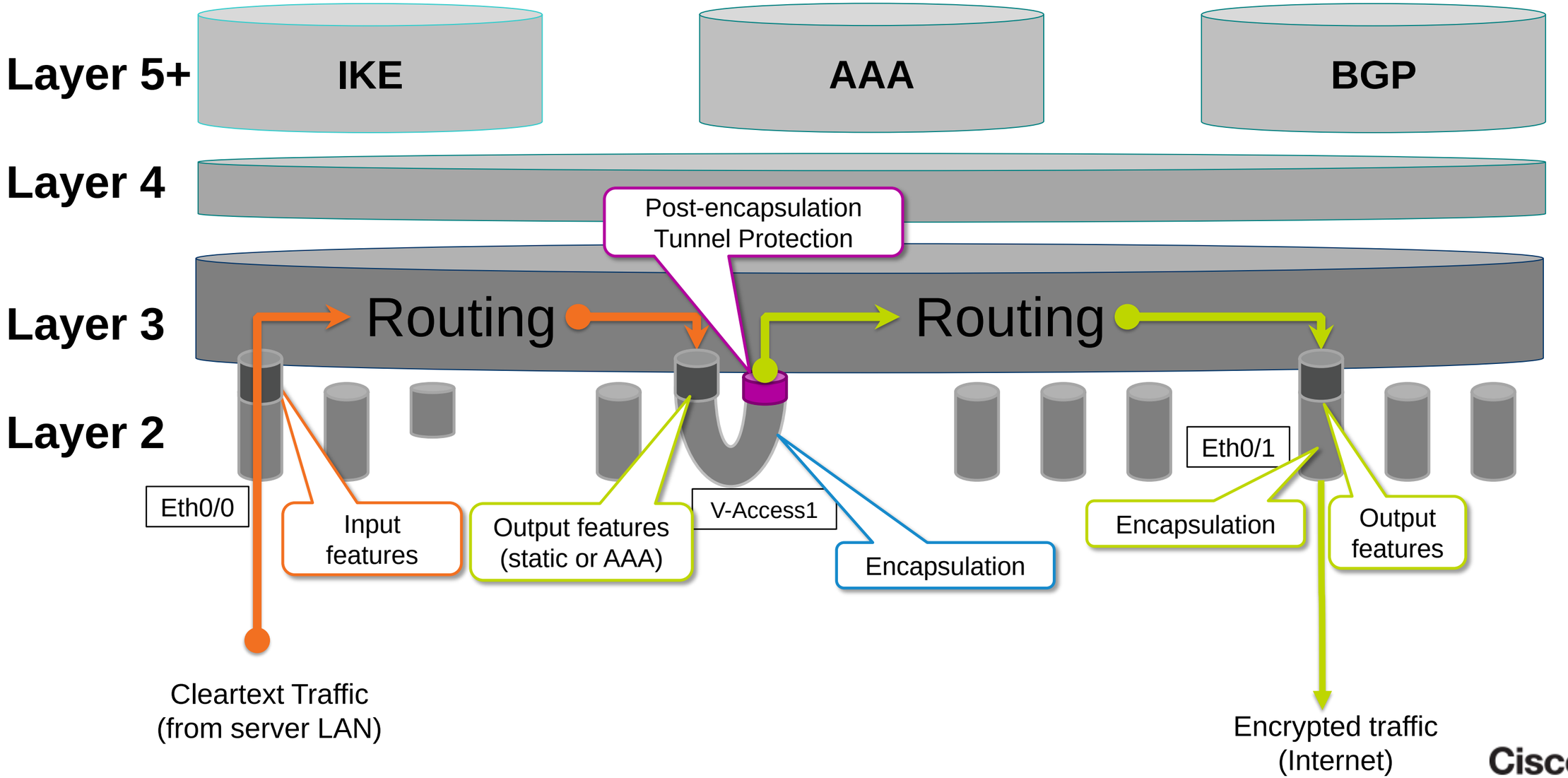
Basic Packet Forwarding



IKE Flow Creation



Packet Forwarding – Tunnels & Features





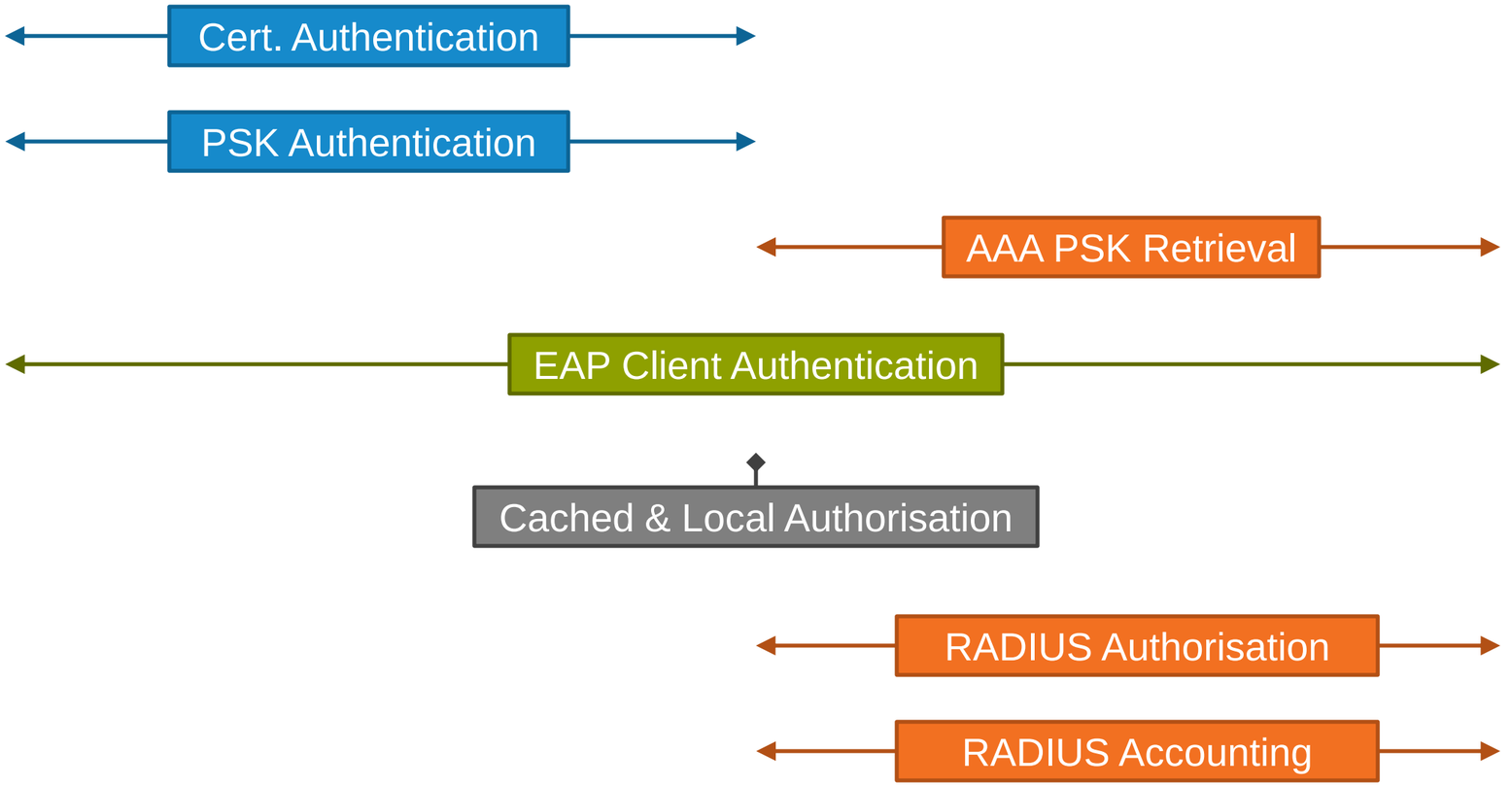

FlexVPN AAA Integration

High-Level AAA Interactions

RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend



Authorisation Types

Not mutually exclusive – May be combined

Implicit User Authorisation

```
crypto ikev2 profile default
 aaa authorization user {psk|eap} cached
```

RADIUS (Access-Accept)

Local PSK = cisco!

Remote PSK = !ocsic

Other user attributes for joe

Cached for authorisation

Uses cached attributes received from RADIUS during AAA PSK retrieval or EAP authentication

Explicit User Authorisation

```
crypto ikev2 profile default
 aaa authorization user {psk|eap|cert} list list [name | name-mangler mangler]
```

Retrieves user attributes from RADIUS (local database not supported)

Explicit Group Authorisation

Reverse order of precedence (group > user)

```
crypto ikev2 profile default
 aaa authorization group {psk|eap|cert} [override] list list [name | name-mangler mangler]
```

Retrieves group attributes from RADIUS or local database

Attributes – Merging

FlexVPN Server

Received during AAA-based authentication

Attribute	Value
Framed-IP-Address	10.0.0.101
ipsec:dns-servers	10.2.2.2

Cached User Attributes

Explicit User Attributes take precedence

Explicit User Attributes

Attribute	Value
Framed-IP-Address	10.0.0.102
ipsec:dns-servers	10.2.2.2

Merged User Attributes

Merged User Attributes take precedence except if “group override” configured

Explicit Group Attributes

Attribute	Value
Framed-IP-Address	10.0.0.102
ipsec:dns-servers	10.2.2.2
ipsec:banner	Welcome !

Final Merged Attributes

AAA Server

Received during explicit user authorisation

Attribute	Value
Framed-IP-Address	10.0.0.102

Received during explicit group authorisation

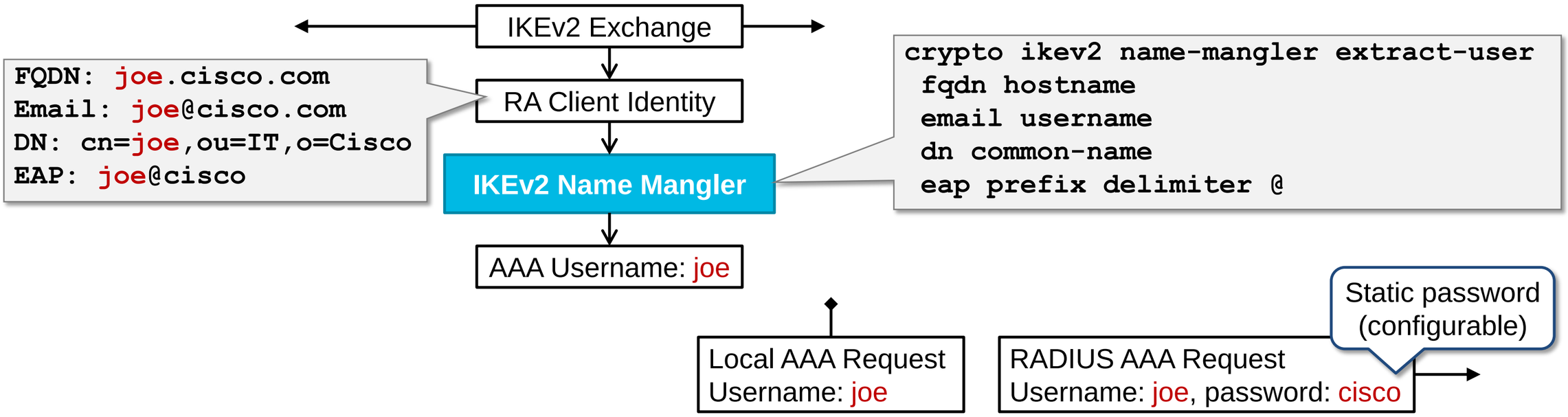
Attribute	Value
ipsec:dns-servers	10.2.2.3
ipsec:banner	Welcome !

Building Block – IKEv2 Name Mangler

RA Client
IKEv2 Initiator
RADIUS Client

FlexVPN Server
IKEv2 Responder
RADIUS NAS

AAA Server
RADIUS Server



- Start with the peer's IKE or EAP identity
- Derive a username that is meaningful to AAA (local or RADIUS)

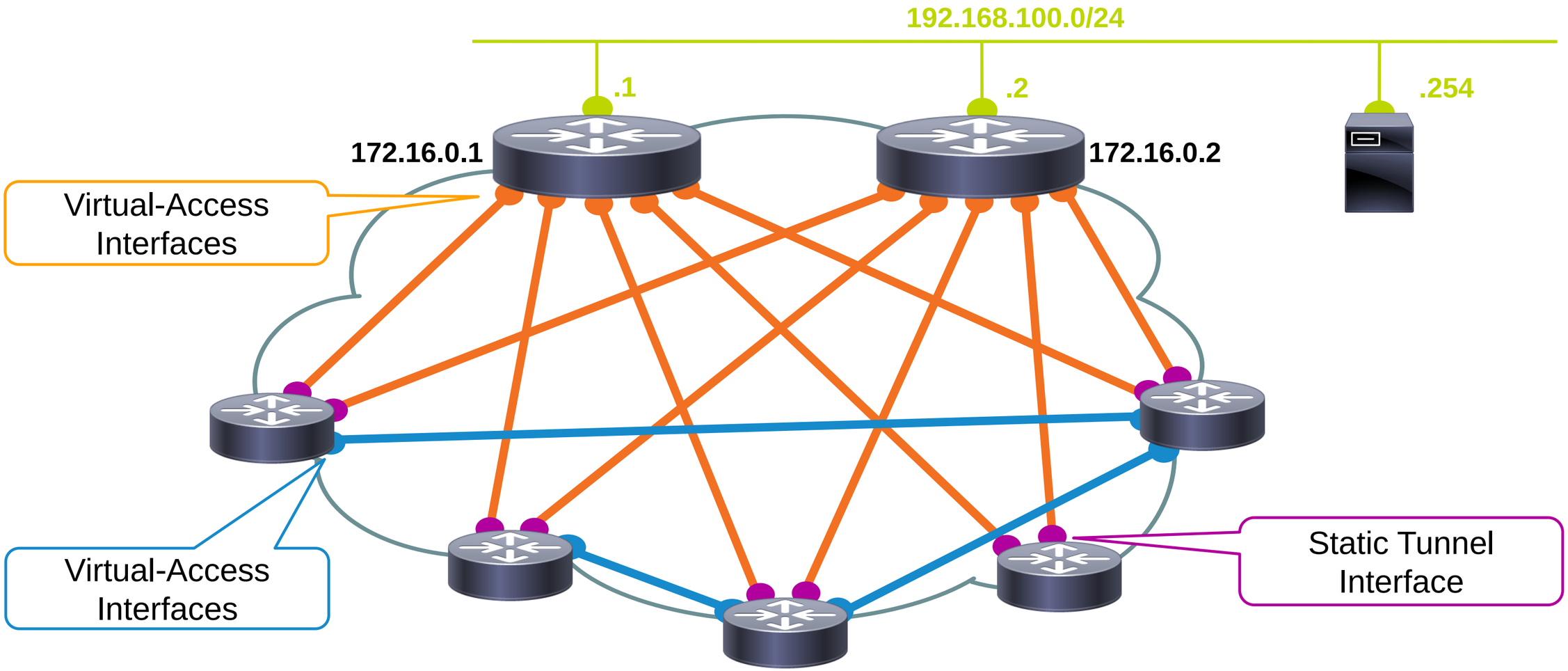



Shortcut Switching

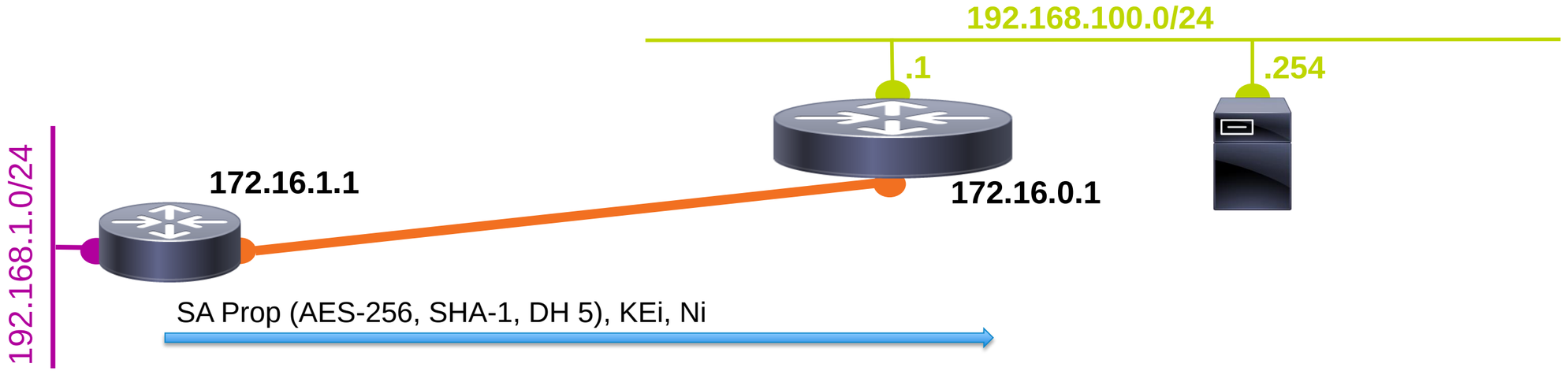
With IKEv2 Policies

FlexVPN Mesh

Network Diagram with Hub Resiliency



Hub & Spoke Bootstrap – Config Exchange



SA Prop (AES-256, SHA-1, DH 5), KEi, Ni

SA Prop (AES-256, SHA-1, DH 5), KEr, Nr

IDi=Spoke1.cisco.com, Auth, TSi, TSr,

CFG_Req(IP4_SUBNET…)

IDr, cert, Auth, TSi, TSr,

CFG_Reply(IP4_SUBNET=10.0.0.254/32, 192.168.0.0/16;
IP4_ADDRESS=10.0.0.1)

CFG_set(IP4_SUBNET=10.0.0.1/32, 192.168.1.0/24,
10.0.0.1/32)

CFG_ack()

Interfaces

Ethernet0/0: 172.16.1.1
Ethernet0/1: 192.168.1.1
Tunnel0: **10.0.0.1**

Spoke Assigned Address (optional)

Routing Table

172.16.0.1/32 → 172.16.1.254 (E0/0)
192.168.1.0/24 → Ethernet 0/1
10.0.0.254/32 → Tunnel 0
192.168.0.0/16 → Tunnel 0

Supernet covering all spokes LAN prefixes

Interfaces

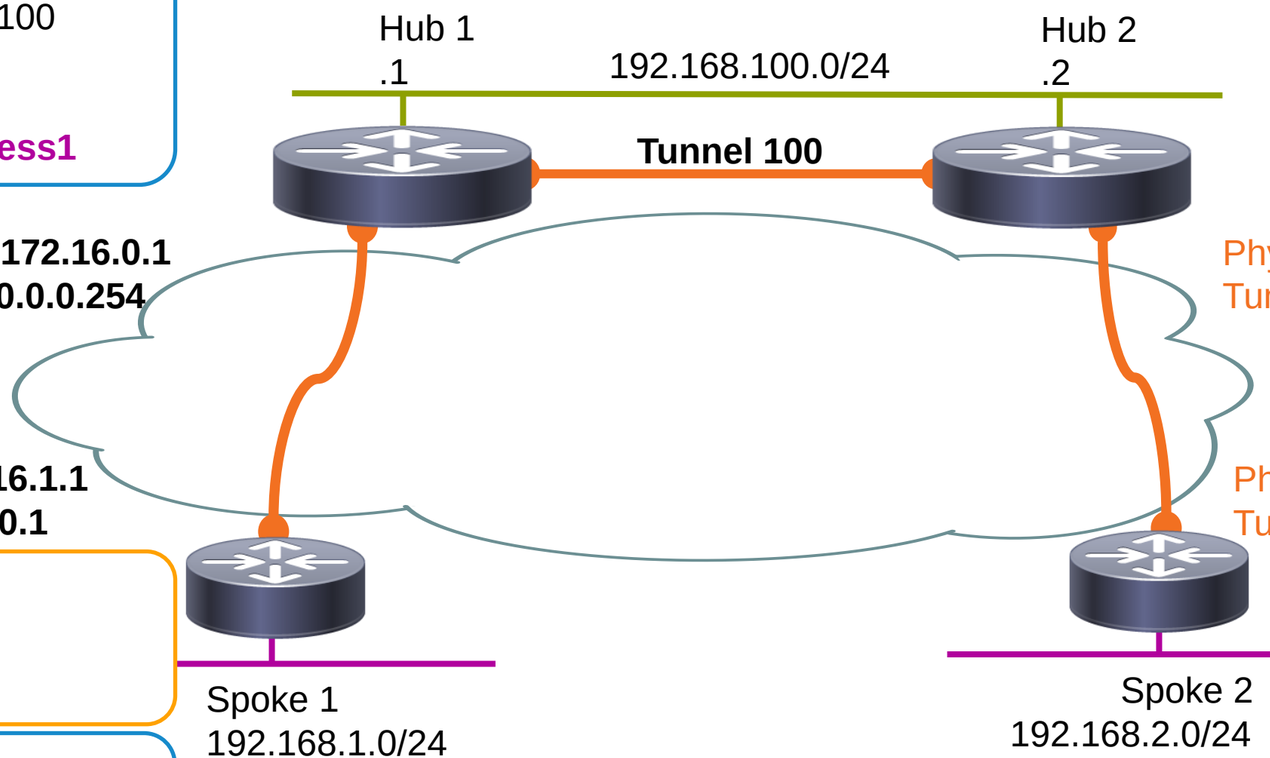
Ethernet0/0: 172.16.0.1
Ethernet0/1: 192.168.100.1
Loopback0: **10.0.0.254/32**
VirtualAccess1: 10.0.0.254/32

Routing Table

0.0.0.0/0 → 172.16.0.254 (E0/0)
192.168.100.0/24 → Ethernet 0/1
10.0.0.1/32 → VirtualAccess1
192.168.1.0/24 → VirtualAccess1

FlexVPN Hub and Spoke

IKE Exchange Routes / Policies



Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1

NHRP Table

-

NHRP Table

-

Routing Table

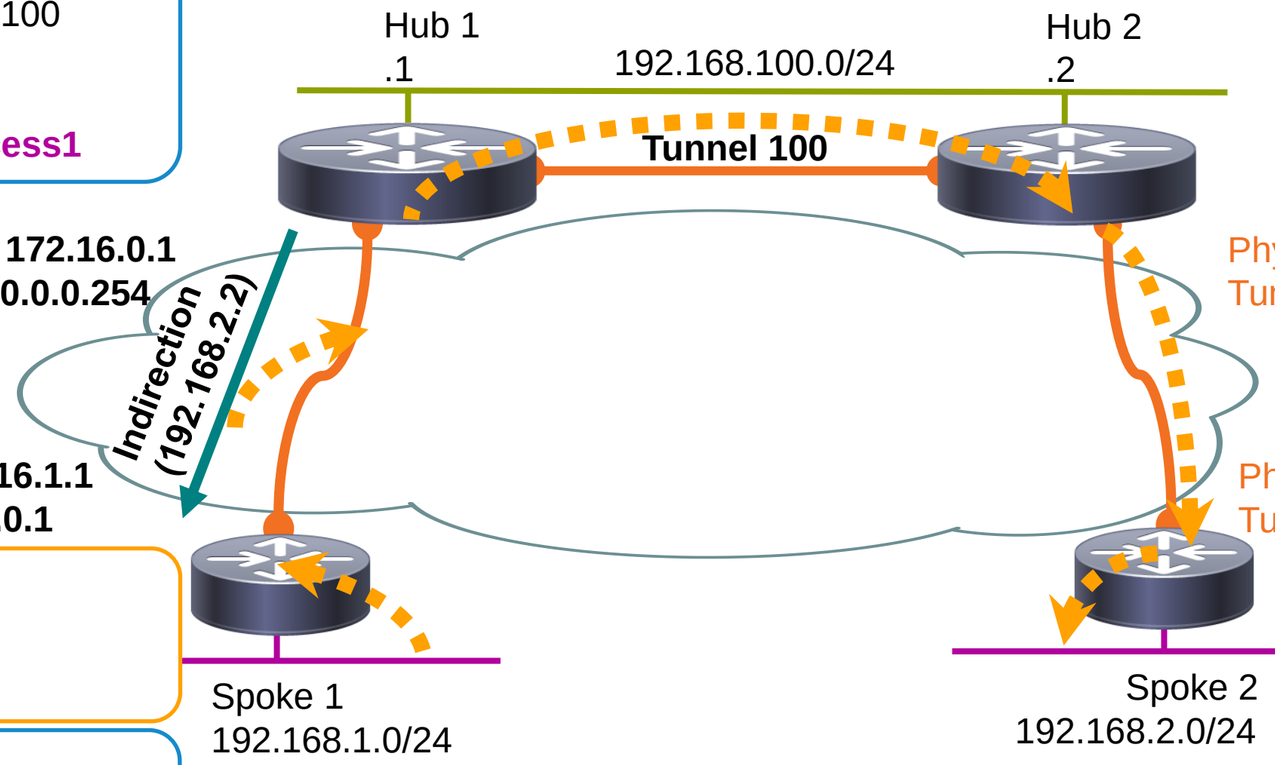
C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1

FlexVPN Mesh w/ IKEv2 Routing

Shortcut Switching (1)



Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1

NHRP Table

-

NHRP Table

-

Routing Table

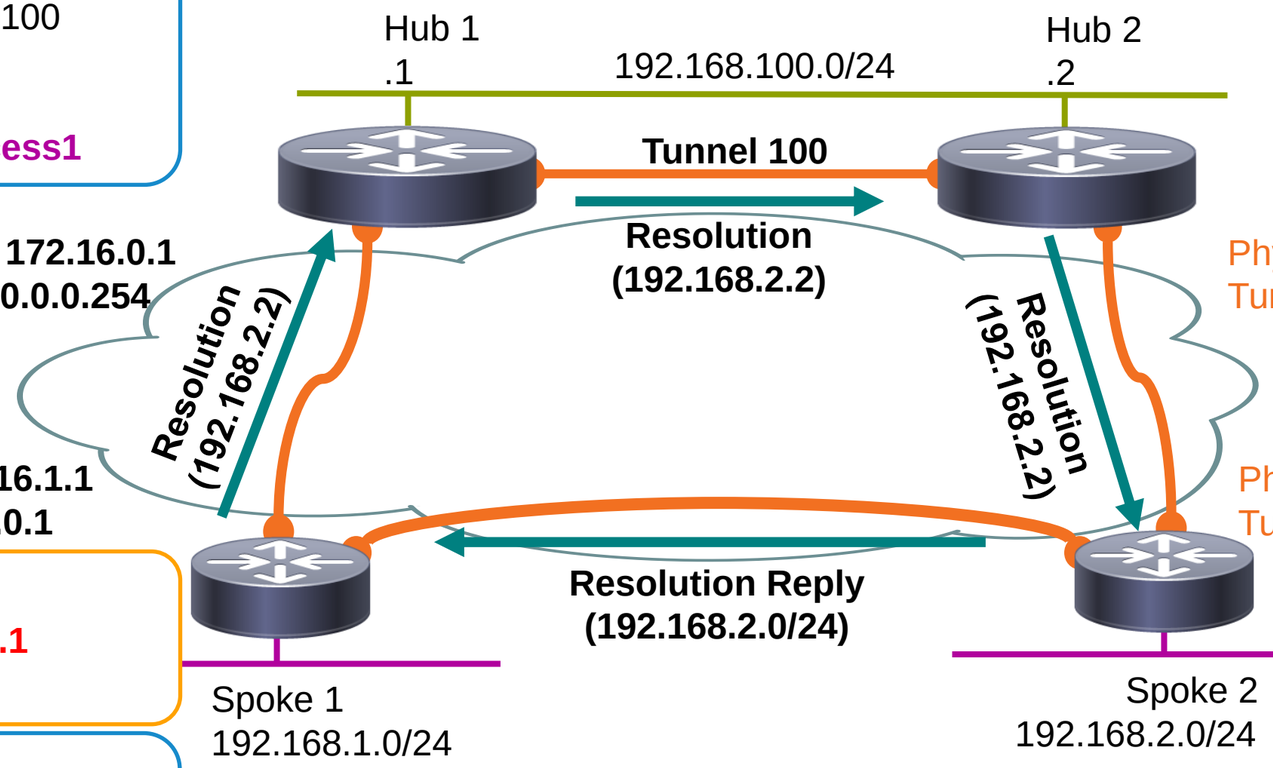
C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1

FlexVPN Mesh w/ IKEv2 Routing

Policy Shortcut Switching (2)



Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1

NHRP Table

10.0.0.2/32 → 172.16.2.1
192.168.2.0/24 → 172.16.2.1

NHRP Table

10.0.0.1 → 172.16.1.1

Routing Table

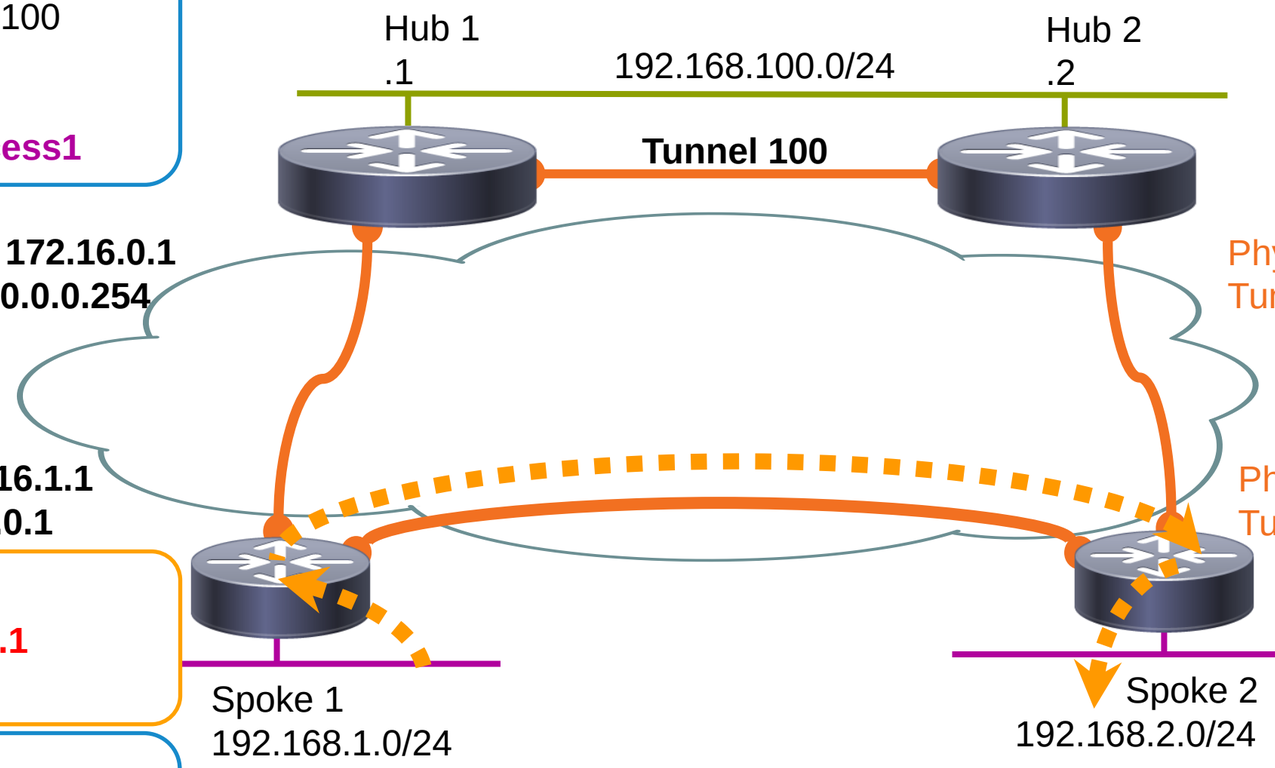
C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0
H/S 10.0.0.2/32 → V-Access1
H/S 192.168.2.0/24 → V-Access1

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1
H/S 10.0.0.1/32 → V-Access1

FlexVPN Mesh w/ IKEv2 Policy

Shortcut Switching (3)



Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1

NHRP Table

10.0.0.2/32 → 172.16.2.1
192.168.2.0/24 → 172.16.2.1

NHRP Table

10.0.0.1 → 172.16.1.1

Routing Table

C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0
H/S 10.0.0.2/32 → V-Access1
H/S 192.168.2.0/24 → V-Access1

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1
H/S 10.0.0.1/32 → V-Access1

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 or AAA spoke profiles supported. Can even control QoS, ZBF, NHRP redirect, network-id, …

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

NHRP is the magic All V-Access will be in the same network-id

Hub 1 dedicated overlay address

Inter-Hub link (not encrypted)

Same NHRP network-id on v-access and inter-hub link

FlexVPN Mesh (IKEv2 Routing)
Hub 2 Configuration

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub2.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
```

Dedicated Identity (optional)

```
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
```

Dedicated Overlay Address

- Configurations of Hub 1 and Hub 2 are almost identical!

FlexVPN Mesh (IKEv2 Routing)

Spoke Configuration

QoS Everywhere!

```
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
```

Needed for tunnel address exchange

```
crypto ikev2 authorization policy default
 route set interface
 route set interface e0/0
```

```
interface Loopback0
 ip address 10.0.0.2 255.255.255.255

interface Tunnel0
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Tunnel1
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel protection ipsec profile default
```

Tunnel to Hub 1

Tunnel1 to Hub 2

V-Template to clone for spoke-spoke tunnels

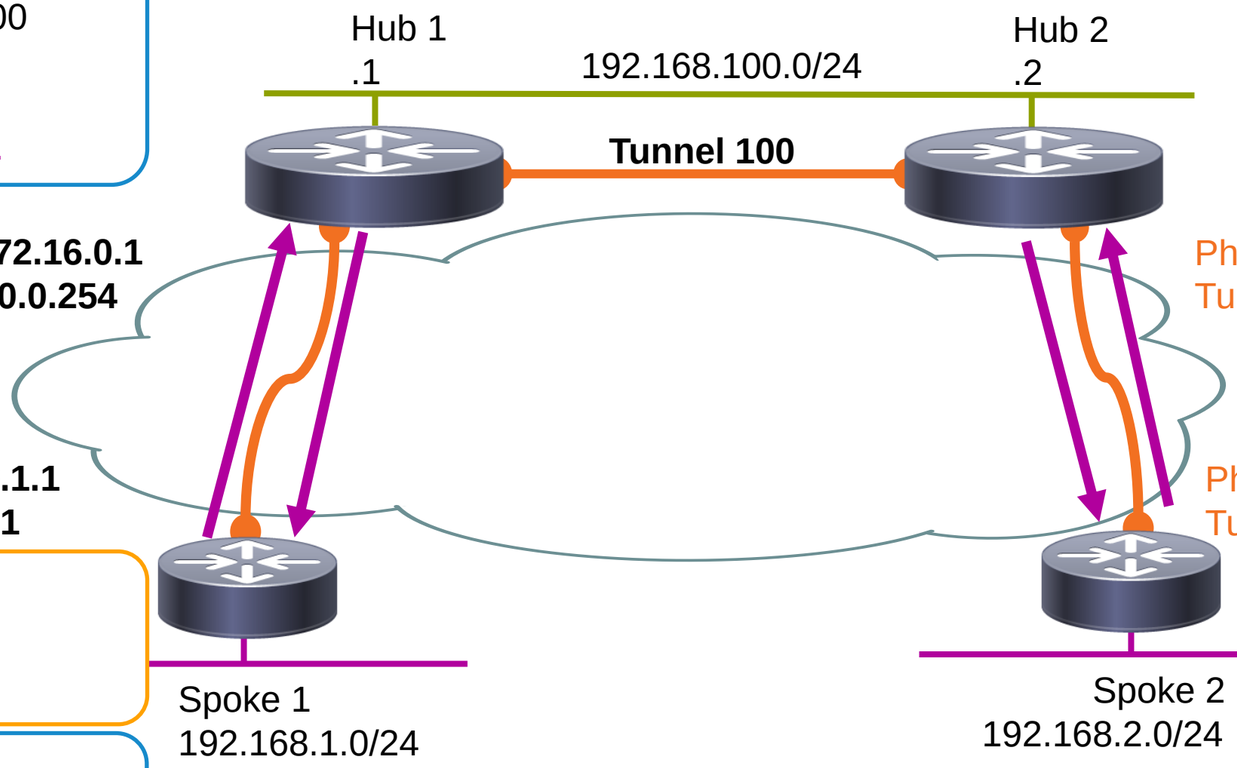
QoS can be applied here




Shortcut Switching

With a routing protocol (BGP)

FlexVPN Mesh with BGP Routing



Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
B 192.168.1.0/24 → 10.0.0.1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
B 192.168.2.0/24 → 10.0.0.2

NHRP Table

-

NHRP Table

-

Routing Table

C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
B 192.168.0.0/16 → 10.0.0.254

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
B 192.168.0.0/16 → 10.0.0.253

FlexVPN Mesh (BGP)
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

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip access-group AllowMyBGP in
 ip nhrp network-id 1
 ip nhrp redirect
 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
```

Accept connections from Spokes

Local or AAA spoke profiles supported. Can even control QoS, NHRP redirect, network-id, …

Static per-per config here…

NHRP is the magic
All V-Access will be in the same network-id

Hub 1 dedicated overlay address

Inter-Hub link (not encrypted)

Same NHRP network-id on v-access and inter-hub link

```
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
  neighbor Flex timers 5 15
  neighbor Flex next-hop-self all
  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

FlexVPN Mesh (BGP)
Hub 2 Configuration

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub2.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

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip access-group AllowMyBGP in
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default

interface Loopback0
 ip address 10.0.0.253 255.255.255.255

interface Tunnel100
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source Ethernet0/1
 tunnel destination 192.168.100.1
```

Dedicated Identity (optional)

Dedicated Overlay Address

```
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
  redistribute static route-map rm
  neighbor Flex peer-group
  neighbor Flex remote-as 1
  neighbor Flex timers 5 15
  neighbor Flex next-hop-self all
 exit-address-family
!
route-map rm permit 10
 match tag 2
```

- Almost the same as Hub 1 again!

FlexVPN Mesh (BGP)
Spoke Configuration

QoS Everywhere!

```
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
```

Needed for tunnel address exchange

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 10.0.0.253 remote-as 1
 neighbor 10.0.0.253 timers 5 15
 neighbor 10.0.0.254 remote-as 1
 neighbor 10.0.0.254 timers 5 15
 !
 address-family ipv4
  network 192.168.2.0
  neighbor 10.0.0.253 activate
  neighbor 10.0.0.254 activate
  maximum-paths ibgp 2
```

V-Template to clone for spoke-spoke tunnels

```
interface Loopback0
 ip address 10.0.0.2 255.255.255.255

interface Tunnel0
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Tunnel1
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel protection ipsec profile default
```

Tunnel to Hub 1

Tunnel1 to Hub 2

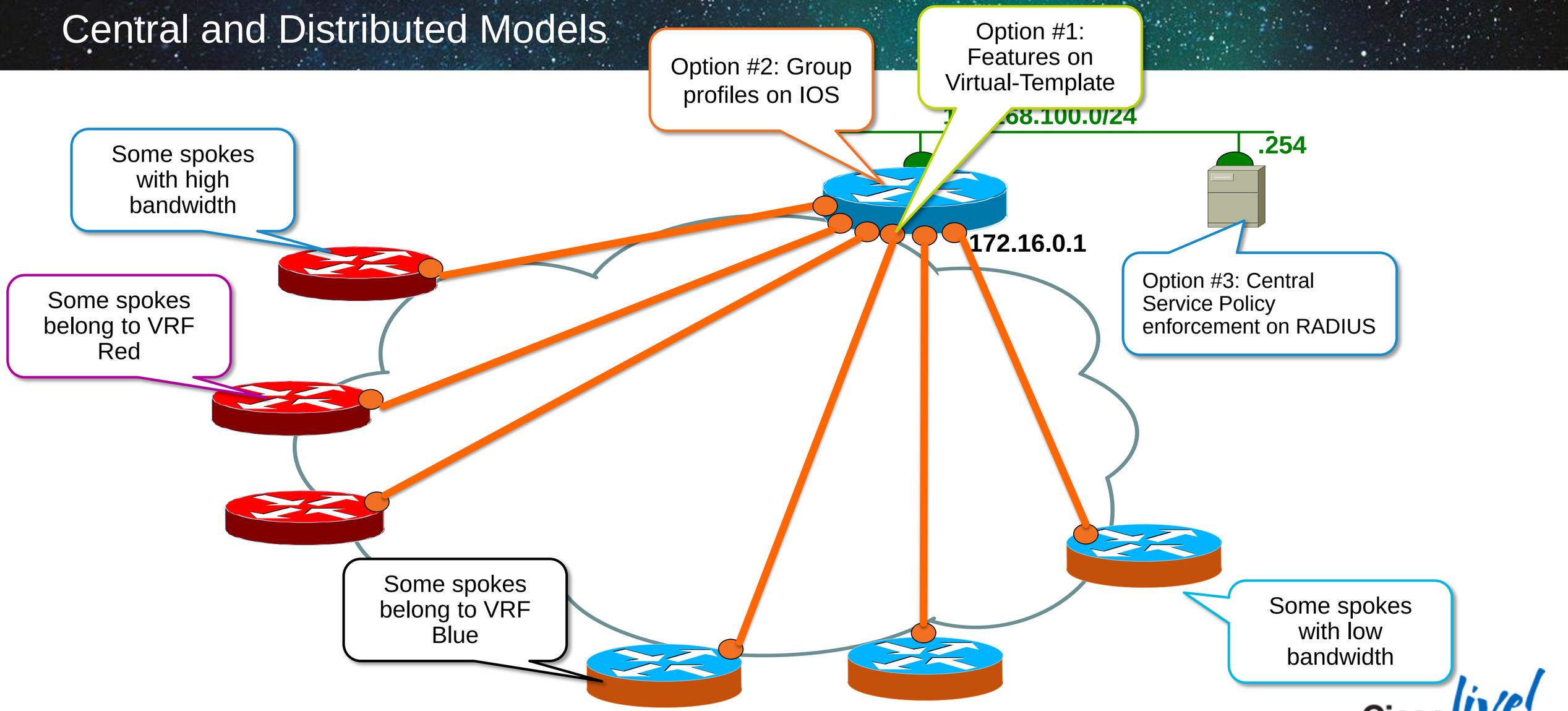
QoS can be applied here




FlexVPN, dVTI and AAA

Provisioning Per-Peer Features

Central and Distributed Models



VRF Injection

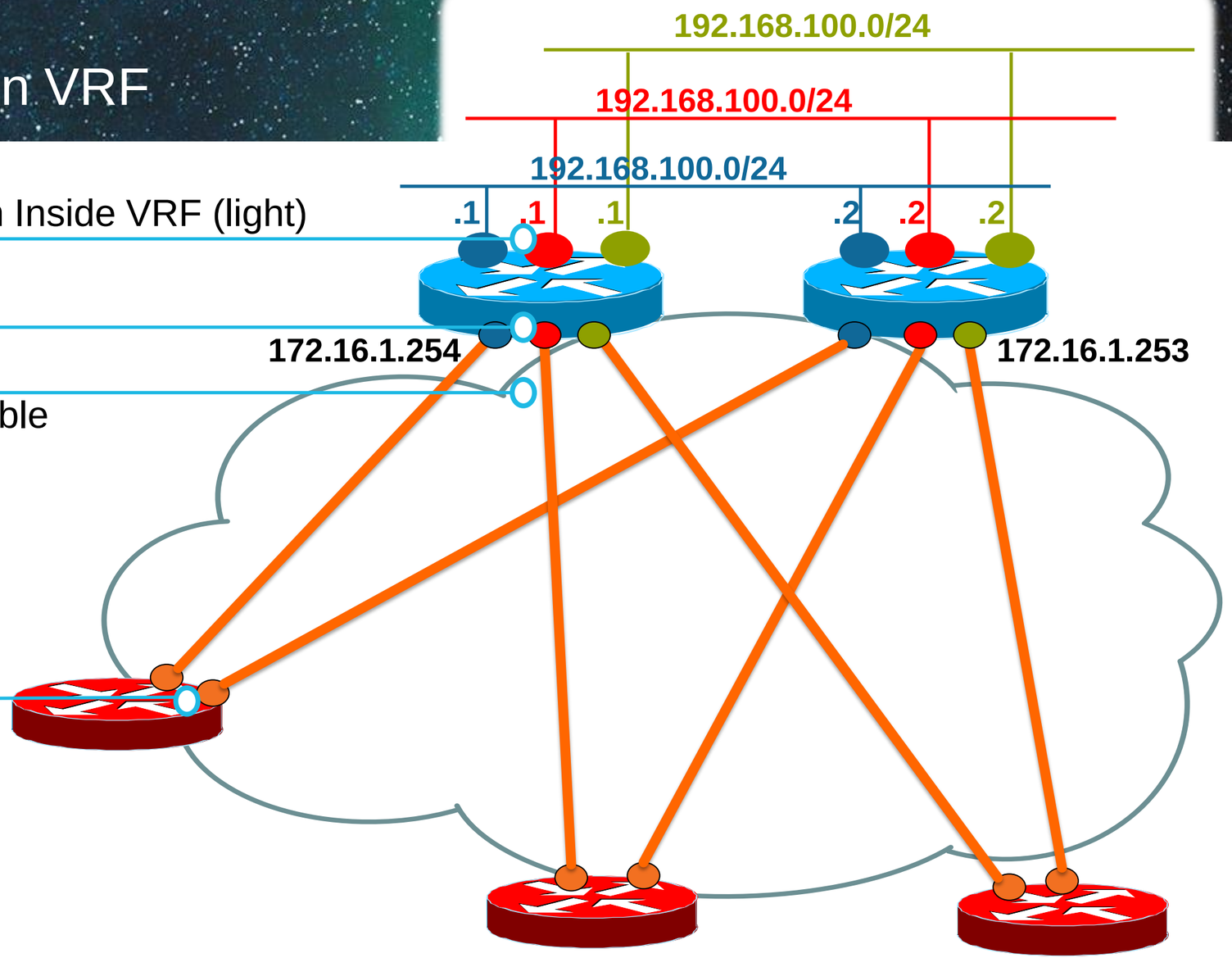
Hub injects traffic in chosen VRF

Hub private interface(s) in Inside VRF (light)

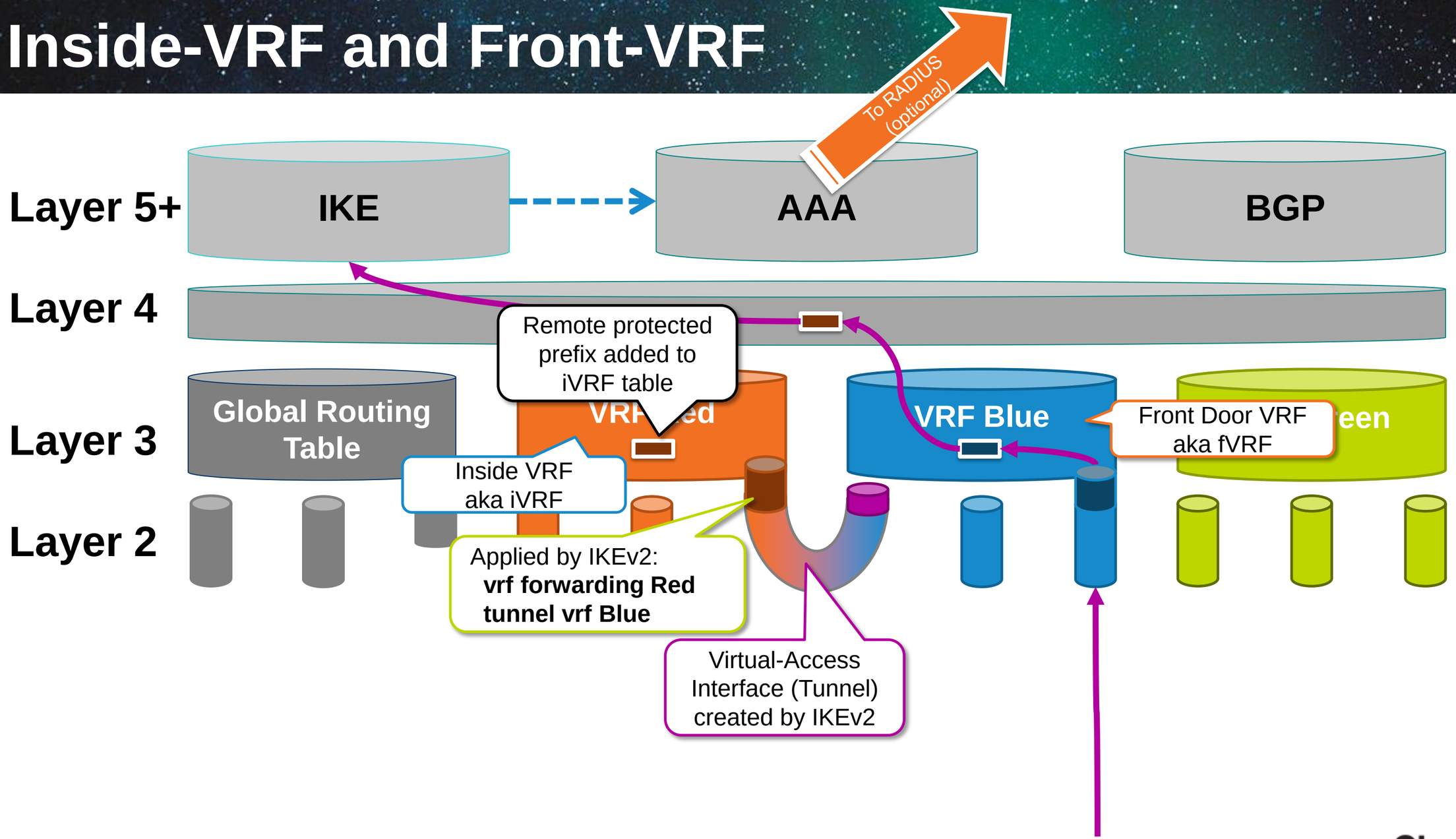
Virtual-Access in iVRF

Wan in Global Routing Table
or Front VRF

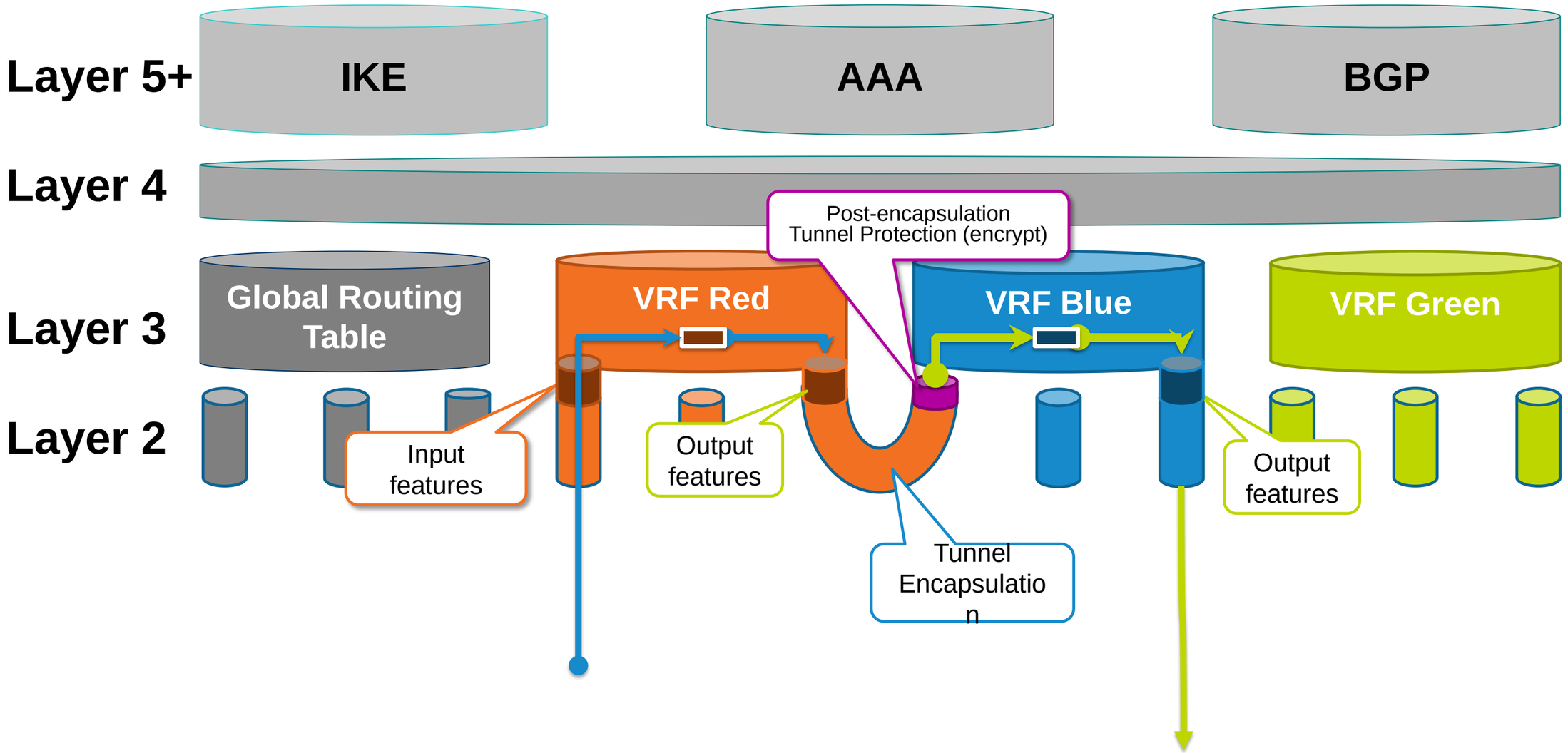
Optional VRF on spokes
(Not in this example)



Inside-VRF and Front-VRF

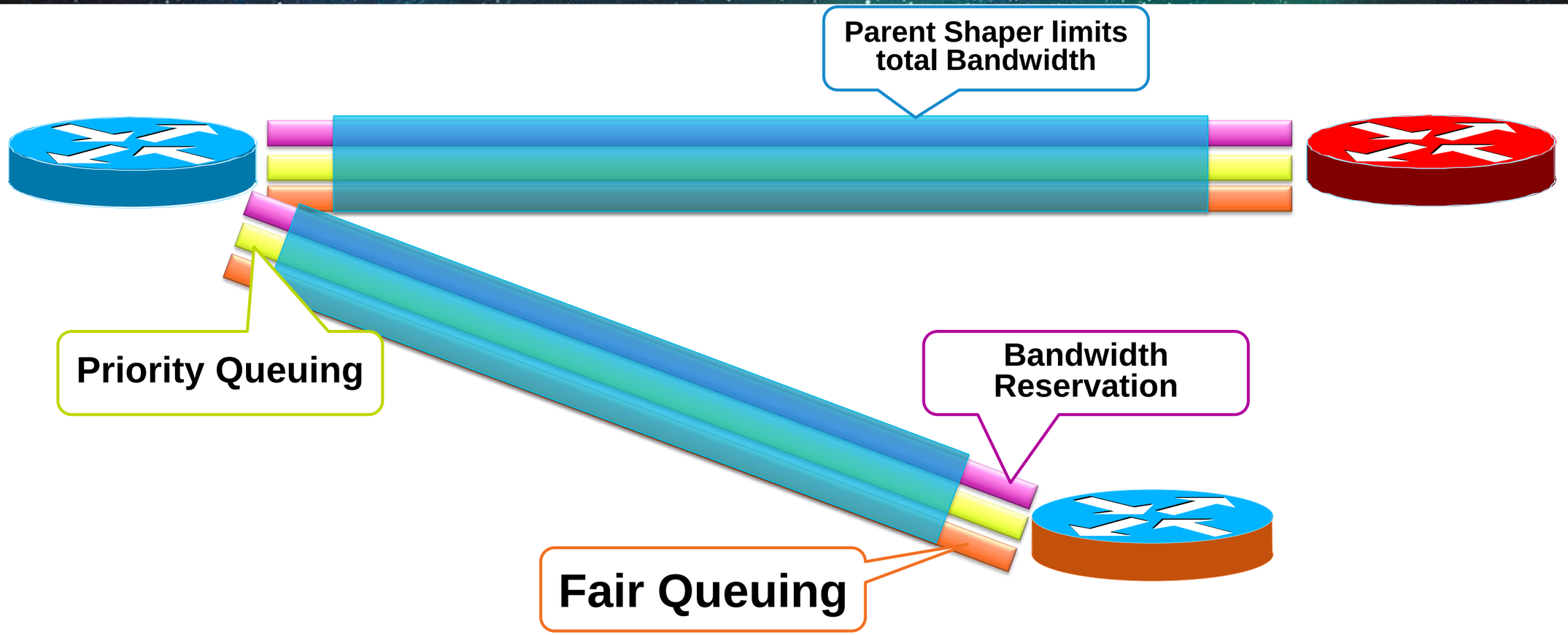


Inside-VRF and Front-VRF

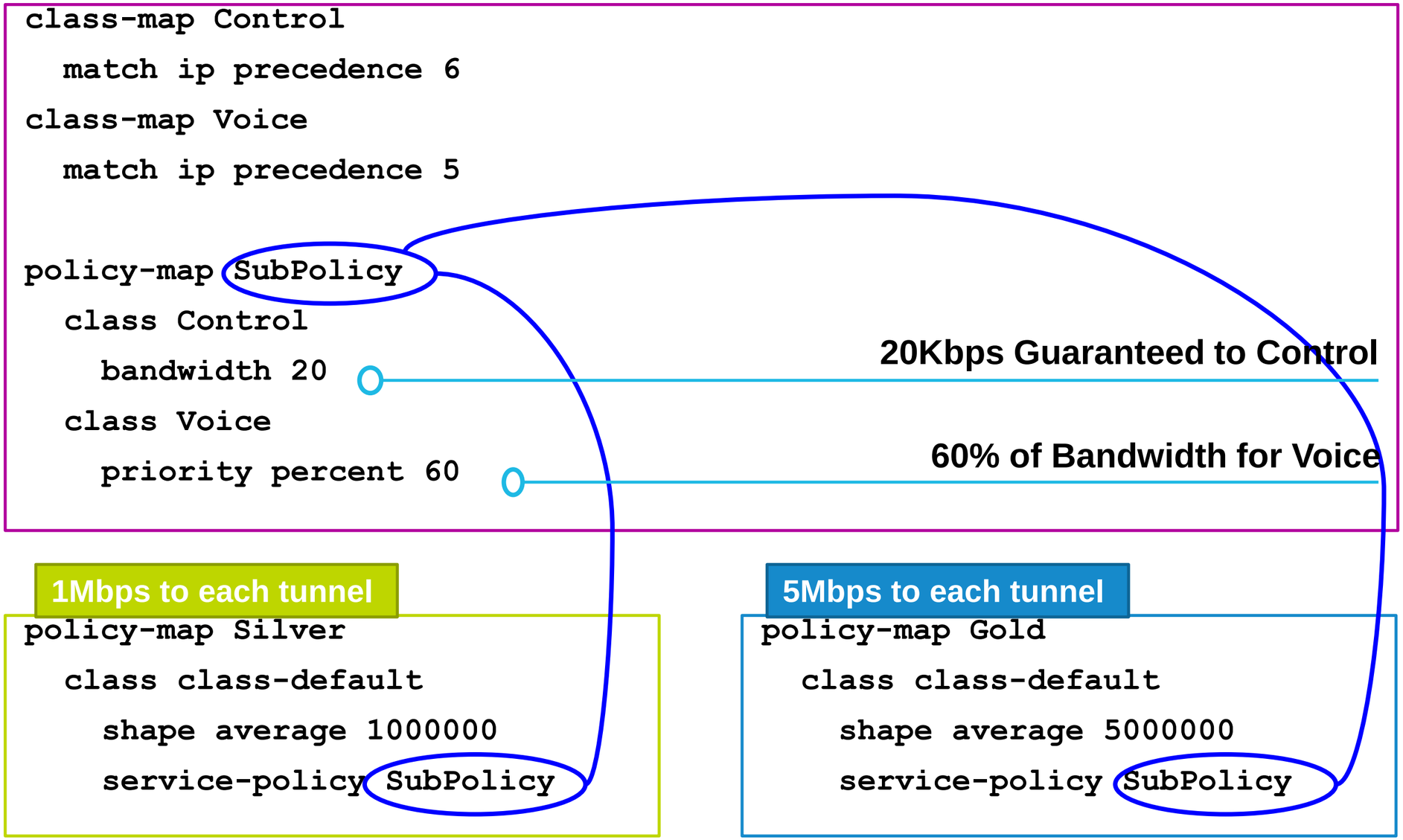


Hierarchical Shaper

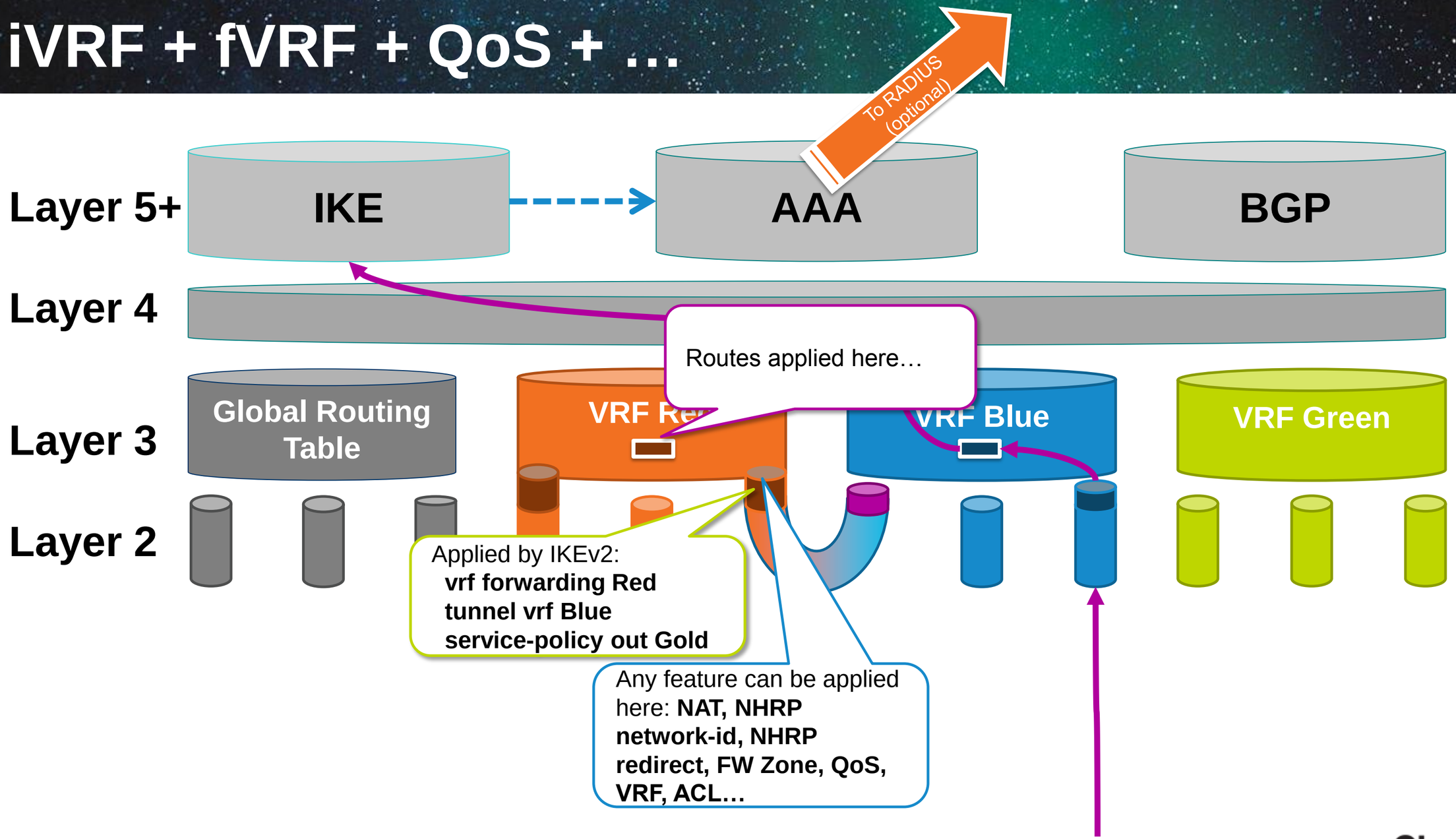
Each Hub V-Access Needs Its Own Policy



Step 1 – Define Policy Map(s)



iVRF + fVRF + QoS + …



VRF Injection – Hub Configuration

Option 1: Mapping with In-IOS configuration (without AAA)

Heavy Configuration

Dedicated IKEv2 profile

```
crypto ikev2 profile BLUE
 match identity fqdn domain blue
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1

interface virtual-template1 type tunnel
 vrf forwarding BLUE
 ip unnumbered loopback1
 service-policy Gold out
 tunnel protection ipsec profile default
```

FQDN Domain is differentiator

Virtual-Template in VRF

Loopback in VRF

Add NHRP, ACL's,…

```
crypto ikev2 profile RED
 match identity fqdn domain red
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 2

interface virtual-template2 type tunnel
 vrf forwarding RED
 ip unnumbered loopback2
  service-policy Gold out
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile GREEN
 match identity fqdn domain green
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 3

interface virtual-template3 type tunnel
 vrf forwarding GREEN
 ip unnumbered loopback3
 service-policy Silver out
 tunnel protection ipsec profile default
```

VRF Injection – Hub Configuration

Option 2: Mapping with AAA group based configuration

Profiles on IOS

Common IKEv2 profile

Profile name extracted from Domain Name

Vanilla Virtual-Template

```
aaa new-model
aaa authorization network default local

crypto ikev2 profile default
 match identity any
 identity local fqdn Hub1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert default name-mangler dom
 virtual-template 1

interface virtual-template1 type tunnel
 tunnel protection ipsec profile default


crypto ikev2 name-mangler dom
  fqdn domain
```

Group profiles on IOS

```
aaa attribute list blue
 attribute type interface-config "vrf forwarding BLUE"
 attribute type interface-config "ip unnumbered loopback1"
 attribute type interface-config "service-policy Gold out"

crypto ikev2 authorization policy blue
 aaa attribute list blue
 route set interface
```

```
aaa attribute list red
 attribute type interface-config "vrf forwarding RED"
 attribute type interface-config "ip unnumbered loopback2"
 attribute type interface-config "service-policy Silver out"

crypto ikev2 authorization policy red
 aaa attribute list red
 route set interface
```

```
aaa attribute list green
 attribute type interface-config "vrf forwarding GREEN"
 attribute type interface-config "ip unnumbered loopback3"
 attribute type interface-config "service-policy GOLD out"

crypto ikev2 authorization policy green
 aaa attribute list green
 route set interface
```

VRF Injection – Hub Configuration

Option 3: RADIUS based profiles

Profiles stored on RADIUS server

Common IKEv2 profile

Profile name extracted from Domain Name

Vanilla Virtual-Template

```
aaa new-model
aaa authorization network default group RADIUS
aaa group server radius RADIUS
 server-private 192.168.100.2 auth-port 1812
                acct-port 1813 key cisco123

crypto ikev2 profile default
 match identity any
 identity local fqdn Hub1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert default name-mangler
dom
 virtual-template 1

interface virtual-template1 type tunnel
 tunnel protection ipsec profile default

crypto ikev2 name-mangler dom
  fqdn domain
```

Group profiles on RADIUS
Could be per peer profiles
or group+peer (derivation)

Profile “**blue**” / password “cisco”
ipsec:route-accept=any
ipsec:route-set=interface
ip:interface-config=“**vrf forwarding BLUE**”
ip:interface-config=“**ip unnumbered loopback 1**”
ip:interface-config=“**service-policy Gold out**”

Profile “**red**” / password “cisco”
ipsec:route-accept=any
ipsec:route-set=interface
ip:interface-config=“**vrf forwarding RED**”
ip:interface-config=“**ip unnumbered loopback 2**”
ip:interface-config=“**service-policy Silver out**”

Profile “**green**” / password “cisco”
ipsec:route-accept=any
ipsec:route-set=interface
ip:interface-config=“**vrf forwarding GREEN**”
ip:interface-config=“**ip unnumbered loopback 3**”
ip:interface-config=“**service-policy Gold out**”

RADIUS Group Profiles

VRF Injection – Hub Configuration

For both options: BGP and VRF configurations

For Your Reference

Attract summaries and drops non-reachable prefixes

BGP dynamic peering

These address can not currently overlap

Follow **CSCtw69765**.

Each VRF has its own control section.

Activate peer group in its corresponding VRF

Redistributes above statics into BGP

```
ip route vrf BLUE 10.0.0.0 255.0.0.0 Null0
ip route vrf BLUE 192.168.0.0 255.255.0.0 Null0

ip route vrf RED 10.0.0.0 255.0.0.0 Null0
ip route vrf RED 192.168.0.0 255.255.0.0 Null0

ip route vrf GREEN 10.0.0.0 255.0.0.0 Null0
ip route vrf GREEN 192.168.0.0 255.255.0.0 Null0

router bgp 1
 bgp listen range 10.1.0.0/16 peer-group BluePeer
 bgp listen range 10.2.0.0/16 peer-group RedPeer
 bgp listen range 10.3.0.0/16 peer-group GreenPeer
 !
 address-family ipv4 vrf BLUE
  redistribute static
  neighbor BluePeer peer-group
  neighbor BluePeer remote-as 1
 exit-address-family
 !
 address-family ipv4 vrf RED
  redistribute static
  neighbor RedPeer peer-group
  neighbor RedPeer remote-as 1
 exit-address-family
 !
 address-family ipv4 vrf GREEN
  redistribute static
  neighbor GreenPeer peer-group
  neighbor GreenPeer remote-as 1
 exit-address-family
```

```
vrf definition BLUE
 rd 1:1
 address-family ipv4
 address-family ipv6

interface Loopback1
 vrf forwarding BLUE
 ip address 10.0.0.254 255.255.255.255
```

```
vrf definition RED
 rd 2:2
 address-family ipv4
 address-family ipv6

interface Loopback2
 vrf forwarding RED
 ip address 10.0.0.254 255.255.255.255
```

```
vrf definition GREEN
 rd 3:3
 address-family ipv4
 address-family ipv6

interface Loopback3
 vrf forwarding GREEN
 ip address 10.0.0.254 255.255.255.255
```

VRF Injection – Spoke Configuration

Vanilla IKE and BGP configurations

For Your Reference

Profiles stored on RADIUS server

Plain simple IKEv2 profile

IKEv2 Identity Defines Group

Just necessary for config exchange

Tunnel to Hub1

Tunnel to Hub2

```
aaa new-model
aaa authorization network default local

crypto ikev2 profile default
 match identity remote fqdn Hub1.cisco.com
 match identity remote fqdn Hub2.cisco.com
 identity local fqdn spoke1.RED
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
!
interface Loopback0
 ip address 10.1.0.2 255.255.255.255
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel destination 172.16.4.1
 tunnel protection ipsec profile default
```

Basic iBGP configuration

```
router bgp 1
 bgp log-neighbor-changes
 network 192.168.0.0 mask 255.255.0.0
 neighbor Hub peer-group
 neighbor Hub remote-as 1
 neighbor Hub next-hop-self
 neighbor 10.0.0.253 peer-group Hub
 neighbor 10.0.0.254 peer-group Hub
 maximum-paths ibgp 2
```

iBGP

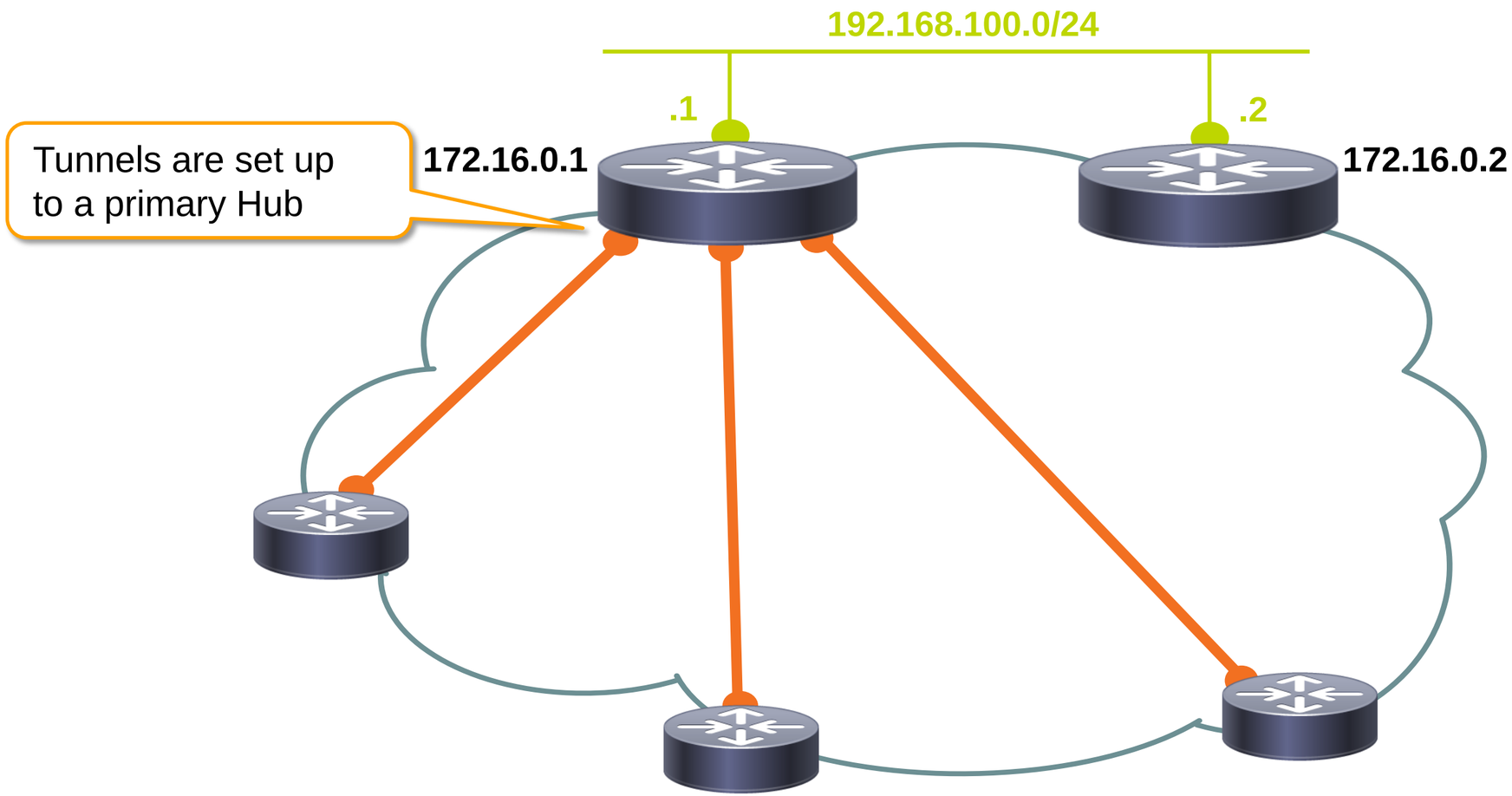
Two Hubs…

Equal Cost Load Balancing

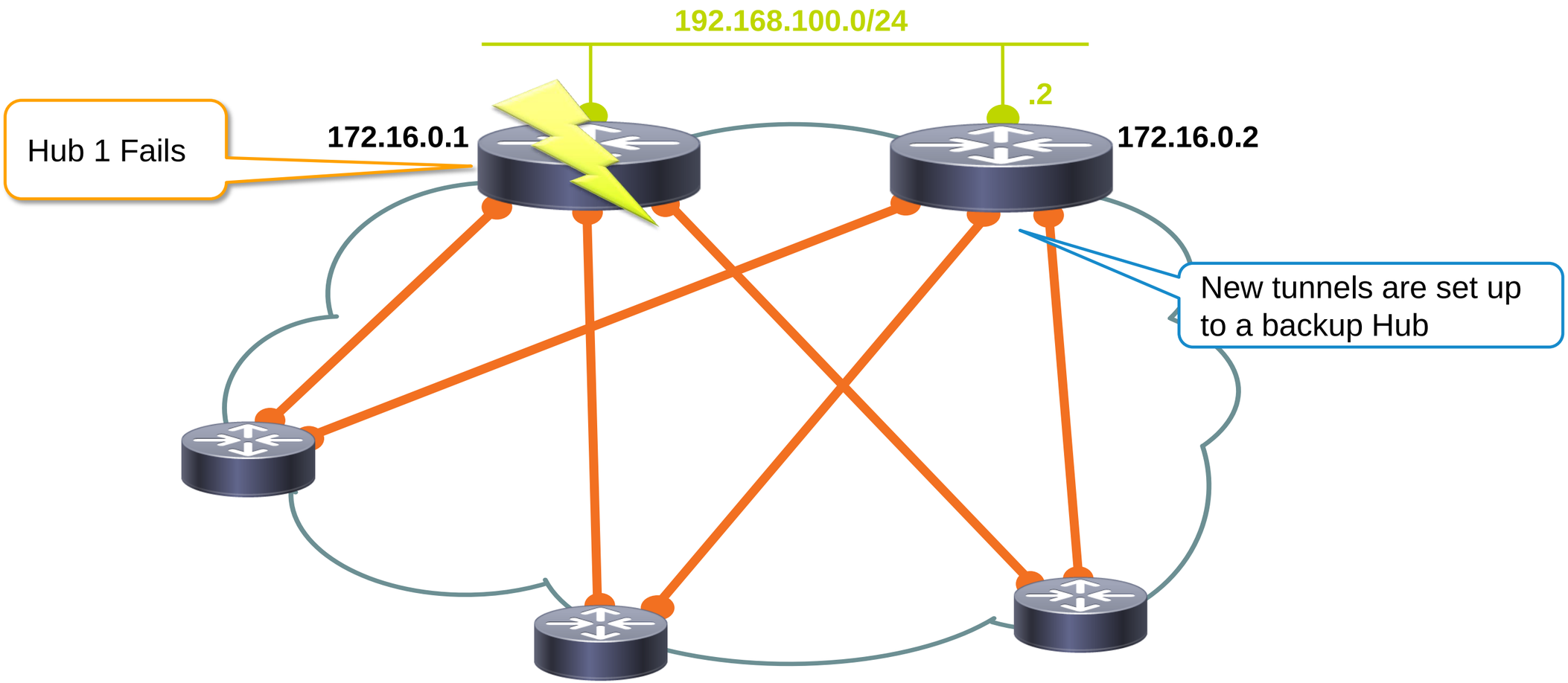



Backup Mechanisms

FlexVPN Backup
IKE Backup Peers (1)



FlexVPN Backup
IKE Backup Peers (2)



FlexVPN Backup
IKE Backup Peers (3) – Spoke Config.

Also works with Routing Protocol

```
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 <n> <ip>
peer <n> <ip> track <x>
peer <n> <fqdn>
peer <n> <fqdn> track <x>
```

Nth source selected only if corresponding track object is up

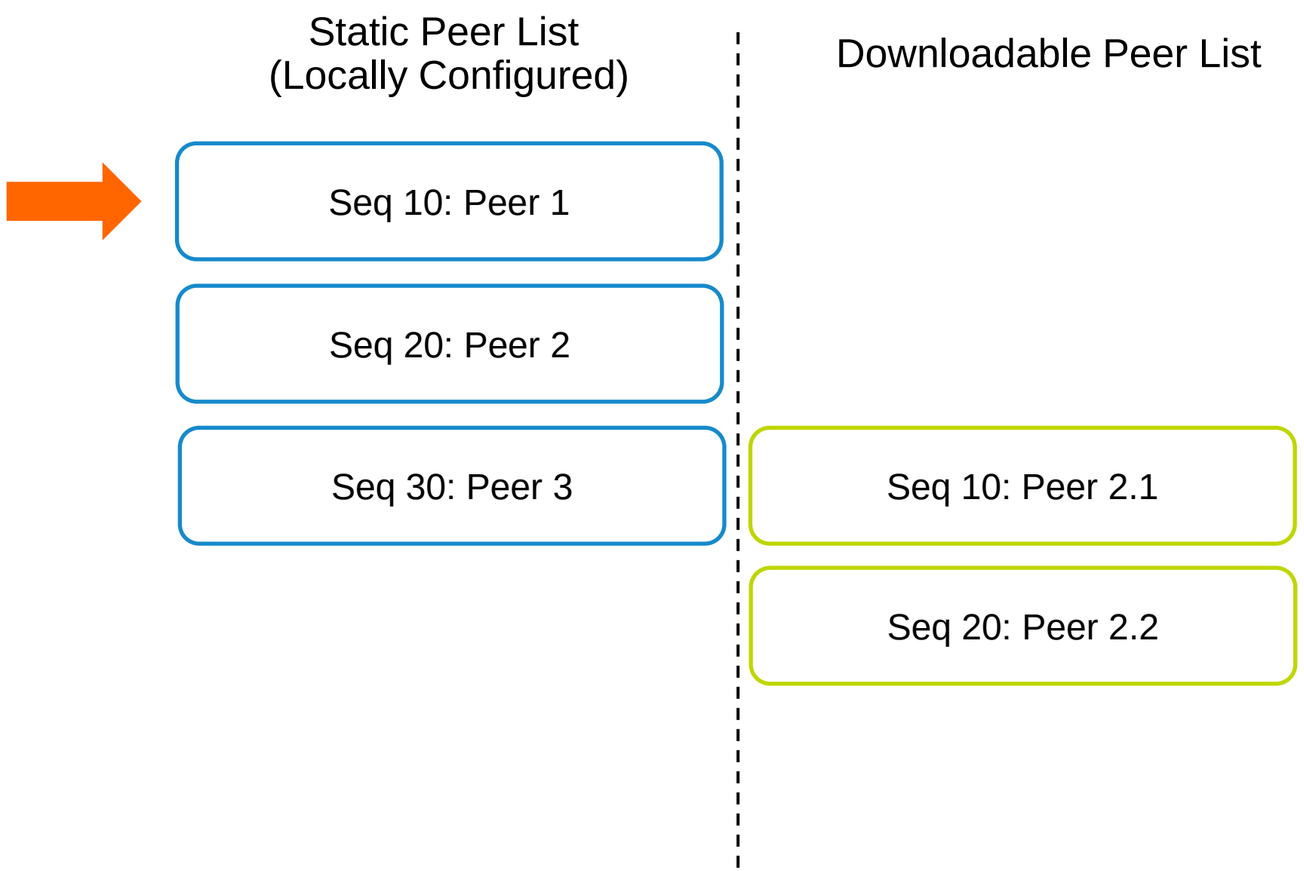
RADIUS Backup List Attribute

`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
```

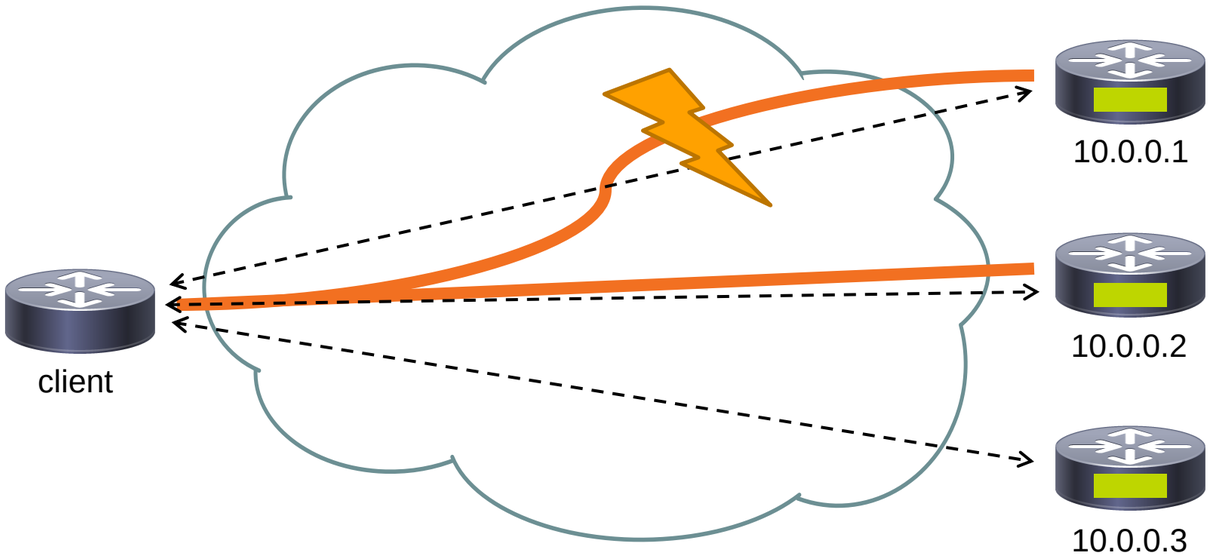
FlexVPN Backup – Downloadable Backup Peer List



- Peer 1 is selected initially (sequence number based)
- If Peer 1 fails, Peer 2 is selected (sequence number based)
- Upon connection to Peer 2, a downloadable peer list is received
- Upon failure of Peer 2, Peer 2.1 then 2.2 are selected (part of downloadable peer list)
- Downloadable list peers are used until last downloadable list peer fails

FlexVPN Backup – Re-activation of Primary Peer

- Allow re-establishing tunnel directly to preferred peer as soon as it is available again
- **Trackers are required for this feature**



Tracker state (Up/Down)

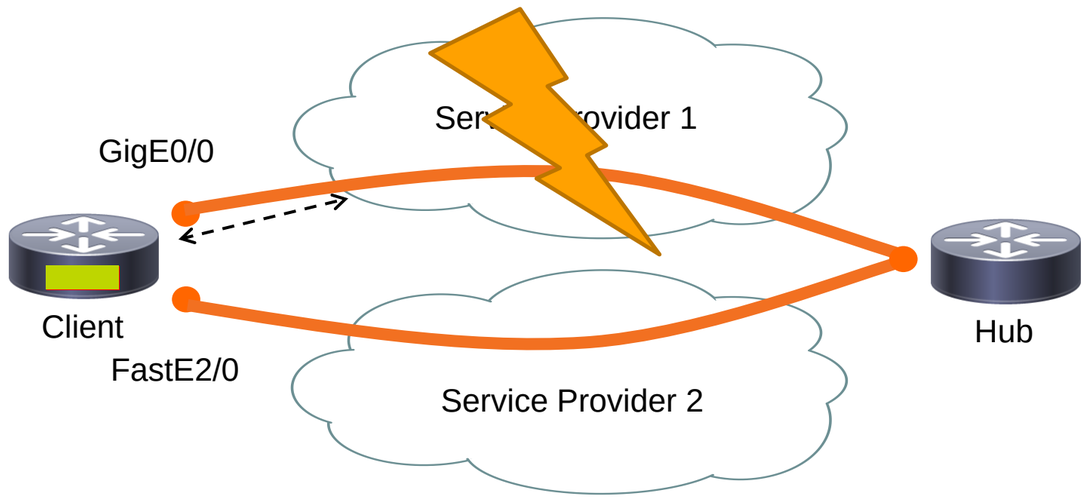
ICMP-echo IP SLA probe

IPsec Tunnel

```
track 1 ip sla 1 reachability
track 2 ip sla 2 reachability
track 3 ip sla 3 reachability
!
crypto ikev2 flexvpn client remote1
  peer 1 10.0.0.1 track 1
  peer 2 10.0.0.2 track 2
  peer 3 10.0.0.3 track 3
  peer reactivate
  client connect Tunnel0
!
interface Tunnel0
  ip address negotiated
  …
  tunnel destination dynamic
  …
```

FlexVPN Backup – Tunnel Pivoting

- 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
   …
```

Tracker state (Up/Down)

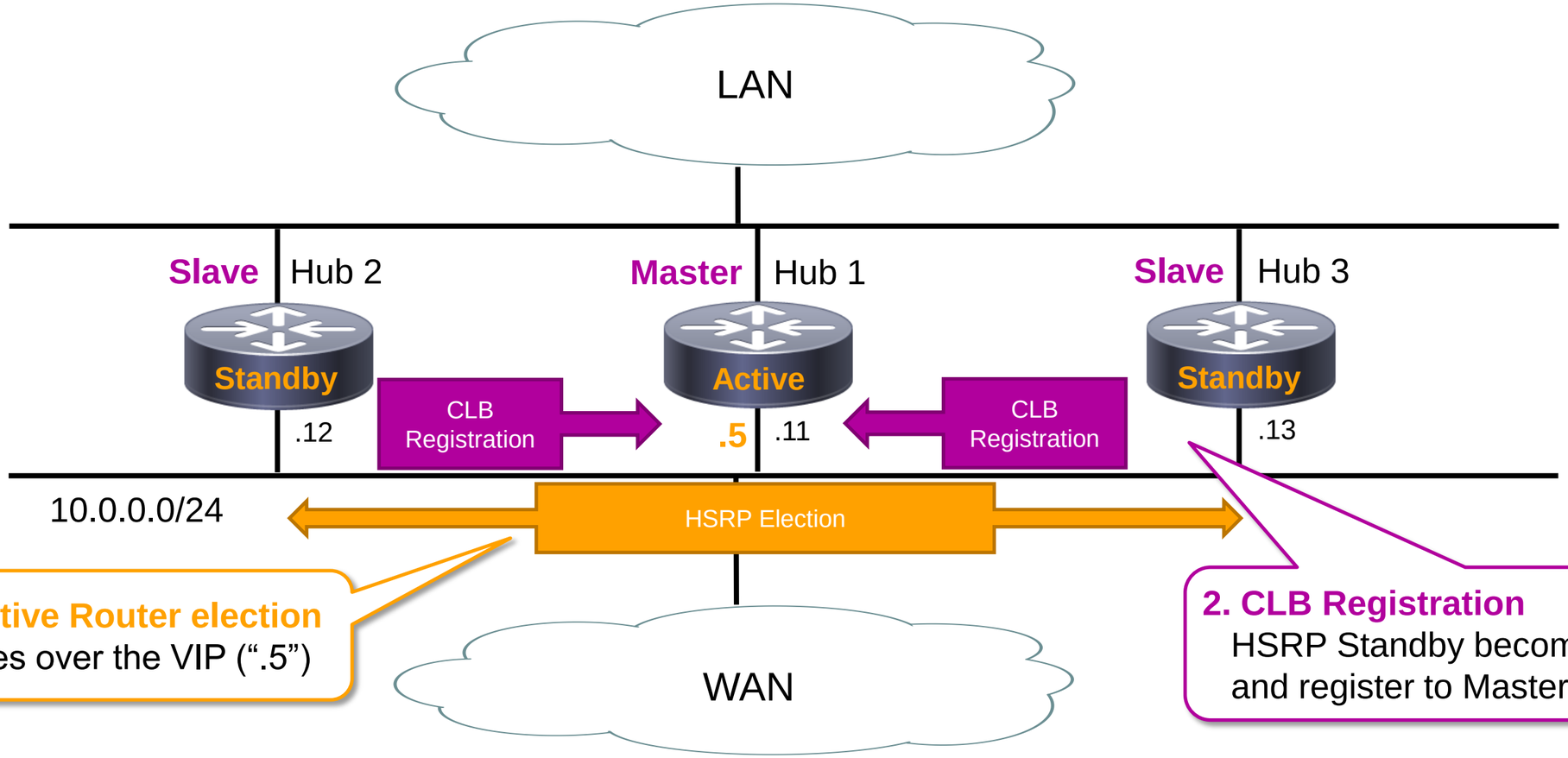
ICMP-echo IP SLA probe

IPsec Tunnel




IKE Load Balancer

FlexVPN Backup
IKEv2 Load-Balancer Bootstrap

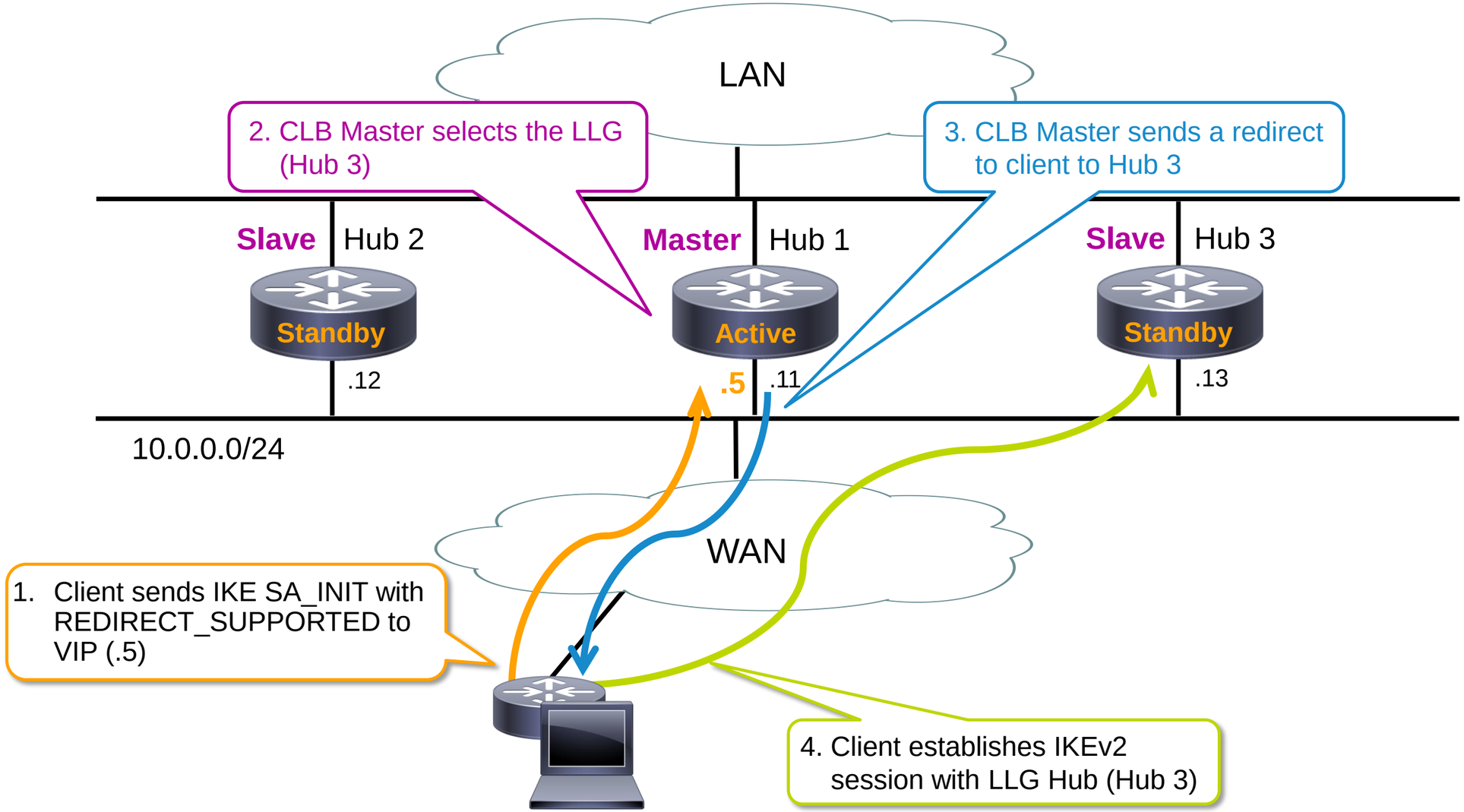


1. HSRP Active Router election
Winner takes over the VIP (".5")

2. CLB Registration
HSRP Standby become CLB Slaves and register to Master (HSRP Active)

```
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.
```

FlexVPN Backup
IKEv2 Load-Balancer Client Connection



IKEv2 Load-Balancer
Hub 1 Configuration

```
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 10.0.0.11 255.255.255.0
 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

- Configuration of slave hubs is almost identical (except HSRP priority)!

IKEv2 Load-Balancer
Client Configuration

```
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**

FlexVPN Backup
IKEv2 Load-Balancer

For Your Reference

- 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

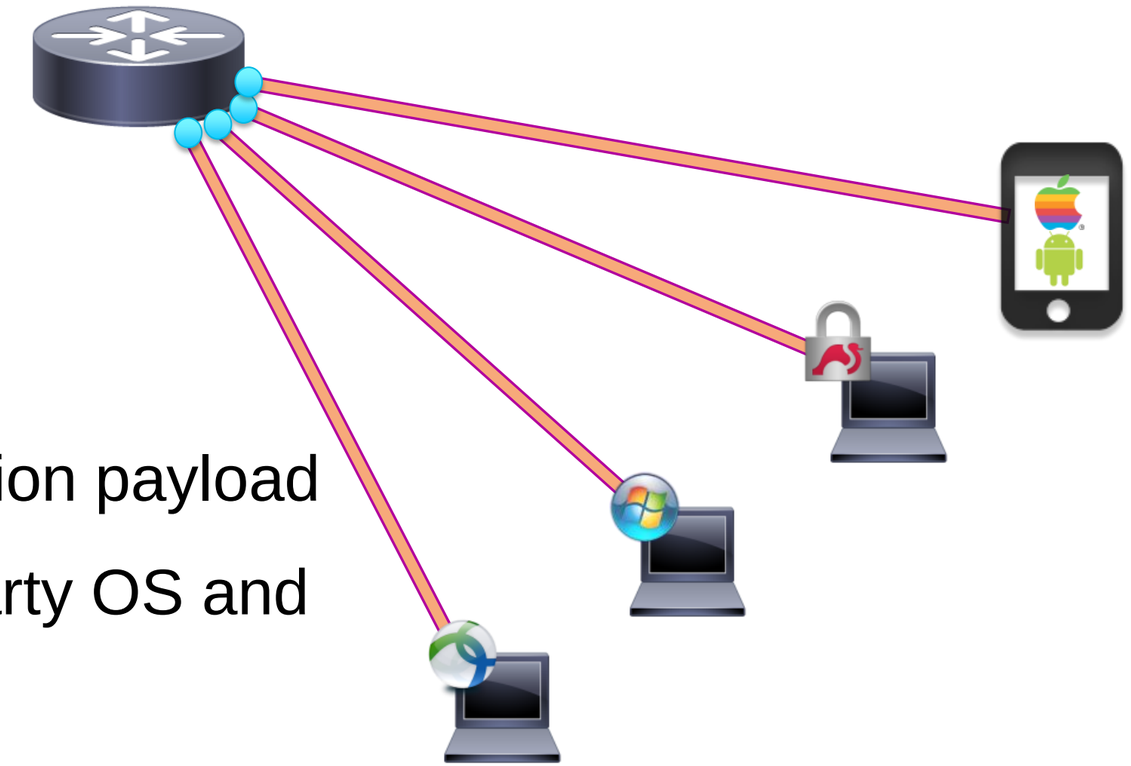



FlexVPN Remote Access

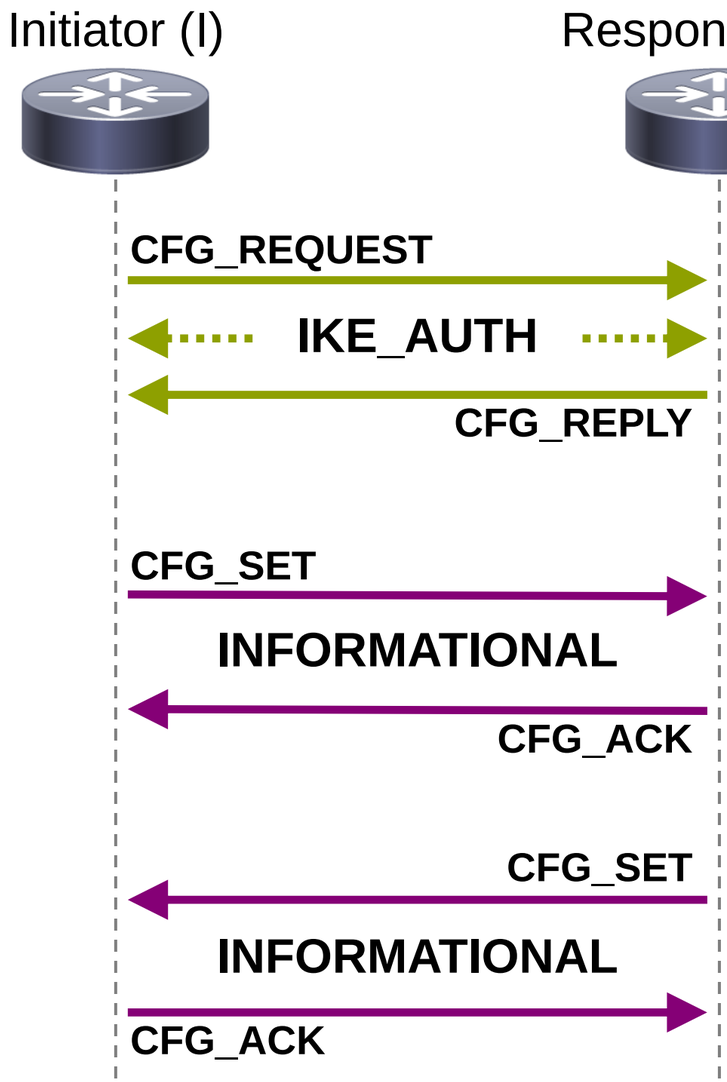
Example with AnyConnect 3.0 for Mobile

FlexVPN Software Client Remote Access

- Remote clients need additional information that aren't usually exchanged:
  - IP address
  - Routes (Split tunnel)
  - DNS servers
  - Domain names
- Exchange handled by IKEv2 configuration payload
- Allows easy integration of many third party OS and clients.



IKEv2 Configuration Exchange



Initiator (RA client) requests configuration parameters from responder (RA server).

I would like:
- ✓ an IPv6 address
- ✓ a DNS & WINS server
- ✓ a list of protected IPv6 subnets

- ✓ Your assigned IPv6 address is ...
- ✓ Your DNS server is ...
- ✖ There is no WINS server
- ✓ My protected IPv6 subnets are ...

Derived from peer authorisation

Initiator and/or responder sends unsolicited configuration parameters to its peer.

Derived from peer authorisation

- ✓ My local IPv6 protected subnets are ...

- ✓ Acknowledged

EAP Authentication

RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

IKE

AAA Server
RADIUS Server
EAP Backend

```
crypto ikev2 profile default
 authentication remote eap query-identity
 aaa authentication eap frad
```

RA server authenticates to client using IKE certificates (mandatory)

Username-Password/Token/Mobile Authentication (One-Way)

TLS

TLS

TLS-Based Certificate Authentication (Mutual)

TLS

TLS

TLS-Protected Nested Authentication (One-Way or Mutual)

EAP Authentication – Packet Flow

RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend

```
crypto ikev2 profile default
 authentication remote eap query-identity
 aaa authentication eap frad
```

IKEv2 (IKE_AUTH)
IDi, CFG_REQ, no AUTH

IKEv2 (IKE_AUTH)
IDr, AUTH(RSA), EAP(ID-Request)

IKEv2 (IKE_AUTH)
EAP(ID-Response: ID_{EAP})

RADIUS (Access-Request)

IKEv2 (IKE_AUTH)
EAP(EAP-Method-Pkt#1)

RADIUS (Access-Challenge)

IKEv2 (IKE_AUTH)
EAP(EAP-Method-Pkt#2)

RADIUS (Access-Request)

MSK

MSK

IKEv2 (IKE_AUTH)
EAP(Success)

RADIUS (Access-Accept)
EAP(Success), MSK, User-Name,
Other user attributes

EAP Username

Cached for authorisation

IKEv2 (IKE_AUTH)
AUTH(MSK)

IKEv2 (IKE_AUTH)
CFG_REPLY, AUTH(MSK)

AnyConnect – Certificate Requirements

For Your Reference

	AnyConnect Client IKEv2 Certificate	FlexVPN Server IKEv2 Certificate
Used for	Mutual RSA-SIG	Mutual RSA-SIG EAP (all types)
Common Name (CN)	Anything	Anything (if SAN field present) Server FQDN (if no SAN field)
Key Usage (KU)	Digital Signature	Digital Signature Key Encipherment or Key Agreement
Extended Key Usage (EKU)	Optional[1,3] If present: TLS Client Authentication	Optional[2,3] If present: TLS Server Authentication or IKE Intermediate
Subject Alternative Name (SAN)	Not required[3]	Optional[3] If present: Server FQDN

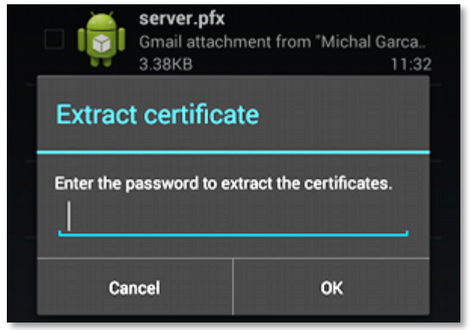
[1] Required in AC 3.0.8 to 3.0.10 (CSCuc07598)

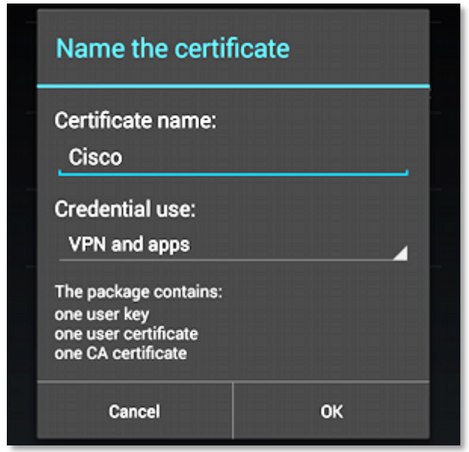
[2] Required in AC 3.0 (all versions), lifted in 3.1

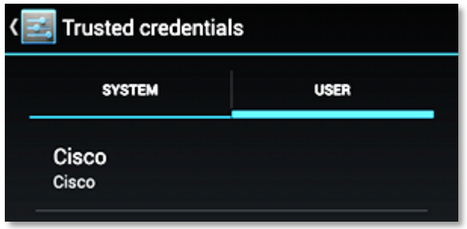
[3] Not required: may be omitted or set to any value – Optional: may be omitted or set to the specified value

AnyConnect Mobile – Certificate Deployment

- Package certificate & keypair into PKCS#12 file
- Apple iOS
  - Import PKCS#12 from URL or email attachment
  - Provision credentials or set up SCEP enrollment using configuration profile (e.g. via iPhone Configuration Utility)
- Android
  - Import PKCS#12 from URL, email or filesystem
  - Use existing credentials from Credential Storage





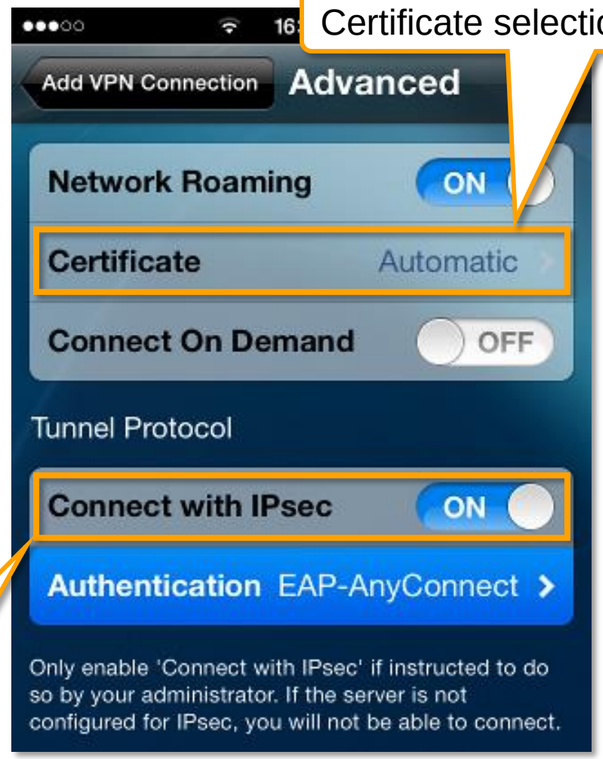


AnyConnect Mobile – Manual Connection

Create new manual connection

Connection name

Server FQDN

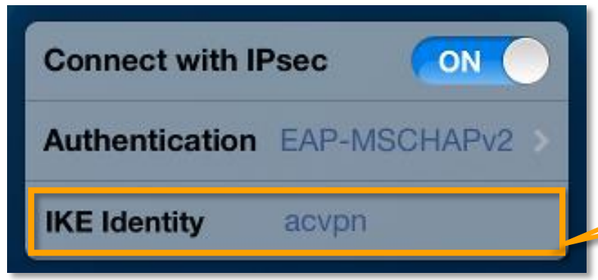


Certificate selection

Enable IKEv2

Cisco ASA only

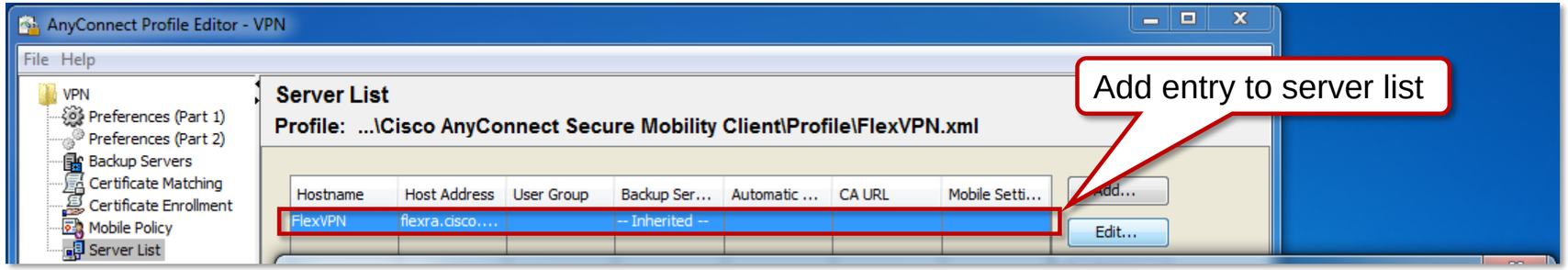
Select authentication method

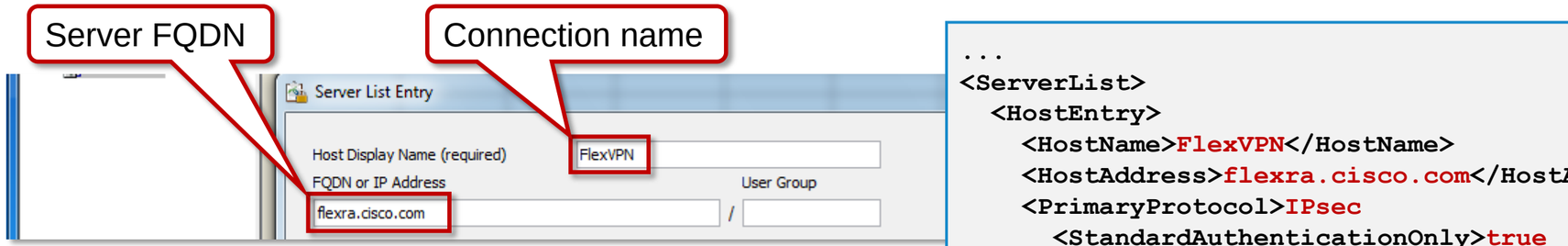


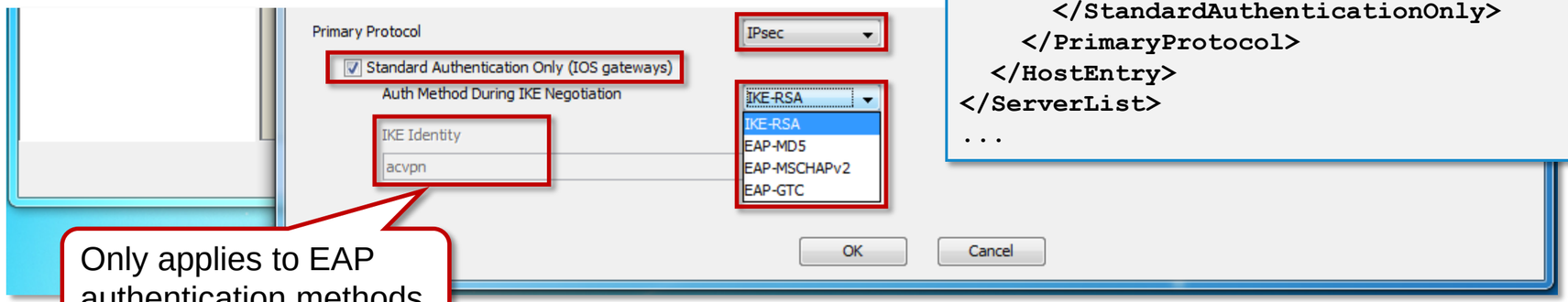
Specify IKE ID for EAP methods

AnyConnect – VPN Profile Editor

For Your Reference







Resulting XML Profile

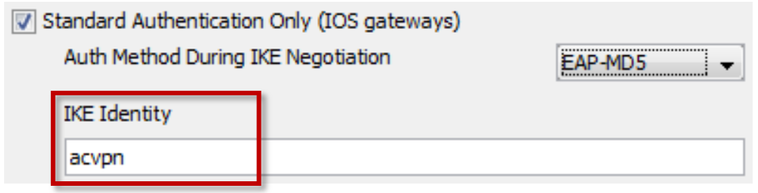
```
...
<ServerList>
  <HostEntry>
    <HostName>FlexVPN</HostName>
    <HostAddress>flexra.cisco.com</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>true
        <AuthMethodDuringIKENegotiation>EAP-GTC</AuthMethodDuringIKENegotiation>
        <IKEIdentity>acvpn</IKEIdentity>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
...
```

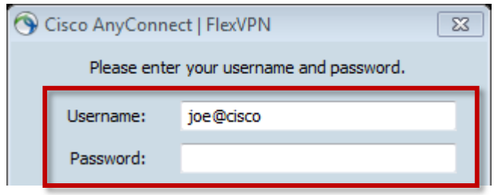
AnyConnect Headend Config – EAP (All Methods)

- EAP-GTC / EAP-MD5 / EAP-MSCHAPv2
  - Client IKE ID = KEY-ID string configured in XML profile
  - Server selects IKEv2 profile based on KEYID string
  - EAP “query-identity” prompts user for credentials
  - EAP ID = username entered by user
  - Password authentication against AAA user database
  - Returned attributes cached for implicit authorisation

```
aaa group server radius frad
 server-private 172.16.0.254 key cisco
aaa authentication login frad group frad

crypto ikev2 profile default
 match identity remote key-id acvpn
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint root sign
 aaa authentication eap frad
 aaa authorization user eap cached
 virtual-template 1
```






```
# RADIUS User definition
joe@cisco
  Cleartext-Password := "c1sc0!"
  Framed-IP-Address = "10.0.1.101",
  Framed-IP-Netmask = "255.255.255.255",
  Cisco-AVPair = "ipsec:dns-servers=10.0.1.1"
```




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	

High-End Scalability & Performances → 3.11

Tentative

Release 3.5+ w/out QoS	ASR1001	ASR1002-F	ASR1000-ESP5	ASR1000-ESP10	ASR1000-ESP20	ASR1000-ESP40	ASR1000-ESP100
Throughput (Max / IMIX)	1.8 / 1Gbps	1 / 0.8 Gbps	1.8 / 1 Gbps	4 / 2.5 Gbps	7 / 6 Gbps	11 / 7.4 Gbps	29 / 16 Gbps
Max tunnels (RP1 / RP2)	4000	1000	1000	1000 / 4000	1000 / 4000	1000 / 4000	-- / 4000
EIGRP neighbours	4000 (1000 recommended)	1000	1000	1000 / 4000 (1000 recommended)	1000 / 4000 (1000 recommended)	1000 / 4000 (1000 recommended)	-- / 4000 (1000 recommended)
BGP neighbours	**4000**	**1000**	**1000**	**1000 / 4000**	**1000 / 4000**	**1000 / 4000**	**-- / 4000**

Release 3.5 w/ QoS	ASR1001	ASR1000-ESP20	ASR1000-ESP40
Throughput (Max / IMIX)	1.8 / 1Gbps	7 / 6 Gbps	11 / 7.4 Gbps
Max tunnels (RP2 only)	4000* (16K Queues)	4000 (128K Queues)	4000 (128K Queues)

4000 tentative

High-End Scalability & Performances – 3.12

Tentative

Release 3.5+ w/out QoS	ISR 4451	ASR1001	ASR1000-ESP5	ASR1000-ESP10	ASR1000-ESP20	ASR1000-ESP40	ASR1000-ESP100
Throughput (Max / IMIX)	1.2 / 0.8Gbps	1.8 / 1Gbps	1.8 / 1 Gbps	4 / 2.5 Gbps	7 / 6 Gbps	11 / 7.4 Gbps	29 / 16 Gbps
Max tunnels (RP1 / RP2)	2000	4000	1000	1000 / **10,000**	1000 / **10,000**	1000 / **10,000**	-- / **10,000**
EIGRP neighbours	2000 (1000 recommended)	4000 (1000 recommended)	1000	1000 / 4000 (1000 recommended)	1000 / 4000 (1000 recommended)	1000 / 4000 (1000 recommended)	-- / 4000 (1000 recommended)
IKE Routing	**2000**	4000	1000	**10,000**	**10,000**	**10,000**	**10,000**
BGP neighbours	**2000**	4000	1000	**1000 / 10,000**	**1000 / 10,000**	**1000 / 10,000**	**-- / 10,000**

Bumping from 4,000 to 10,000 spokes/hub with FlexVPN in 3.12 (RP2 only)

Release 3.10 w/ QoS	ISR 4451	ASR1001	ASR1000-ESP20	ASR1000-ESP40
Throughput (Max / IMIX)	1.2 / 0.8 Gbps	1.8 / 1 Gbps	7 / 6 Gbps	11 / 7.4 Gbps
Max tunnels (RP2 only)	**2000**	4000* (16K Queues)	**10,000** (128K Queues)	**10,000** (128K Queues)

FlexVPN - ISR G2 Scalability

Tentative

Platform	Sec-K9		SEC-K9 + HSEC-K9	
	Recommended	Max	Recommended	Max
3945E	Up to 225	Up to 225	Up to 2000	Up to 3000
3925E	Up to 225	Up to 225	Up to 1500	Up to 3000
3945	Up to 225	Up to 225	Up to 1000	Up to 2000
3925	Up to 225	Up to 225	Up to 750	Up to 1500
2951	Up to 225	Up to 225	Up to 500	Up to 1000
2921	Up to 225	Up to 225	Up to 400	Up to 900
2911	Up to 225	Up to 225	HSEC-K9 license does not apply since the max. encrypted tunnel count is below the restricted limits.	
2901	Up to 150	Up to 225		
1941	Up to 150	Up to 225		
1921	TBD	TBD		

Per-Tunnel QoS: divide by 10

FlexVPN - ISR G2 Performances

75% CPU, IMIX, IPsec/AES, single tunnel

Tentative

Platform	Sec-K9 (Mbps)		C-K9 + HSEC-K9 (Mbps)	
	Recommended	Max	Recommended	Max
3945E	Up to 170	Up to 170	Up to 670	Up to 1503
3925E	Up to 170	Up to 170	Up to 477	Up to 1497
3945	Up to 170	Up to 170	Up to 179	Up to 848
3925	Up to 154	Up to 170	Up to 154	Up to 770
2951	Up to 103	Up to 170	Up to 103	Up to 228
2921	Up to 72	Up to 170	Up to 72	Up to 207
2911	Up to 61	Up to 164	HSEC-K9 license does not apply since the max. encrypted tunnel count is below the restricted limits.	
2901	Up to 53	Up to 154		
1941	Up to 48	Up to 156		
1921	Up to 44	N/A		
891	Up to 66	N/A		




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com


CISCO
TM

FlexVPN CCO Documentation

- CCO doc link
  - http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec-flex-vpn-15-mt-book.html
  - Reflects latest release (currently 15.4(1)T)
- Doc organised into chapters
  - FlexVPN Site-Site
  - FlexVPN Server
  - FlexVPN Client
  - FlexVPN Spoke-Spoke
  - FlexVPN Load-Balancer
  - FlexVPN Reconnect
  - Appendix-1: FlexVPN Radius Attributes
  - Appendix-2: Legacy VPNs
- Changes across releases
  - Documentation reflects latest release
  - Behaviour/CLI changes noted in corresponding sections


CISCO
TM