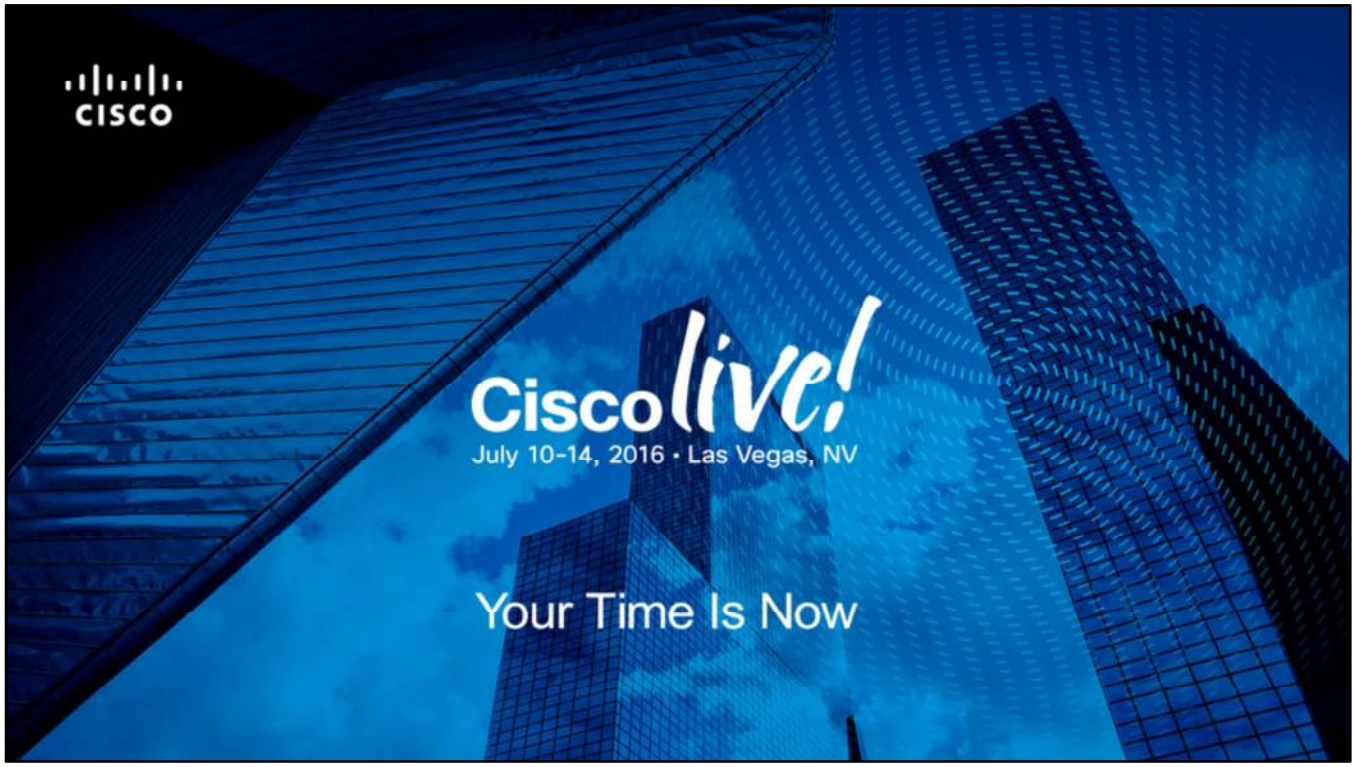
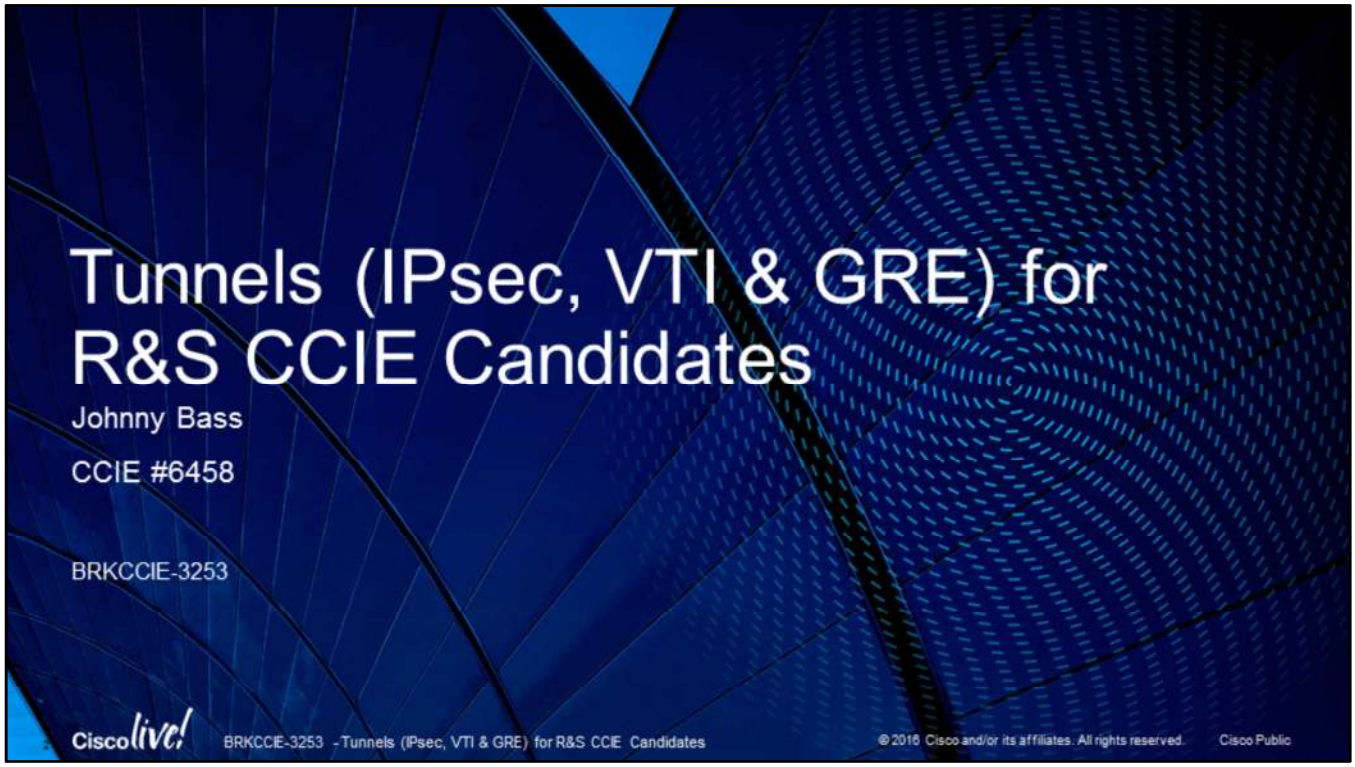

cisco
Cisco live!
July 10-14, 2016 • Las Vegas, NV
Your Time Is Now


Tunnels (IPsec, VTI & GRE) for R&S CCIE Candidates
Johnny Bass
CCIE #6458
BRKCCIE-3253
Ciscolive!
BRKCCIE-3253 - Tunnels (IPsec, VTI & GRE) for R&S CCIE Candidates
© 2016 Cisco and/or its affiliates. All rights reserved.
Cisco Public

About the Presenter

- Johnny Bass
- Networking industry since the late 1980s
- CCIE R&S #6458
- CCSI 97168
- Cisco 360 R&S Master Instructor
- Course director for several programs, including Cisco 360 Route Switch, for Global Knowledge

Johnny Bass has been in the networking industry since the late 1980s, specializing on Cisco System products since 1990 and has worked extensively in the Aerospace, Health Care, and Service Provider industries, providing network design, education, and technical support expertise. Holding both CCIE and CCSI credentials, Johnny has a proven record of teaching and consulting on Cisco Routing, Switching, Design, Implementation, and Support. During his tenure as a Senior Instructor with Global Knowledge, Johnny has developed extensive experience teaching CCNP/CCIP/CCVP/Cisco Nexus and CCIE R&S courses. This experience has also allowed him to excel in the role of Course Director and Subject Matter Expert, with technical responsibility for Global Knowledge's North American CCIE R&S curriculum and Service Provider Technical Segment, including the Cisco CCIE 360 program for Routing and Switching; IPv6 Fundamentals, Design and Development; and the Cisco Service Provider Next Generation Network Operations series of courses. Johnny is also the author of the CCIE Routing & Switching Written Exam Boot Camp currently running for Global Knowledge in Europe. Johnny is a Cisco 360 R&S Master instructor; the first to achieve this level outside of the organization that created the program. In addition to his teaching engagements, Johnny is the owner and President of Bass Consulting Services, Inc, a network engineering consultancy based outside of Seattle, WA specializing with service provider and large enterprise networks for design, configuration, and troubleshooting support. Johnny lives in Gig Harbor Washington with his wife Tiffany, children Sean and Cayman, their cats Gus & Callie and puppy Beignet.

Why Are We Here?

- Because Tunnels and IPsec are on the CCIE Routing & Switching version 5.0 blueprint!

3.1 Tunneling and the CCIE R&S Exam (V5.0)

- 3.1.a Implement and troubleshoot MPLS operations
  - 3.1.a [i] Label stack, LSR, LSP
  - 3.1.a [ii] LDP
  - 3.1.a [iii] MPLS ping, MPLS traceroute
- 3.1.b Implement and troubleshoot basic MPLS L3VPN
  - 3.1.b [i] L3VPN, CE, PE, P
  - 3.1.b [ii] Extranet [route leaking]
- **3.1.c Implement and troubleshoot encapsulation**
  - **3.1.c [i] GRE**
  - **3.1.c [ii] Dynamic GRE**
- 3.1.d Implement and troubleshoot DMVPN [single hub]
  - 3.1.d [i] NHRP
  - 3.1.d [ii] DMVPN with IPsec using preshared key
  - 3.1.d [iii] QoS profile
  - 3.1.d [iv] Pre-classify

3.1 Tunneling and the CCIE R&S Exam (V5.0)

3.1.c Implement and troubleshoot encapsulation
- **3.1.c [i] GRE**
- **3.1.c [ii] Dynamic GRE**

3.2 Encryption and the CCIE R&S Exam (V5.0)

3.2 Encryption

- 3.2.a Implement and troubleshoot IPsec with preshared key
  - 3.2.a [i] IPv4 site to IPv4 site
  - 3.2.b [ii] IPv6 in IPv4 tunnels
  - 3.2.a [iii] Virtual tunneling interface [VTI]

Tunnels & Encryption o the CCIE R&S Exam (V5.0)

3.1 Tunneling

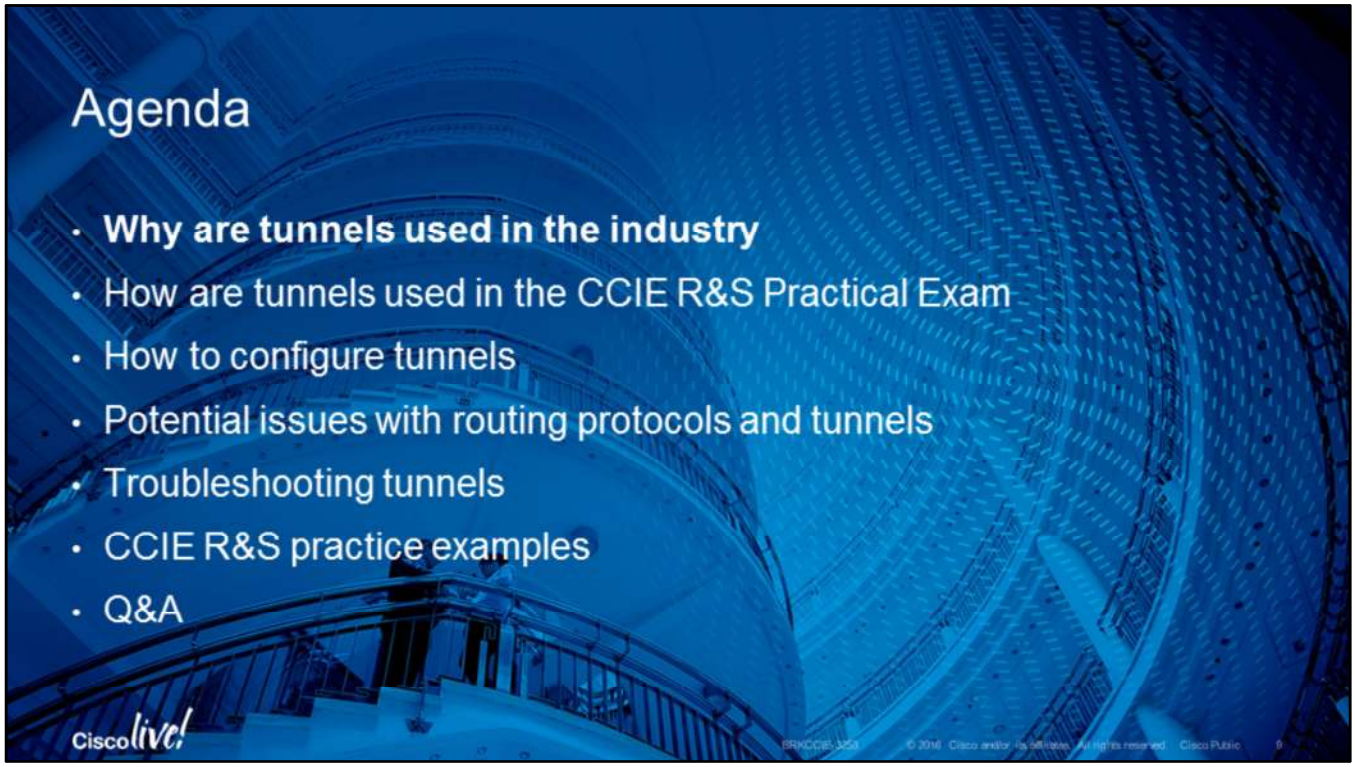
3.1.c Implement and troubleshoot encapsulation

- 3.1.c [i] GRE
- 3.1.c [ii] Dynamic GRE

3.2 Encryption

3.2.a Implement & troubleshoot IPsec with preshared key

- 3.2.a [i] IPv4 site to IPv4 site
- 3.2.b [ii] IPv6 in IPv4 tunnels
- 3.2.a [iii] Virtual tunneling interface [VTI]


Agenda
• Why are tunnels used in the industry
• How are tunnels used in the CCIE R&S Practical Exam
• How to configure tunnels
• Potential issues with routing protocols and tunnels
• Troubleshooting tunnels
• CCIE R&S practice examples
• Q&A
Cisco live!

Why Tunnels?

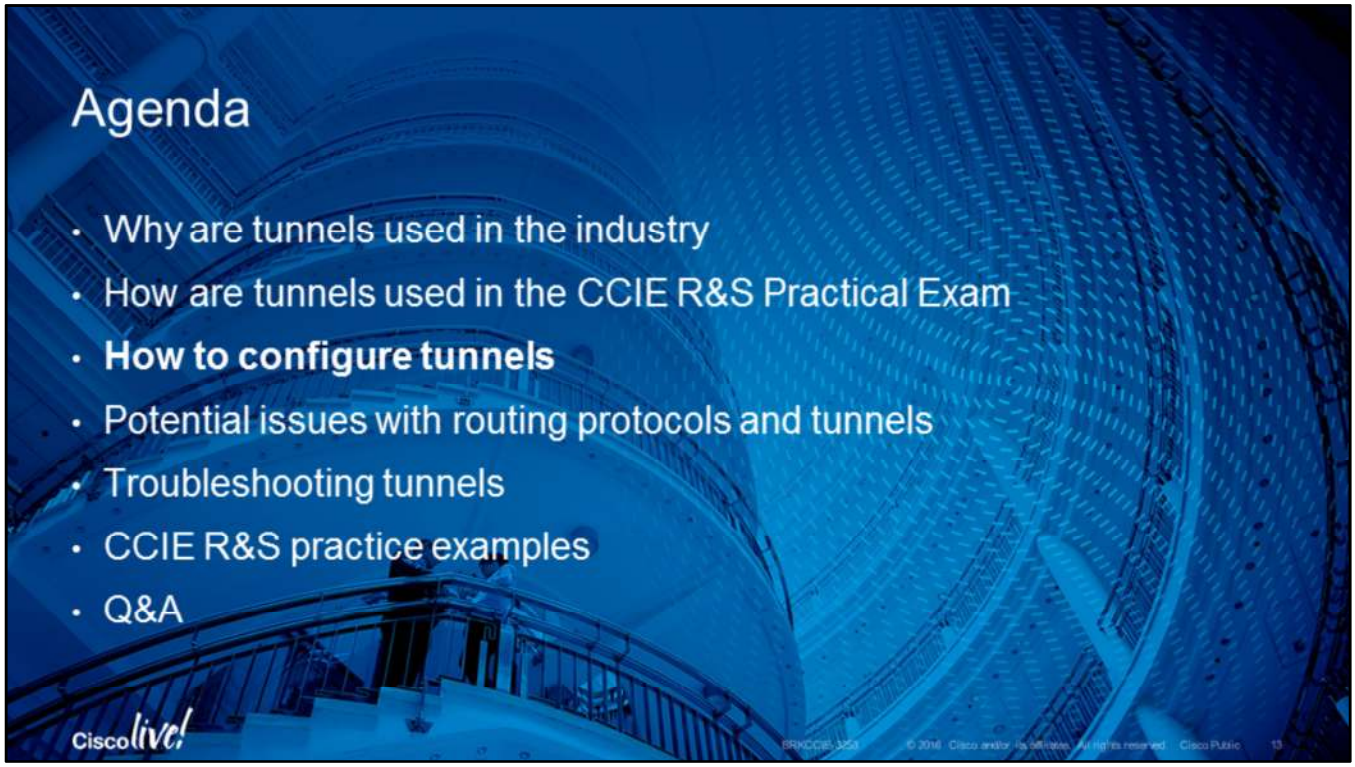
- Tunnels to hide traffic
  - Virtual Private Networks
- Tunnels to transit third party networks or the Internet
  - Low cost site to site reachability
- Tunnels for legacy protocols
  - AppleTalk, IPX and others
- Tunnels to transition
  - IPv6
- Tunnels for non-routable traffic
  - Datacenter traffic: Vmotion, FCoE
- Others???

Agenda

- Why are tunnels used in the industry
- **How are tunnels used in the CCIE R&S Practical Exam**
- How to configure tunnels
- Potential issues with routing protocols and tunnels
- Troubleshooting tunnels
- CCIE R&S practice examples
- Q&A

Tunnels in the CCIE, why?

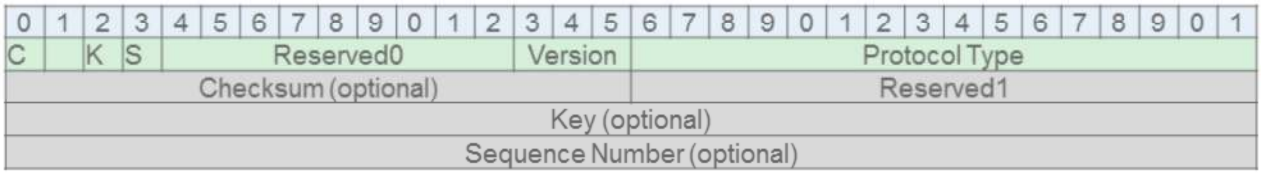
- Because they can!
- To test how well you understand how tunnels could be used in the real world
- A little more real world like scenarios
  - DMVPN, VTI, IPsec through the Internet


Agenda
• Why are tunnels used in the industry
• How are tunnels used in the CCIE R&S Practical Exam
• How to configure tunnels
• Potential issues with routing protocols and tunnels
• Troubleshooting tunnels
• CCIE R&S practice examples
• Q&A
Cisco live!

GRE and Dynamic GRE Tunnels

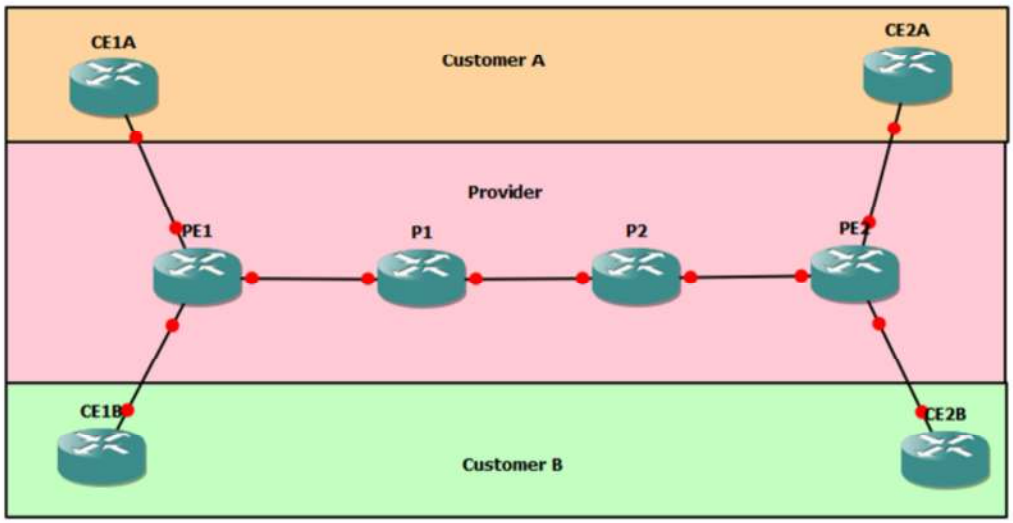
- Generic Routing Encapsulation introduced in 1994 RFC 1701
- Multipoint GRE with Next Hop Resolution Protocol = Dynamic Multipoint VPN
  - Not covered in this session
- Dynamic GRE Tunnels
  - What does that really mean?
    - GRE Tunnels with IP Unnumbered?
    - GRE Tunnels with DHCP?
    - Dynamic Layer 3 VPN with mGRE?

GRE Header



- C – if checksum is present
- K – if key is present
- S – if sequence is present
- Protocol Type = EtherType

Small Topology to Test



GRE

PE1:

```
interface Tunnel0
 ip address 12.12.12.1
255.255.255.0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination
192.168.1.33
!
```

PE2:

```
interface Tunnel0
 ip address 12.12.12.2
255.255.255.0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination
192.168.1.17
!
```


PE1:

```
!
interface Loopback0
 ip address 192.168.1.17 255.255.255.255
!
interface Tunnel0
 ip address 12.12.12.1 255.255.255.0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination 192.168.1.33
!
interface FastEthernet0/0
 ip address 192.168.1.49 255.255.255.240
 speed auto
 duplex auto
!
interface FastEthernet1/0
 ip address 172.16.11.18 255.255.255.240
 speed auto
 duplex full
!
interface FastEthernet1/1
 ip address 172.16.11.34 255.255.255.240
```

```
 speed auto
 duplex full
!
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
!
router ospf 2
 network 172.16.0.0 0.0.255.255 area 0
!
```

PE2:

```
!
interface Loopback0
 ip address 192.168.1.33 255.255.255.255
!
interface Tunnel0
 ip address 12.12.12.2 255.255.255.0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination 192.168.1.17
!
interface FastEthernet0/0
 ip address 192.168.1.65 255.255.255.240
 speed auto
 duplex auto
!
interface FastEthernet1/0
 ip address 172.16.22.18 255.255.255.240
 speed auto
 duplex full
!
interface FastEthernet1/1
 ip address 172.16.22.34 255.255.255.240
 speed auto
 duplex full
!
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
!
router ospf 2
 network 172.16.0.0 0.0.255.255 area 0
!
```

GRE

```
PE1(config-if)#do sh ip route ospf

      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        172.16.22.16/28 [110/1001] via 12.12.12.2, 00:08:40, Tunnel0
O        172.16.22.32/28 [110/1001] via 12.12.12.2, 00:08:40, Tunnel0
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.1.33/32 [110/4] via 192.168.1.50, 00:36:48, FastEthernet0/0
O        192.168.1.64/28 [110/3] via 192.168.1.50, 00:36:48, FastEthernet0/0
O        192.168.1.81/32 [110/2] via 192.168.1.50, 00:36:48, FastEthernet0/0
O        192.168.1.97/32 [110/3] via 192.168.1.50, 00:36:48, FastEthernet0/0
O        192.168.1.112/28 [110/2] via 192.168.1.50, 00:36:48, FastEthernet0/0
```

GRE with Unnumbered

PE1:

```
interface Tunnel0
 ip unnumbered Loopback0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination
192.168.1.33
!
```

PE2:

```
interface Tunnel0
 ip unnumbered Loopback0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination
192.168.1.17
!
```

GRE with Unnumbered

```
PE1(config-if)#do sh ip route ospf

 172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        172.16.22.16/28 [110/1001] via 192.168.1.33, 00:00:14, Tunnel0
O        172.16.22.32/28 [110/1001] via 192.168.1.33, 00:00:04, Tunnel0
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.1.33/32 [110/4] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.64/28 [110/3] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.81/32 [110/2] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.97/32 [110/3] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.112/28 [110/2] via 192.168.1.50, 00:28:59, FastEthernet0/0
```

GRE with DHCP

PE1:

```
ip dhcp pool ForPE1
 network 12.12.12.0
255.255.255.0
!
interface Tunnel0
 ip address pool ForPE1
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination
192.168.1.33
```

PE2:

```
interface Tunnel0
 ip address 12.12.12.2
255.255.255.0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination
192.168.1.17
!
```

GRE with DHCP

```
PE1#sh ip int brie
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        192.168.1.49    YES manual up                    up
FastEthernet0/1        unassigned      YES NVRAM  up                    up
FastEthernet1/0        172.16.11.18    YES manual up                    up
FastEthernet1/1        172.16.11.34    YES manual up                    up
Loopback0              192.168.1.17    YES NVRAM  up                    up
Tunnel0                12.12.12.1      YES manual up                    up
```

GRE with DHCP

```
PE1(config-if)#do sh ip route ospf

 172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        172.16.22.16/28 [110/1001] via 12.12.12.2, 00:00:51, Tunnel0
O        172.16.22.32/28 [110/1001] via 12.12.12.2, 00:00:51, Tunnel0
      192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
O        192.168.1.33/32 [110/4] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.64/28 [110/3] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.81/32 [110/2] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.97/32 [110/3] via 192.168.1.50, 00:28:59, FastEthernet0/0
O        192.168.1.112/28 [110/2] via 192.168.1.50, 00:28:59, FastEthernet0/0
```

Dynamic Layer 3 VPN with mGRE

- Dynamic L3 VPNs with mGRE Tunnels feature provides an L3 transport
- L3 tunneling transport can also be used within IP networks to transport VPN traffic across another IPv4 network

Dynamic Layer 3 VPN with mGRE

```
vrf definition MGRE
 rd 1:2
 route-target export 1:2
 route-target import 1:2
 address-family ipv4
 exit-address-family
!
interface FastEthernet1/0
 vrf forwarding MGRE
 ip address 172.16.11.18 255.255.255.240
```

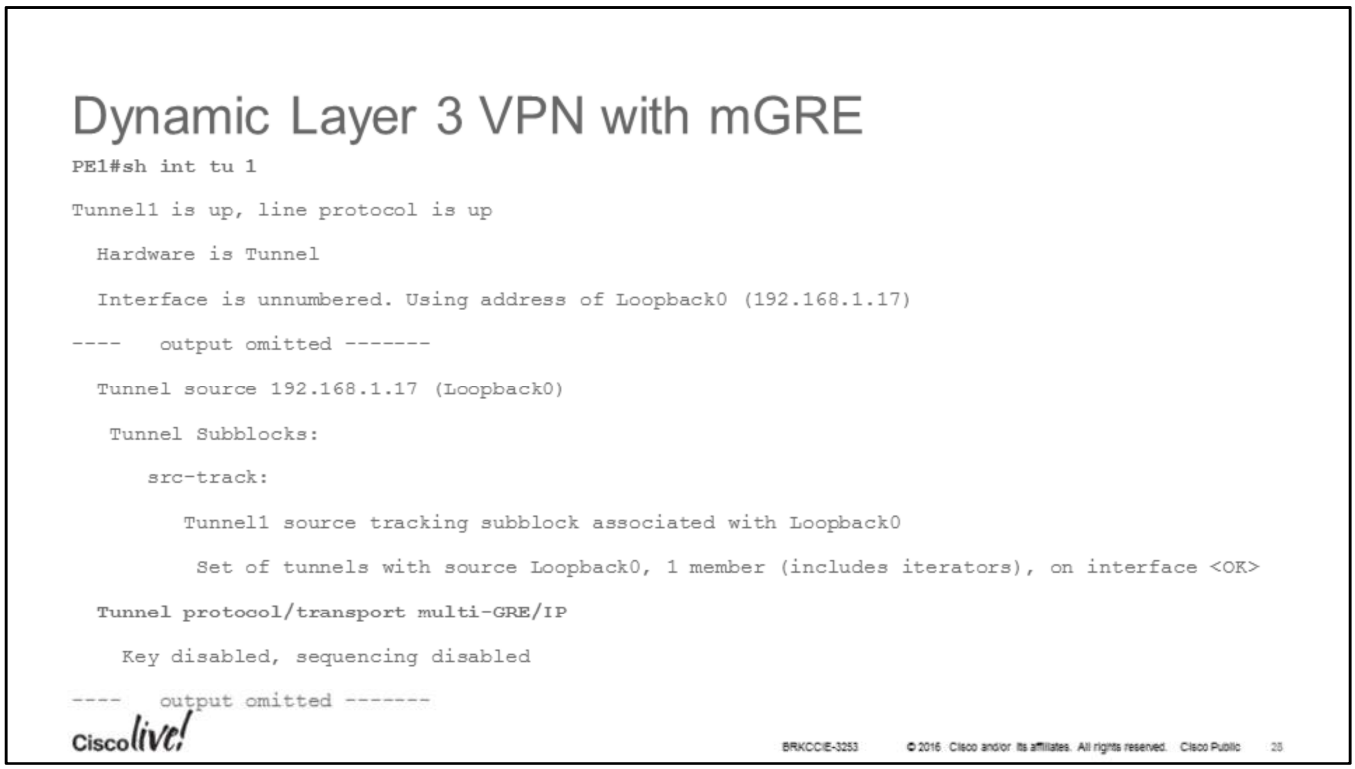
```
l3vpn encapsulation ip MGRE
 transport ipv4 source Loopback0
!
route-map MGRE-NEXT-HOP permit 10
 set ip next-hop encapsulate l3vpn MGRE
```

Dynamic Layer 3 VPN with mGRE

```
router bgp 65534
 bgp log-neighbor-changes
 neighbor 192.168.1.33 remote-as 65534
 neighbor 192.168.1.33 update-source Loopback0
 address-family vpnv4
  neighbor 192.168.1.33 activate
  neighbor 192.168.1.33 send-community extended
  neighbor 192.168.1.33 route-map MGRE-NEXT-HOP in
address-family ipv4 vrf MGRE
  redistribute connected
```

Dynamic Layer 3 VPN with mGRE

```
PE1#sh tunnel endpoints

 Tunnel1 running in multi-GRE/IP mode

 Endpoint transport 192.168.1.33 Refcount 3 Base 0x696B874C Create Time
00:14:00

   overlay 192.168.1.33 Refcount 2 Parent 0x696B874C Create Time 00:14:00

PE1#show ip int brie

Interface              IP-Address      OK? Method Status
Protocol

----   output omitted -------

Loopback0              192.168.1.17    YES NVRAM  up                    up

Tunnel1                192.168.1.17    YES unset  up                    up
```




```
PE1#sh int tu 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Loopback0
(192.168.1.17)
  MTU 17916 bytes, BW 10000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.1.17 (Loopback0)
   Tunnel Subblocks:
      src-track:
         Tunnel1 source tracking subblock associated with
Loopback0
          Set of tunnels with source Loopback0, 1 member
(includes iterators), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
```

```
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:13:15, output 00:13:15, output hang never
  Last clearing of "show interface" counters 00:51:44
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total
output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7 packets input, 840 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,
0 abort
     5 packets output, 640 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped
out
```

```
PE1#sh int tu 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Loopback0
(192.168.1.17)
----   output omitted -------
  Tunnel source 192.168.1.17 (Loopback0)
   Tunnel Subblocks:
      src-track:
         Tunnel1 source tracking subblock associated with
Loopback0
          Set of tunnels with source Loopback0, 1 member
(includes iterators), on interface <OK>
  Tunnel protocol/transport multi-GRE/IP
    Key disabled, sequencing disabled
----   output omitted -------
```

Dynamic Layer 3 VPN with mGRE

```
PE1#show ip route vrf MGRE
----   output omitted -------
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C        172.16.11.16/28 is directly connected, FastEthernet1/0
L        172.16.11.18/32 is directly connected, FastEthernet1/0
B        172.16.22.16/28 [200/0] via 192.168.1.33, 00:14:50, Tunnel1
```

Dynamic Layer 3 VPN with mGRE

```
PE1#show ip route vrf MGRE 172.16.22.16
Routing Table: MGRE
Routing entry for 172.16.22.16/28
  Known via "bgp 65534", distance 200, metric 0, type internal
  Last update from 192.168.1.33 on Tunnel1, 00:18:40 ago
  Routing Descriptor Blocks:
  * 192.168.1.33 (default), from 192.168.1.33, 00:18:40 ago, via Tunnel1
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 16
      MPLS Flags: MPLS Required
```

Dynamic Layer 3 VPN with mGRE

```
PE1#ping vrf MGRE 172.16.22.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.22.18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1048/1262/1404 ms

PE1#show run | i mpls
PE1#show run int tunnel 1
Building configuration...
Current configuration : 5 bytes
end
PE1#
```

Implement & Troubleshoot IPsec with preshared key

- IPv4 site to IPv4 site
- IPv6 in IPv4 tunnels
- Virtual tunneling interface [VTI]

IPv4 site to IPv4 site

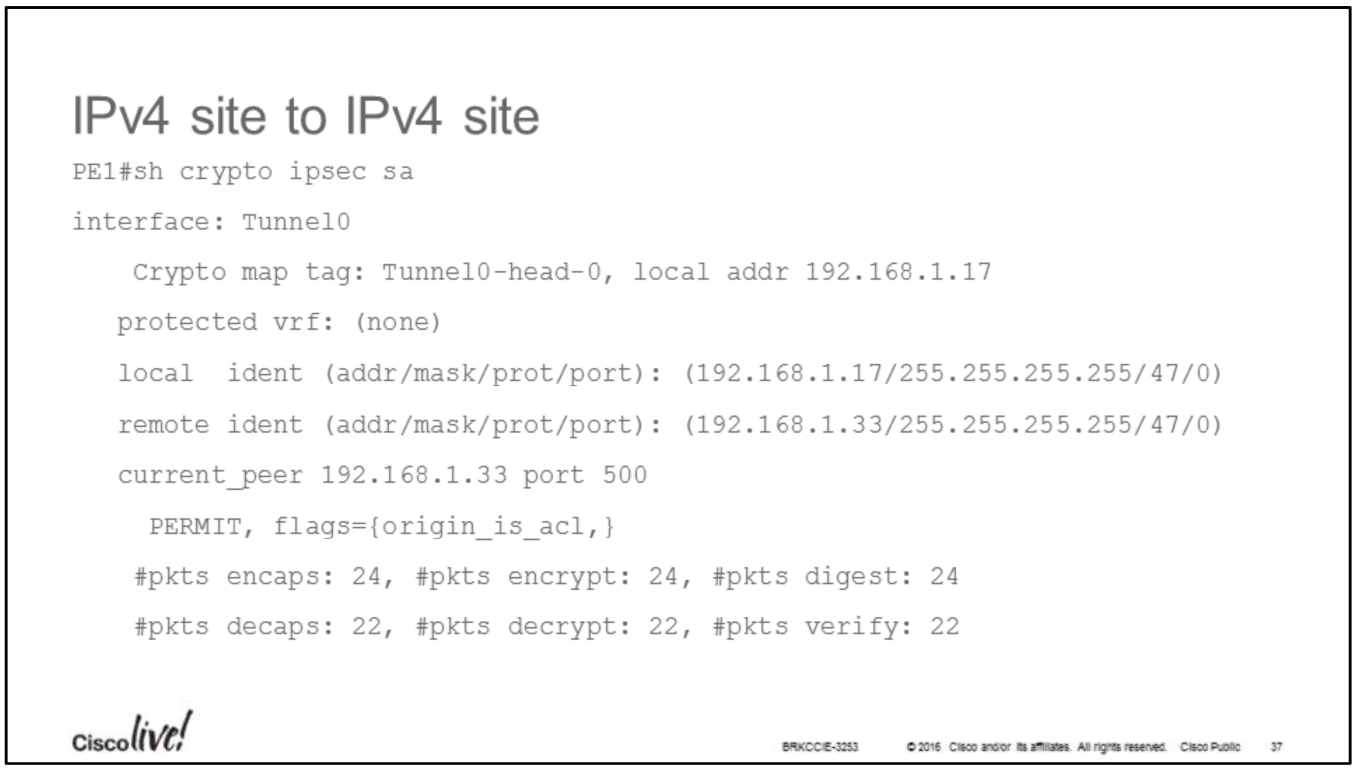
```
crypto isakmp policy 1
 encr aes 256
 hash sha512
 authentication pre-share
 group 14
crypto isakmp key Cisco address 0.0.0.0
!
crypto ipsec transform-set MyTS esp-aes esp-sha256-hmac
 mode transport
!
crypto ipsec profile MyProfile
 set transform-set MyTS
```

IPv4 site to IPv4 site

```
interface Tunnel0
 ip address 12.12.12.1 255.255.255.0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel destination 192.168.1.33
 tunnel protection ipsec profile MyProfile
!
```

IPv4 site to IPv4 site

```
PE1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.1.17    192.168.1.33    MM_NO_STATE          0 ACTIVE (deleted)
192.168.1.33    192.168.1.17    QM_IDLE           1001 ACTIVE
PE1#ping 172.16.22.18 sou fa1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.22.18, timeout is 2 seconds:
Packet sent with a source address of 172.16.11.18
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1140/1336/1408 ms
```



PE1#sh crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 192.168.1.17

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.17/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.1.33/255.255.255.255/47/0)
current_peer 192.168.1.33 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 22, #pkts decrypt: 22, #pkts verify: 22
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.1.17, remote crypto endpt.: 192.168.1.33
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x5394CA98(1402260120)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0xC9733487(3379770503)

IPv4 site to IPv4 site

```
PE1#sh ip route
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.12.12.0/24 is directly connected, Tunnel0
L        12.12.12.1/32 is directly connected, Tunnel0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
C        172.16.11.16/28 is directly connected, FastEthernet1/0
L        172.16.11.18/32 is directly connected, FastEthernet1/0
C        172.16.11.32/28 is directly connected, FastEthernet1/1
L        172.16.11.34/32 is directly connected, FastEthernet1/1
O        172.16.22.16/28 [110/1001] via 12.12.12.2, 00:00:36, Tunnel0
O        172.16.22.32/28 [110/1001] via 12.12.12.2, 00:00:36, Tunnel0
```

IPv6 in IPv4 tunnels

```
PE1(config-if)#do sh run int tu 0
interface Tunnel0
 ip address 12.12.12.1 255.255.255.0
 ip ospf 2 area 0
 ipv6 address 2005:DEAD:BEEF:12::1/80
 ospfv3 1 ipv6 area 0
 tunnel source Loopback0
 tunnel destination 192.168.1.33
 tunnel protection ipsec profile MyProfile
end
```

IPv6 in IPv4 tunnels

```
PE1#show ospfv3 interface brief
Interface    PID   Area            AF         Cost  State Nbrs F/C
Tu0          1     0               ipv6       1000  P2P   1/1
Fa1/0        1     0               ipv6       1     DR    0/0

PE1#show ospfv3 neighbor

          OSPFv3 1 address-family ipv6 (router-id 192.168.1.17)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.168.1.33      0   FULL/  -        00:00:35    8               Tunnel0
```

IPv6 in IPv4 tunnels

```
PE1#show ipv6 route
C   2005:DEAD:BEEF:1::/80 [0/0]
     via FastEthernet1/0, directly connected
L   2005:DEAD:BEEF:1::1/128 [0/0]
     via FastEthernet1/0, receive
O   2005:DEAD:BEEF:2::/80 [110/1001]
     via FE80::C803:35FF:FEB8:8, Tunnel0
C   2005:DEAD:BEEF:12::/80 [0/0]
     via Tunnel0, directly connected
L   2005:DEAD:BEEF:12::1/128 [0/0]
     via Tunnel0, receive
```

IPv6 in IPv4 tunnels

```
PE1#ping 2005:DEAD:BEEF:2::1 source fastEthernet 1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2005:DEAD:BEEF:2::1, timeout is 2 seconds:
Packet sent with a source address of 2005:DEAD:BEEF:1::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 912/1354/1888 ms
PE1#
```

Virtual tunneling interface [VTI]

```
PE1#sh run int tu 0
interface Tunnel0
 ip address 12.12.12.1 255.255.255.0
 ip ospf 2 area 0
 tunnel source Loopback0
 tunnel mode ipsec ipv4
 tunnel destination 192.168.1.33
 tunnel protection ipsec profile MyProfile
end
```

Virtual tunneling interface [VTI]

- VTI can be configured in a hub and spoke with the hub using a virtual template
  - We'll see an example in the CCIE section
- This is referred to as a Dynamic VTI (DVTI)
- Spoke are configured using Static VTI
  - The example we just saw
- The hub is setup as DVTI using a virtual template interface to terminate the VPN

IPsec with Crypto Map

- Legacy configuration, requires access list to identify “interesting traffic”
- Does not have it’s own tunnel interface
- Does not support multicast or broadcast traffic directly
  - GRE within IPsec to support multicast and/or broadcast

IPsec with Crypto Map – P1

```
crypto isakmp policy 1
 encr aes 256
 hash sha512
 authentication pre-share
crypto isakmp key C1sc0 address 0.0.0.0
crypto ipsec transform-set MyTS esp-aes 256
 mode transport
crypto map MyMap 10 ipsec-isakmp
 set peer 192.168.1.114
 set transform-set MyTS
 match address 100
```

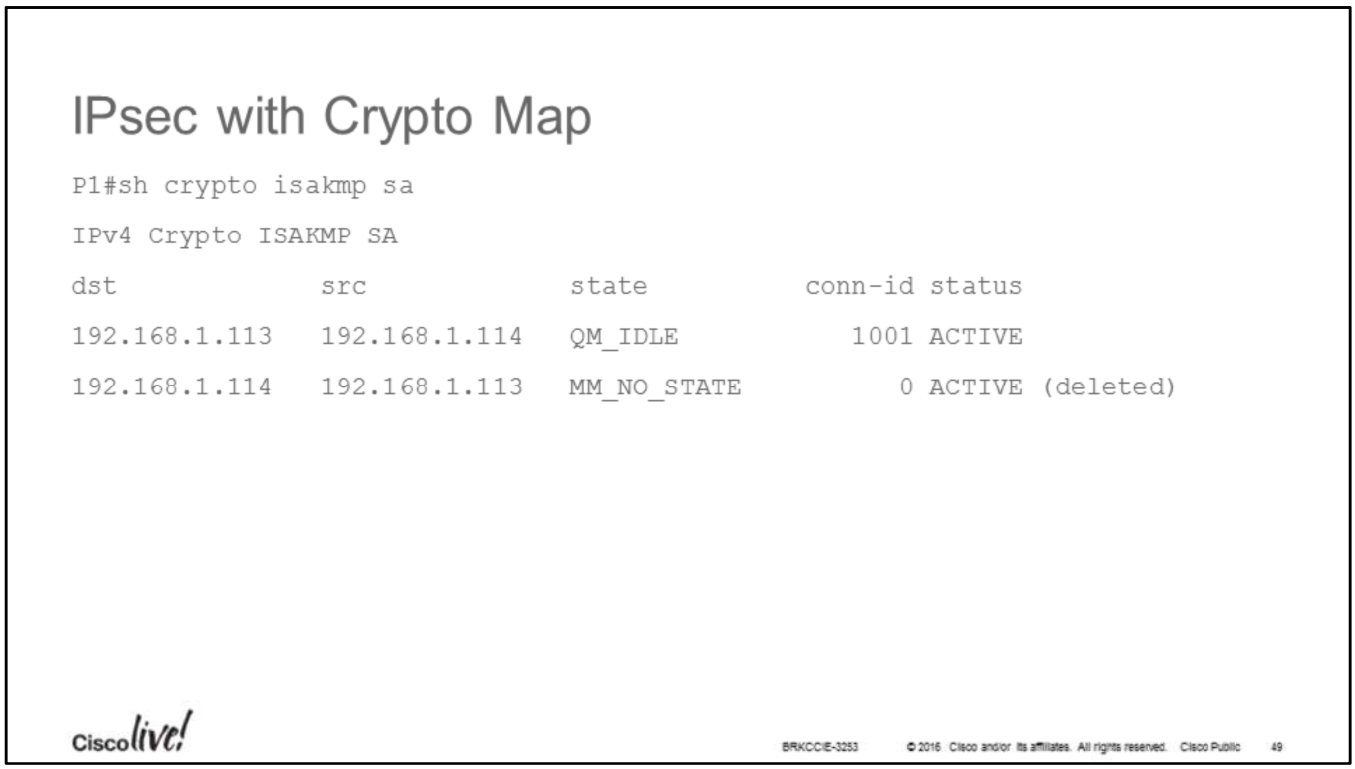
```
access-list 100 permit ip any any
!
interface FastEthernet0/1
 ip address 192.168.1.113
255.255.255.240
 speed auto
 duplex auto
 crypto map MyMap
```

IPsec with Crypto Map – P2

```
crypto isakmp policy 1
 encr aes 256
 hash sha512
 authentication pre-share
crypto isakmp key C1sc0 address 0.0.0.0
crypto ipsec transform-set MyTS esp-aes 256
 mode transport
crypto map MyMap 10 ipsec-isakmp
 set peer 192.168.1.113
 set transform-set MyTS
 match address 100
```

```
access-list 100 permit ip any any
!
interface FastEthernet0/1
 ip address 192.168.1.114
255.255.255.240
 speed auto
 duplex auto
 crypto map MyMap
```

```
P1#sh crypto map
Crypto Map IPv4 "MyMap" 10 ipsec-isakmp
        Peer = 192.168.1.114
        Extended IP access list 100
            access-list 100 permit ip any any
        Current peer: 192.168.1.114
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                MyTS:  { esp-256-aes  } ,
        Interfaces using crypto map MyMap:
                FastEthernet0/1
```



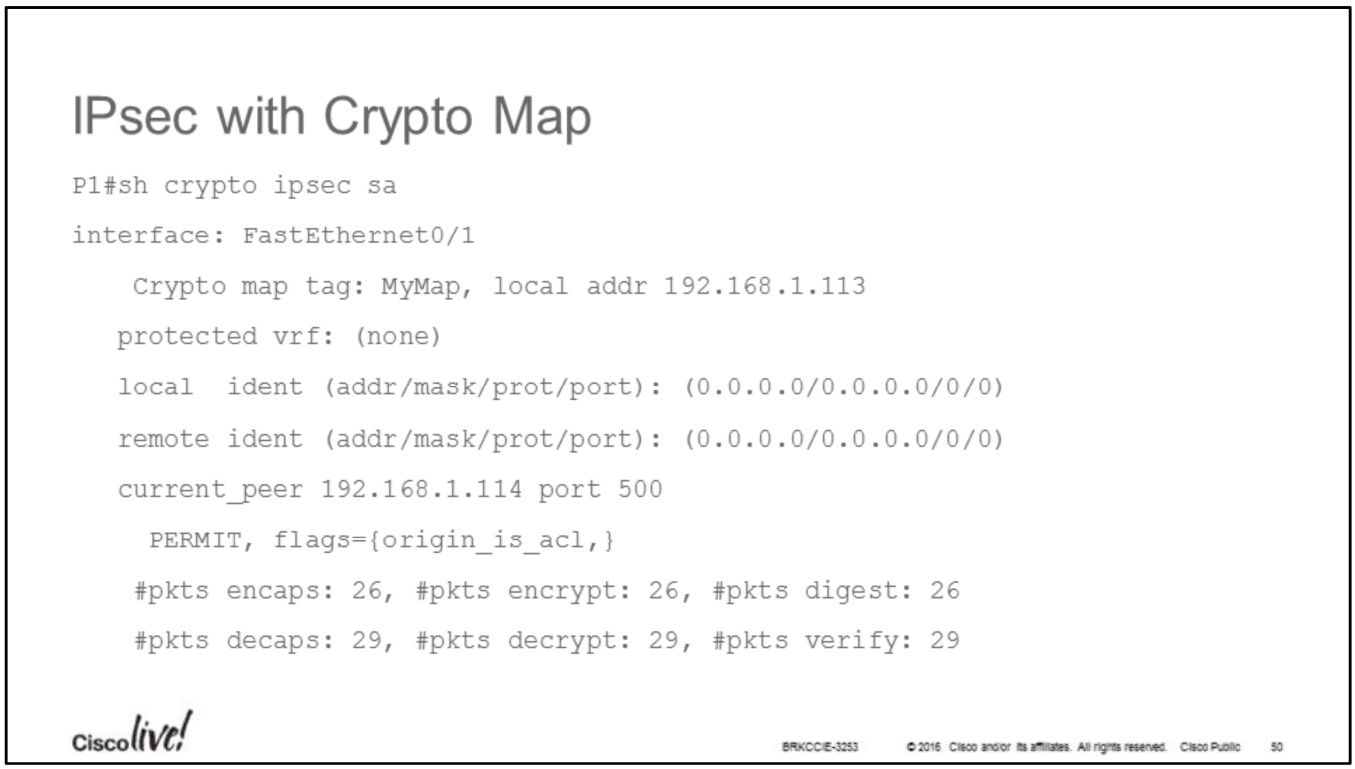
P1#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1001 192.168.1.113 192.168.1.114 ACTIVE aes sha512 psk 1 23:59:08
Engine-id:Conn-id = SW:1

0 192.168.1.113 192.168.1.114 ACTIVE 0 0
Engine-id:Conn-id = ???
(deleted)

IPv6 Crypto ISAKMP SA



P1#sh crypto ipsec sa

interface: FastEthernet0/1
Crypto map tag: MyMap, local addr 192.168.1.113

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 192.168.1.114 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
#pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

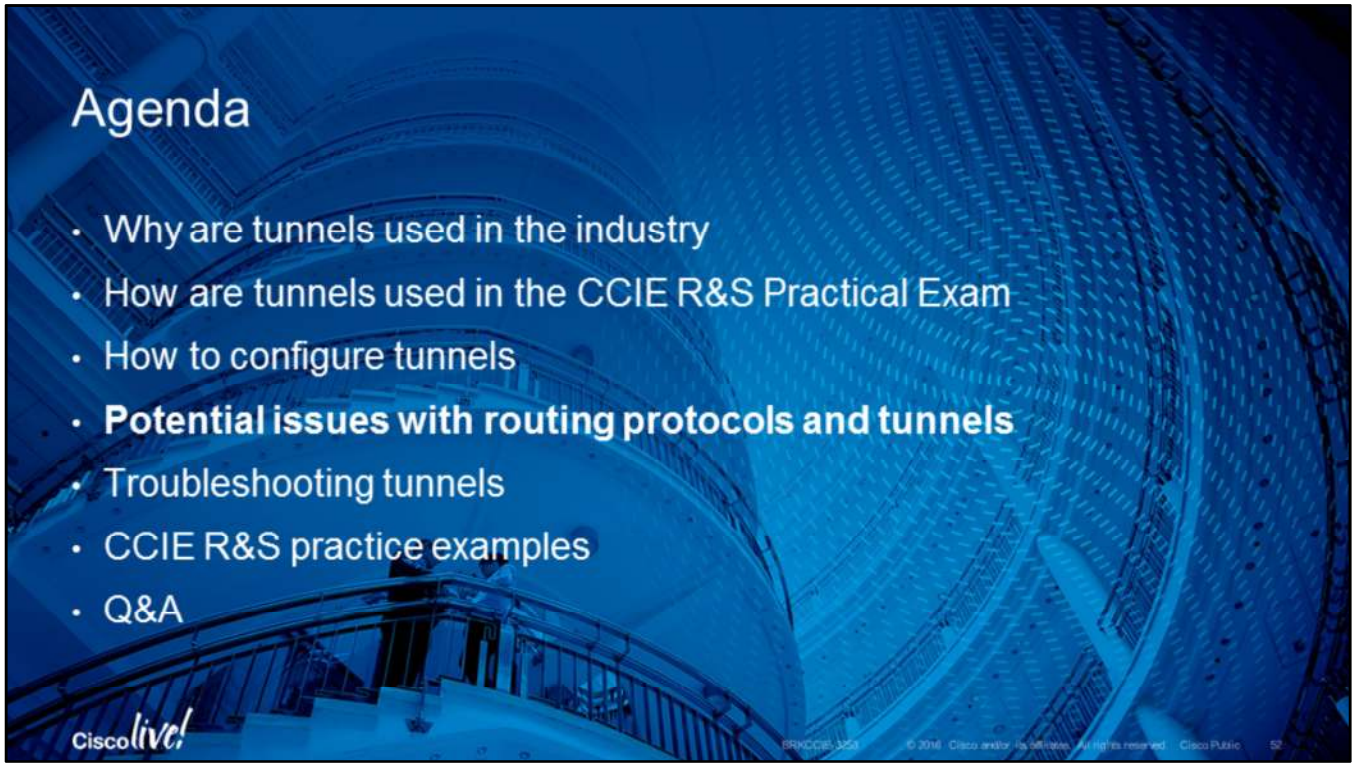
local crypto endpt.: 192.168.1.113, remote crypto endpt.: 192.168.1.114
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
current outbound spi: 0xC6ED174D(3337426765)
PFS (Y/N): N, DH group: none

inbound esp sas:

```
     spi: 0x5344F5C(87314268)
       transform: esp-256-aes ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: 1, sibling_flags 80000040, crypto map: MyMap
       sa timing: remaining key lifetime (k/sec): (4608000/3537)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
     spi: 0x244A8699(608863897)
       transform: esp-256-aes ,
       in use settings ={Tunnel, }
       conn id: 3, flow_id: 3, sibling_flags 80000040, crypto map: MyMap
       sa timing: remaining key lifetime (k/sec): (4242933/3540)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x8AE6E7E8(2330388456)
       transform: esp-256-aes ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: 2, sibling_flags 80000040, crypto map: MyMap
       sa timing: remaining key lifetime (k/sec): (4608000/3537)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
     spi: 0xC6ED174D(3337426765)
       transform: esp-256-aes ,
       in use settings ={Tunnel, }
       conn id: 4, flow_id: 4, sibling_flags 80000040, crypto map: MyMap
       sa timing: remaining key lifetime (k/sec): (4242933/3540)
       IV size: 16 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
P1#
```

IPsec with Crypto Map

```
P1#ping 192.168.1.114

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.114, timeout is 2
seconds:

!!!!!
```


Agenda
• Why are tunnels used in the industry
• How are tunnels used in the CCIE R&S Practical Exam
• How to configure tunnels
• Potential issues with routing protocols and tunnels
• Troubleshooting tunnels
• CCIE R&S practice examples
• Q&A
Cisco live!

Potential issues with routing protocols and tunnels

- Recursive routing
- Multicast thru IPsec
- Hub and spoke issues

Recursive Routing

- Make sure that the tunnel endpoints (tunnel source & destination) are not learned through the tunnel

```
%TUN-5-RECURDOWN: Tunnel0 temporarily disabled due to recursive routing
```

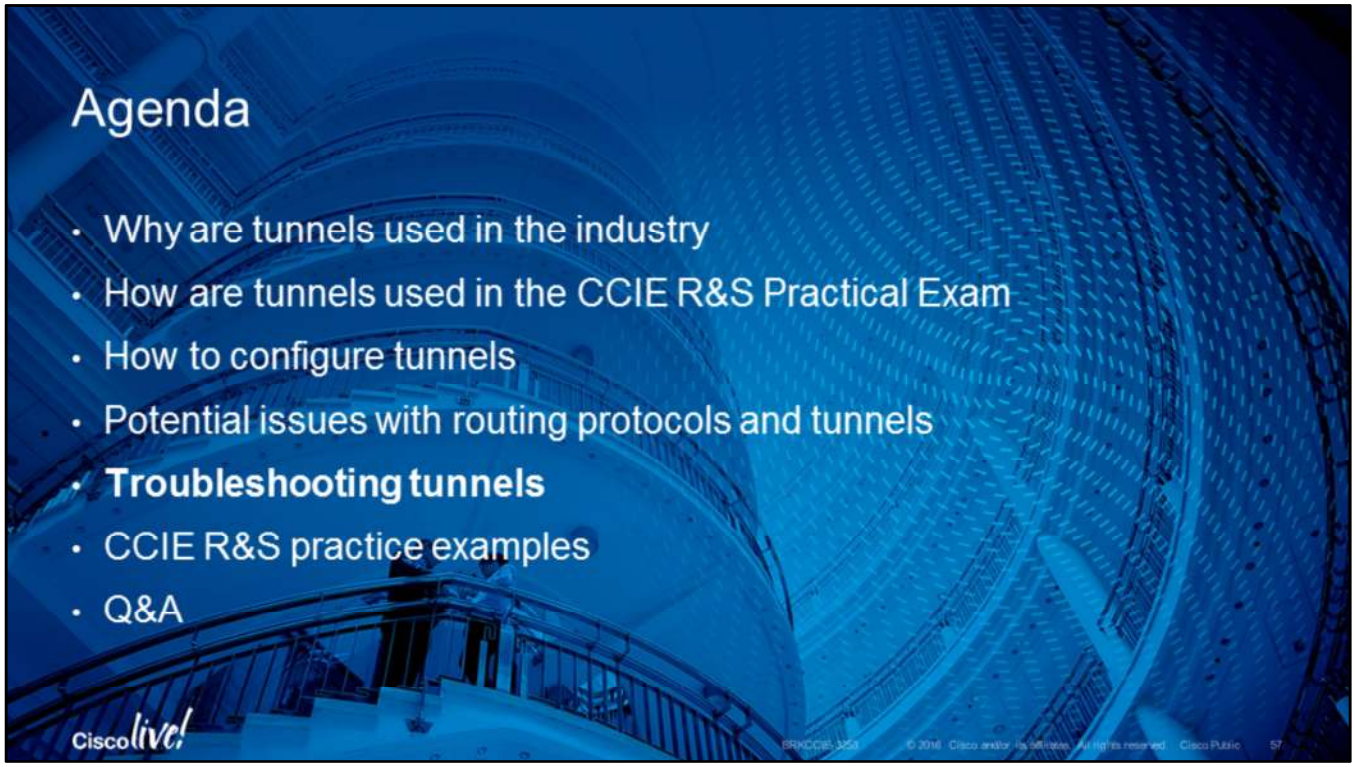
- If the tunnel destination is known through routing within the tunnel, the tunnel will go down.
- Keep the tunnel routing separate from the transport networks routing

Multicast thru IPsec

- IPsec, if applied through a crypto map to an interface, does not support multicast or broadcast
- Either use VTI, a protected GRE tunnel or a GRE tunnel within an IPsec tunnel.

Hub and spoke issues

- With dynamic VTI, there may be issues with reachability between same subnet spokes.
- Either tunnel between spokes or use DMVPN


Agenda
• Why are tunnels used in the industry
• How are tunnels used in the CCIE R&S Practical Exam
• How to configure tunnels
• Potential issues with routing protocols and tunnels
• Troubleshooting tunnels
• CCIE R&S practice examples
• Q&A
Cisco live!

Show Tunnel

```
PE1#sh tunnel int tu 0
Tunnel0
   Mode:GRE/IP, Destination 192.168.1.33, Source Loopback0
   IP transport: output interface FastEthernet0/0 next hop 192.168.1.50
   Application ID 1: unspecified
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Loopback0
          Set of tunnels with source Loopback0, 1 member (includes iterators), on
    interface <OK>
       Linestate - current up
```

Show Tunnel - continued

```
Internal linestate - current up, evaluated up
   Tunnel Source Flags: Local
   Transport IPv4 Header DF bit cleared
   OCE: IP tunnel decap
   Provider: interface Tu0, prot 47
     Performs protocol check [47]
     Protocol Handler: GRE: opt 0x0
       ptype: ipv4 [ipv4 dispatcher: from if Tu0]
       ptype: ipv6 [ipv6 dispatcher: punt]
       ptype: mpls [mpls dispatcher: drop]
       ptype: otv [otv dispatcher: drop]
```

GRE and Keepalive

- The tunnel interface will be up/up if there is a valid source for the tunnel and the destination is reachable through the routing table
  - There is no guarantee that the other end is configured or is correct
- GRE Tunnels support an optional keepalive
- Keepalive has to be configured on both ends of the tunnel and will trigger the line protocol
  - `router(config-if)# keepalive [period [retries]]`
    - Period is the interval of the keepalive, 10 seconds is the default
    - Retires are the number of failures before line protocol goes down, default is 3

Tunnels and MTU

- Remember that the tunnel interfaces add additional headers, therefore the IP MTU has to be reduced. For GRE over IPv4, the addition of 24 bytes of headers, so the IP MTU should be 1476 (assuming the path has an MTU of 1500). The router should adjust this for you, but to verify use the **show ip interface tunnel x** command.

```
PE1(config-if)#do sh ip int tu 0
Tunnel0 is up, line protocol is up
  Internet address is 12.12.12.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1476 bytes
  Helper address is not set
```

Troubleshooting Tunnels

- Tunnel doesn't pass traffic!
  - IPsec
    - Phase 1 functioning?
      - Show crypto isakmp sa
    - Phase 2 functioning?
      - Show crypto ipsec sa
  - GRE
    - Source interface has an IP address
    - Destination address is reachable
    - Source of local router is destination of the remote router
    - Destination of local router is the source of the remote router
    - Tunnel mode of both routers are the same

IPv6 in IPv4 tunnels

- IPv6 is only known at the endpoints only
- Verify IPv6 routing
- Verify tunnel functionality with IPv4
- Tunnel modes are the same on both ends

Virtual tunneling interface [VTI]

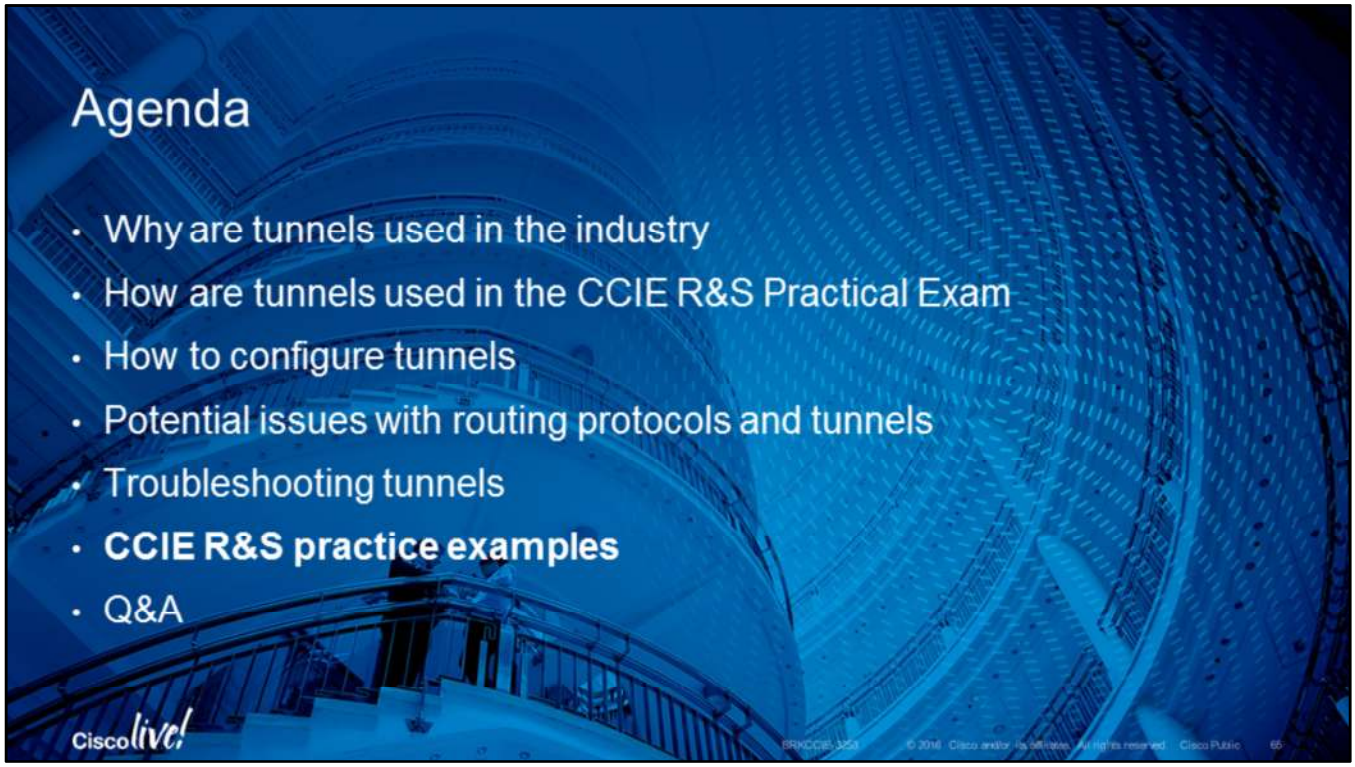
You may experience the following message when you try to modify the Virtual Template:

```
% Virtual-template config is locked, active vaccess present on R2
```

The virtual template cannot be modified when the virtual template is associated with a virtual access interface. Perform the following steps to modify an existing virtual template configuration:

- Shut down the Loopback interface that is the source of the unnumbered for the virtual template.
- Clear the active sessions using the **clear crypto session** command or wait for session termination.
- Make necessary modification on the Virtual-Template interface.
- Enable the Loopback interface

The new session will use the new virtual template.


Agenda
• Why are tunnels used in the industry
• How are tunnels used in the CCIE R&S Practical Exam
• How to configure tunnels
• Potential issues with routing protocols and tunnels
• Troubleshooting tunnels
• CCIE R&S practice examples
• Q&A
Cisco live!

Virtual tunneling interface [VTI]

Configure VTIs

- Connectivity between the Loopback 214 interfaces of R1, R2, and R4 is provided via static routing during the lab initialization.
- Configure the static virtual tunnel interface (SVTI) Tunnel214 interfaces on spokes R1 and R4.
- Use the Loopback 214 interfaces on R1 and R4 for the Tunnel214 interface source.
- Reference the Loopback 214 interface as the Tunnel214 interface IP address on R1 and R4 according to the “IPv4 IGP” diagram.
- Configure the dynamic VTI (DVTI) Virtual-Template124 interface on hub R2.
- Link the IP address of the dynamic VTI interface to the Loopback214 interface on R2.

Virtual tunneling interface [VTI]

Configure IPsec DVTI Communications

Configure the IP Security (IPsec) Internet Security Association and Key Management Protocol (ISAKMP) policy on R1, R2, and R4 according to the following specifications:

Parameter	Value
Pre-shared key	CIERS2
Encryption	3DES
Hash	MD5
IPsec transform name	CIERS2_vti_transform
IPsec transform algorithm	esp-3des esp-md5-hmac
IPsec profile name	CIERS2_vti_profile
ISAKMP profile	CIERS2_vti_isakmp_profile

- Apply the IPsec profile on the dynamic VTI interface on R2.
- Apply the IPsec profile on the static VTI interfaces on R1 and R4.
- Verify connectivity and IPsec protection between spokes R1 and R4, and the hub R2.

Virtual tunneling interface [VTI] – R1/R4 (Spoke)

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key CIERS2 address 0.0.0.0
crypto isakmp diagnose error
crypto ipsec transform-set
CIERS2_vti_transform esp-3des esp-md5-hmac
 mode tunnel
!
crypto ipsec profile CIERS2_vti_profile
 set transform-set CIERS2_vti_transform
```

```
interface Tunnel214
 ip unnumbered Loopback214
 ip ospf dead-interval 6
 ip ospf hello-interval 2
 ip ospf 1 area 0
 ip ospf cost 10
 tunnel source Loopback214
 tunnel mode ipsec ipv4
 tunnel destination 172.16.214.2
 tunnel protection ipsec profile
CIERS2_vti_profile
```

Virtual tunneling interface [VTI] – R2 (Hub)

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key CIERS2 address 0.0.0.0
crypto isakmp profile CIERS2_vti_isakmp_profile
   keyring default
   match identity address 0.0.0.0
   virtual-template 124
crypto isakmp diagnose error
crypto ipsec transform-set CIERS2_vti_transform
esp-3des esp-md5-hmac
 mode tunnel
```

```
crypto ipsec profile CIERS2_vti_profile
 set transform-set CIERS2_vti_transform
!
interface Virtual-Template124 type tunnel
 ip unnumbered Loopback214
 ip ospf dead-interval 6
 ip ospf hello-interval 2
 ip ospf 1 area 0
 ip ospf cost 10
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile
CIERS2_vti_profile
```

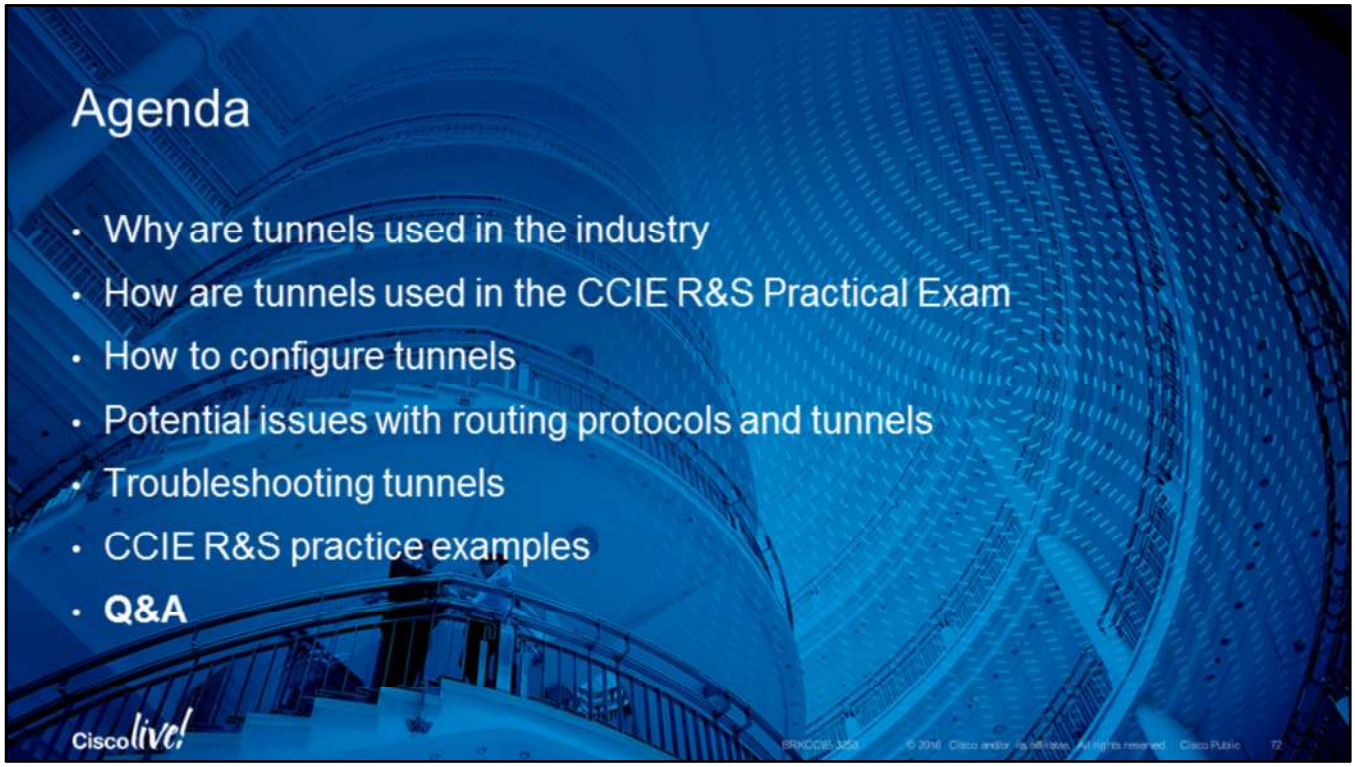
Cisco live!

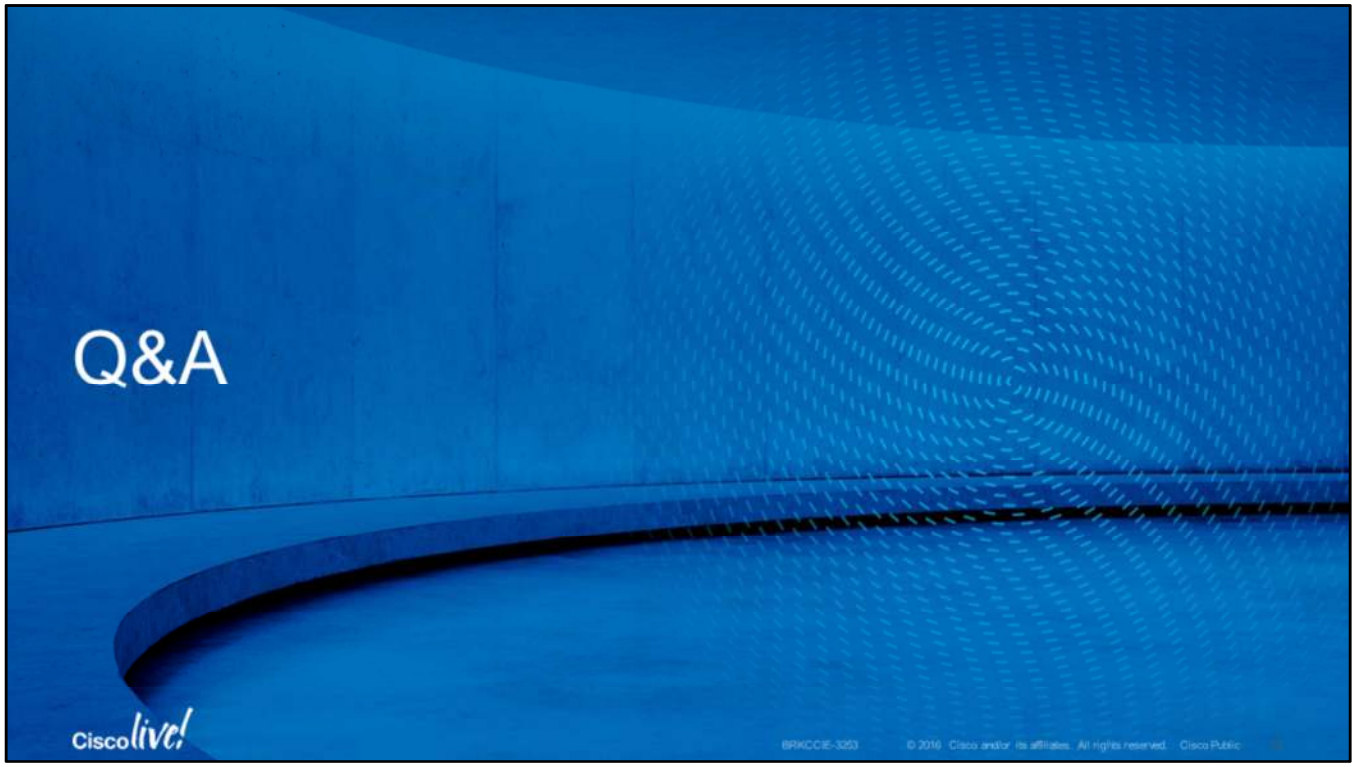
Virtual tunneling interface [VTI]

```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Virtual-Access1            172.16.214.2    YES unset  up                    up
Virtual-Access2            172.16.214.2    YES unset  up                    up
Virtual-Template124        172.16.214.2    YES unset  up                    down
R2#
```

Virtual tunneling interface [VTI]

```
R2#ping 172.16.214.1 source Loopback214

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.214.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.214.2

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R2#

R2#ping 172.16.214.4 source Loopback214

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.214.4, timeout is 2 seconds:

Packet sent with a source address of 172.16.214.2

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```


Agenda
• Why are tunnels used in the industry
• How are tunnels used in the CCIE R&S Practical Exam
• How to configure tunnels
• Potential issues with routing protocols and tunnels
• Troubleshooting tunnels
• CCIE R&S practice examples
• Q&A
Cisco live!


Q&A
Ciscolive!
BRKCCIE-3253
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

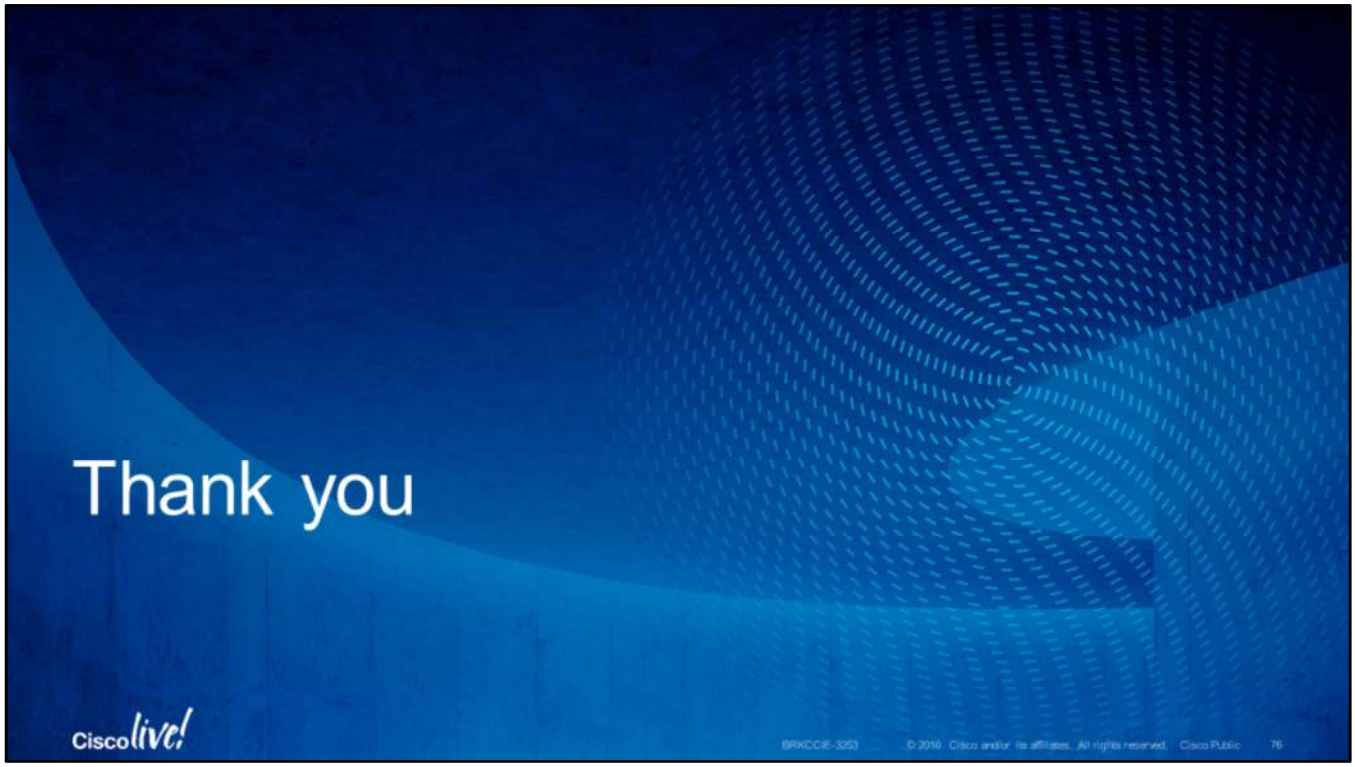
Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.
- Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.

Don't forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions


Thank you
Ciscolive!
BRKCCIE-3253
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public 76


cisco
Cisco live!
July 10-14, 2016 • Las Vegas, NV