...to Virtual Routing & Forwarding
(For Campus Engineers)

Dr. John S. Graham
(OARnet)
Example: Campus Departments

Chemistry

150.1.5.0/24

192.168.5.0/24

R5

Physics

150.1.3.0/24

192.168.3.0/24

R3

R2

R4

150.1.4.0/24
Security Specification

• Point-to-Point link subnets should not be advertised by OSPF.
• Routing of the 150.1.0.0/16 subnets should be unrestricted.
• The 192.168.0.0/16 subnets should not be advertised to other departments; only to the central administrative LAN.
• All security should be centrally controlled on the hub router R2
Let’s Try Area-Based Filtering...

```
router ospf 1
 area 1 filter-list CHEMISTRY ROUTES out
!
ip prefix-list CHEMISTRY ROUTES permit 150.1.5.0/24
ip prefix-list CHEMISTRY ROUTES deny 0.0.0.0/0 le 32
```

R2 Configuration
What the Textbooks Say
• All inter-area traffic must pass through Area 0.

What Actually Happens
• An ABR floods Type-3 LSAs describing each area out interfaces participating in all other areas
• Routers with an active adjacency in Area 0 will ignore Summary LSAs that are received on non-backbone interfaces
• Ergo, OSPF downshifts to DV behavior when all backbone connectivity is lost.
OSPF Configuration

Area 0

150.1.3.0/24

192.168.3.0/24

150.1.5.0/24

192.168.5.0/24

150.1.4.0/24

R4

R5

R2

R3

150.1.4.0/24

150.1.5.0/24

192.168.3.0/24

192.168.5.0/24
VRF Configuration

1. Create VRF Instances
   1. Pick Alphanumeric Name
   2. Assign the *Route Distinguisher* (RD)

2. Assign Interfaces to a VRF
   1. The interface IP address will need to be reapplied after configuring: `ip vrf forwarding <VRF_NAME>`

3. Create OSPF Processes
   1. One per VRF
The Route Distinguisher (RD)

- A formatted 8-byte number
  - `<GLOBAL_ADMINISTRATOR>:`<LOCAL_IDENTIFIER>

- Used to create new address family
  - RD + IP Prefix \(\rightarrow\) VPNV4 address (12-bytes)

- Allows multiple customers of a SP to advertise same prefix
Hub Configuration So Far...

ip vrf BLUE
  rd 10.0.23.3:1
!
interface Serial0/0
  no ip address
  encapsulation frame-relay
  clock rate 2000000
  no frame-relay inverse-arp
!
interface Serial0/0.1 point-to-point
  ip vrf forwarding BLUE
  ip address 10.0.23.2 255.255.255.0
  frame-relay interface-dlci 203
!
router ospf 1 vrf BLUE
  router-id 0.1.0.2
  network 0.0.0.0 255.255.255.255 area 0
1. Three disconnected VRF routing tables. Each filled with routes learned from OSPF neighbors.

2. Add a BGP table containing VPNV4 addresses. Unique RD prevents duplicate IP prefixes from clashing.

```
show ip route vrf {BLUE | GREEN | RED} ospf

show ip bgp vpnv4 all
```
interface Loopback0
    ip address 10.0.2.2 255.255.255.255
!
router bgp 65534
    no bgp default ipv4-unicast
!
    address-family ipv4 vrf BLUE
        redistribute ospf 1 vrf BLUE route-map OSPF_TO_BGP
        no synchronization
        exit-address-family
!
ip prefix-list P2P_SUBNETS seq 5 permit 10.0.0.0/8 ge 24
!
route-map OSPF_TO_BGP deny 10
    match ip address prefix-list P2P_SUBNETS
!
route-map OSPF_TO_BGP permit 20
Route Target – Export & Import

Export RT
• Assigned to *Prefixes* within a VRF instance
• One RT per prefix
• Export maps are a useful tool

Import RT
• Assigned to *VRF Instances*
• Multiple Import tags per instance permitted
• Usually best to assign statically
BGP Extended Communities

• A formatted 8-Byte value
  – ‘Type’ field indicates format of the 6-Byte value
  – ‘Subtype’ field indicates intrinsic meaning
    • Route Target Community (0x02)
    • OSPF Domain Identifier (0x05)

• See RFC 7153 for full details
Route Leaking Schema
Configuring the RT

ip vrf VRF_BLUE
   rd 10.0.23.3:1
   export map EXPORT_MAP-VRF_BLUE
route-target import 65534:3
route-target import 65534:4
!
ip prefix-list VLAN3 seq 5 permit 192.168.3.0/24
!
route-map EXPORT_MAP-VRF_BLUE permit 10
   match ip address prefix-list VLAN3
   set extcommunity rt 65534:2
!
route-map EXPORT_MAP-VRF_BLUE permit 20
   set extcommunity rt 65534:1
MP_BGP ➔ OSPF 1/2

- This final step causes ‘leaked’ routes to be advertised to spoke routers
- Leaked routes perceived by OSPF as External
  - This looks ugly and is not representative of reality
  - Alternative routes may be preferred
- Setting an OSPF ‘domain-id’ will cause leaked routes to appear as inter-area Type-III
  - This tag is propagated through MP-BGP using the OSPF Domain Identifier Extended Community
MP_BGP → OSPF 2/2

! router ospf 1 vrf VRF_BLUE
    router-id 0.1.0.2
    domain-id 123.123.123.123
    redistribute bgp 65534 subnets
    network 0.0.0.0 255.255.255.255 area 0

!
But... I Hate BGP!

• Route leaking can be accomplished statically
  – Between pairs of VRF
  – Between a VRF and the Global RIB
    • Useful for installing a Default route into a VRF

• Require two static routes
  – One in VRF pointing to Global prefix
  – One in Global RIB pointing to VRF (for return traffic)

• Remember to redistribute Static $\rightarrow$ IGP!
So Why Do Folks Want to Use MPLS?

• A question of scale
• Only 961 DLCI are available (16 through 976)
• Rather more (4,089) VLAN tags
  – Normal range = 1 through 1005
    • Reserved numbers comprise 1, 1002 – 1005
  – Extended range = 1006 to 4094
• Stacked MPLS labels
  – Outer (aka ‘Transport’) label connects pairwise PE routers
  – Inner (aka ‘VPN’) label assigned per customer
That's All Folks!