
TOMORROW starts here.
CISCO
Cisco live!

WAN Architectures and Design Principles

BRKRST-2041

Stephen Lynn
stlynn@cisco.com
Consulting Systems Architect

Cisco live!

Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

The Architectural Continuum

Early Networking	Early-Mid 1990s	Mid 1990s-Early 2000s	Today
• Flat/Bridged • Experimental Networks	• Multiprotocol • Business Enabling	• Large Scale • Mission Critical	• Global Scale • IP Ubiquity • Advanced Techs • Business Survival
↓	↓	↓	↓
Architectural Lessons	**Architectural Lessons**	**Architectural Lessons**	**Planning**
• Protocols required for Scale & Restoration	• Path Diversity • Route First , Bridge only if Must	• Hierarchy • Redundancy • Build to Scale	?

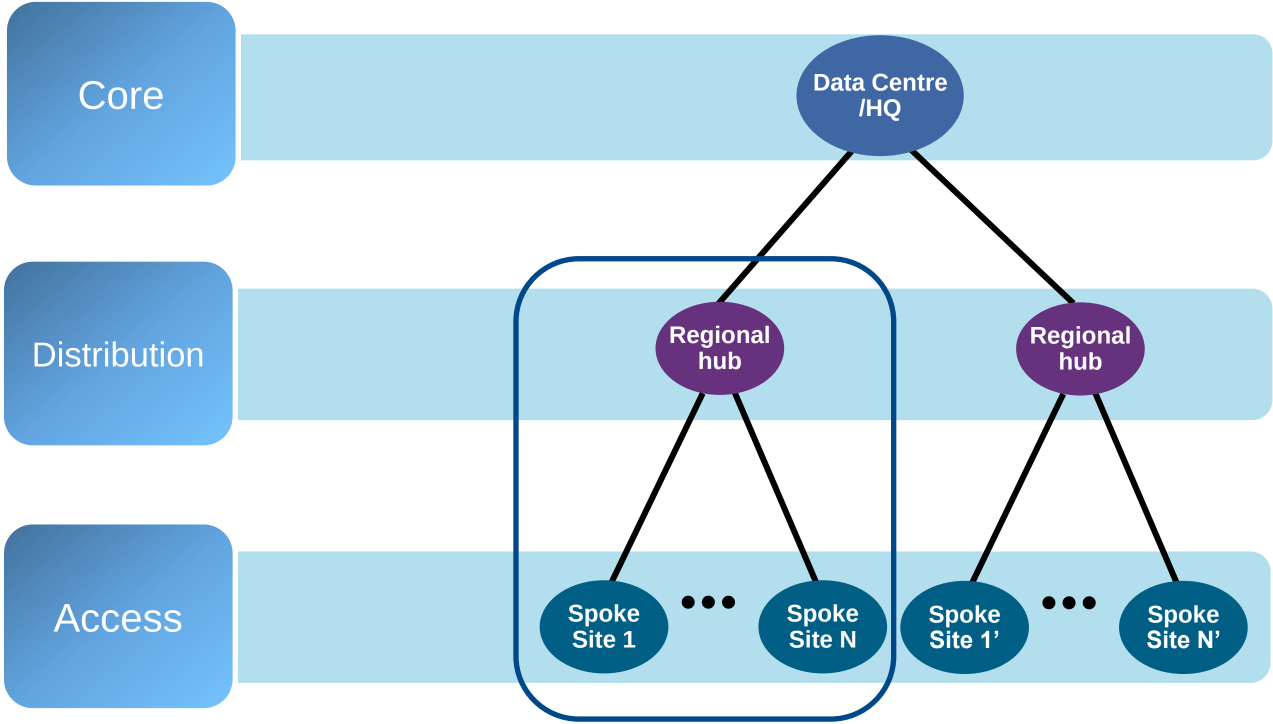
1960 → 2010+

Time

The Challenge

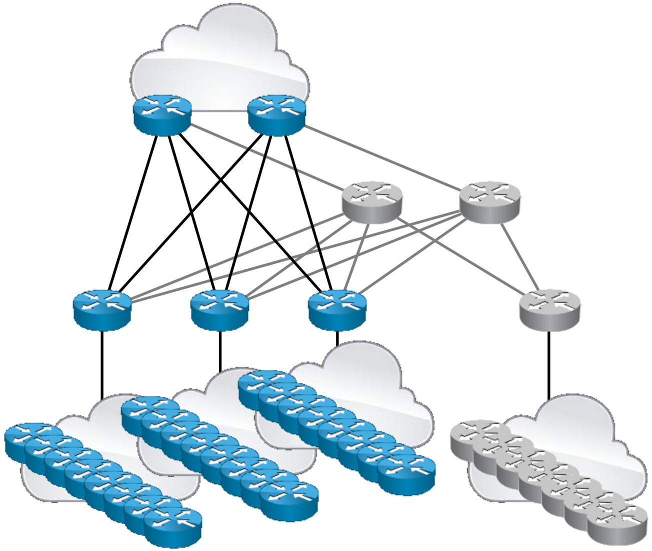
- Build a network that can adapt to a quickly changing business and technical environment
- Realise rapid strategic advantage from new technologies
  - IPv6: global reachability
  - Cloud: flexible diversified resources
  - Bring Your Own Device (BYOD)
  - What's next?
- Adapt to business changes rapidly and smoothly
  - Mergers & divestures
  - Changes in the regulatory environment
  - Changes in public perception of services

Network Design Modulation

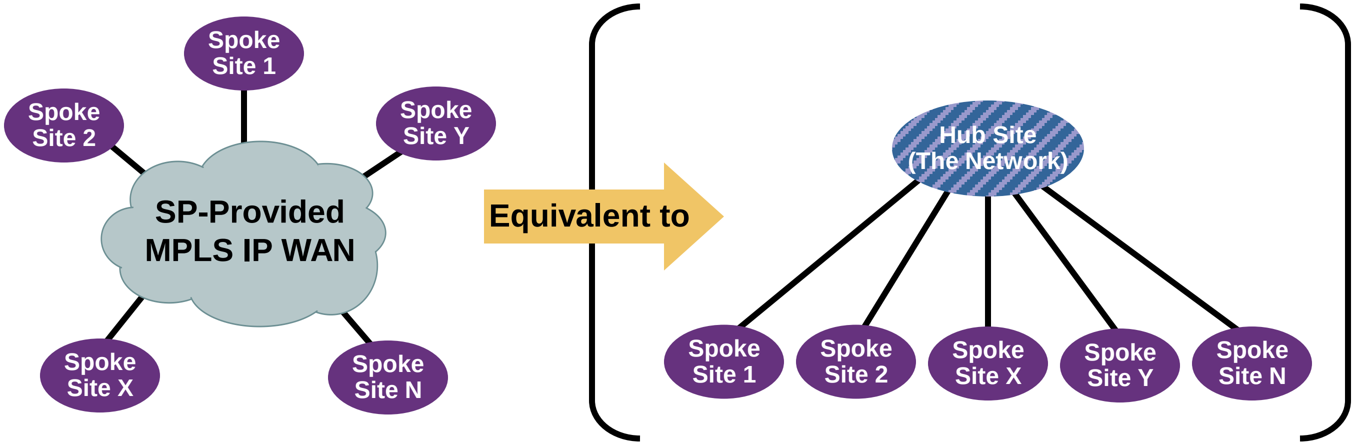


Hierarchical Network Design

- Hierarchical design used to be…
  - Three routed layers
  - Core, distribution, access
  - Only one hierarchical structure end-to-end
- Hierarchical design has become any design that…
  - Splits the network up into “places,” or “regions”
  - Separates these “regions” by hiding information
  - Organises these “regions” around a network core
  - “hub and spoke” at a macro level



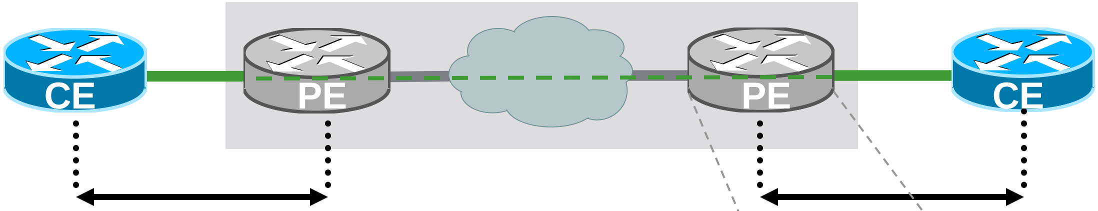
MPLS VPN Topology
Definition



- MPLS WAN is provided by a service provider
- As seen by the enterprise network, every site is one IP “hop” away
- Equivalent to a full mesh, or to a “hubless” hub-and-spoke

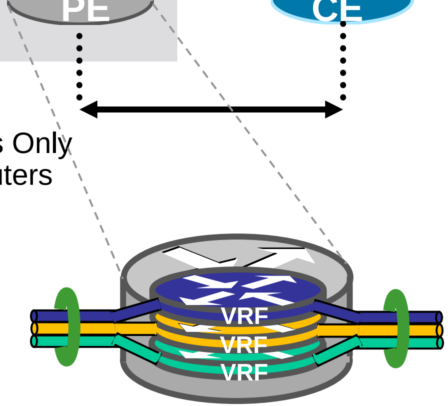
Virtual Routing and Forwarding Instance (VRF)

Provides Network Virtualisation and Path Isolation



Direct Layer 3 Adjacencies Only
Between CE and PE Routers

```
! PE Router – Multiple VRFs
ip vrf blue
 rd 65100:10
 route-target import 65100:10
 route-target export 65100:10
ip vrf yellow
 rd 65100:20
 route-target import 65100:20
 route-target export 65100:20
!
interface GigabitEthernet0/1.10
 ip vrf forwarding blue
interface GigabitEthernet0/1.20
 ip vrf forwarding yellow
```



VRF—Virtual Routing and Forwarding

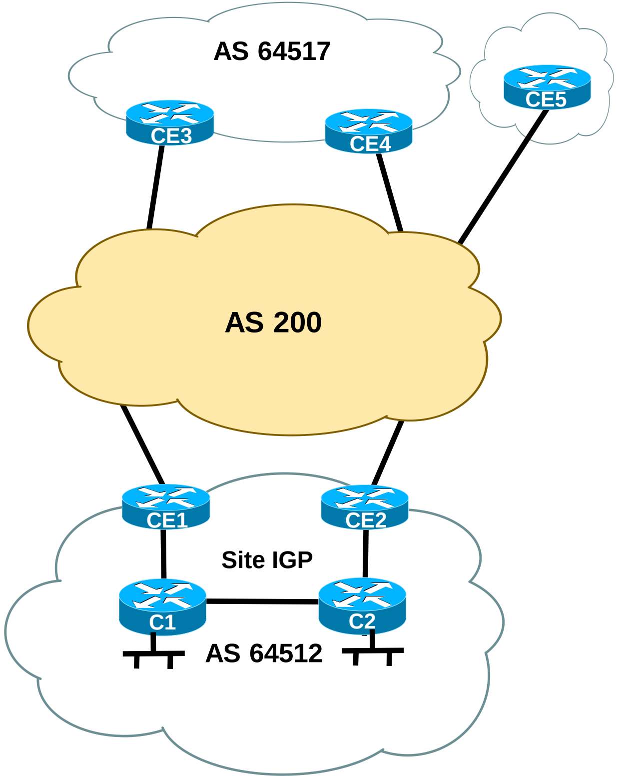
MPLS VPN Design Trends

- **Single Carrier Designs**:
  - Enterprise will home all sites into a single carrier to provide L3 MPLS VPN connectivity.
  - **Pro:** Simpler design with consistent features
  - **Con:** Bound to single carrier for feature velocity
  - **Con:** Does not protect against MPLS cloud failure with Single Provider

- **Dual Carrier Designs:**
  - Enterprise will single or dual home sites into one or both carriers to provide L3 MPLS VPN connectivity.
  - **Pro:** Protects against MPLS service failure with Single Provider
  - **Pro:** Potential business leverage for better competitive pricing
  - **Con:** Increased design complexity due to Service Implementation Differences (e.g. QoS, BGP AS Topology)
  - **Con:** Feature differences between providers could force customer to use least common denominator features.

- **Variants of these designs and site connectivity:**
  - Encryption Overlay (e.g. IPSec, DMVPN, GET VPN, etc.)
  - Sites with On-demand / Permanent backup links

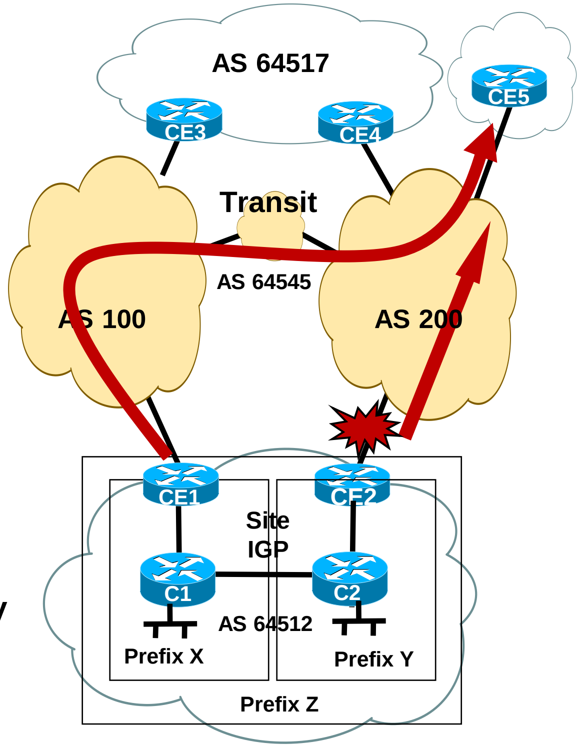
Single Carrier Site Types (Non-Transit)



- **Dual Homed Non Transit**
  - Only advertise local prefixes (^$)
  - Typically with Dual CE routers
  - BGP design:
    - eBGP to carrier
    - iBGP between CEs
  - Redistribute cloud learned routes into site IGP
- **Single Homed Non Transit**
  - Advertise local prefixes and optionally use default route.

Dual Carrier: Transit vs. Non Transit

- To guarantee single homed site reachability to a dual homed site experiencing a failure, transit sites had to be elected.
- Transit sites would act as a BGP bridge transiting routes between the two provider clouds.
- To minimise latency costs of transits, transits need to be selected with geographic diversity (e.g. from the East, West and Central US.)

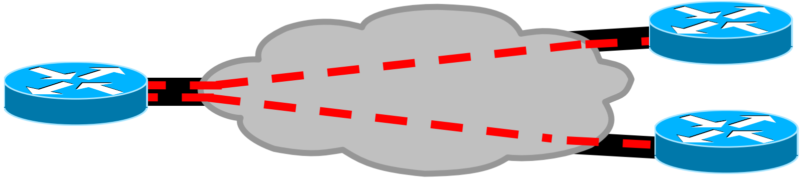


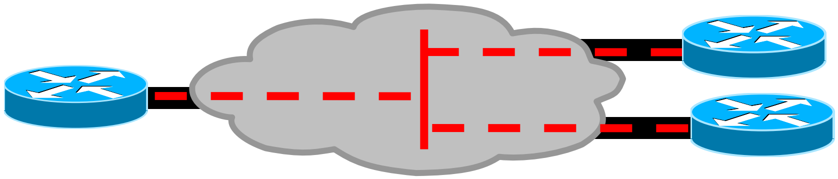
Single vs. Dual Carriers

Single Provider	Dual Providers
Pro: Common QoS support model	**Pro:** More fault domains
Pro: Only one carrier to "tune"	**Pro:** More product offerings to business
Pro: Reduced head end circuits	**Pro:** Ability to leverage vendors for better pricing
Pro: Overall simpler design	**Pro:** Nice to have a second vendor option
Con: Carrier failure could be catastrophic	**Con:** Increased Bandwidth "Paying for bandwidth twice"
Con: Do not have another carrier "in your pocket"	**Con:** Increased overall design complexity
	Con: May be reduced to "common denominator" between carriers

Resiliency Drivers vs. Simplicity

Metro Ethernet Service (L2VPN)





E-Line (Point-to-Point)

- Replaces TDM private line
- Point-to-point EVCs offer predictable performance for applications
- One or more EVCs allowed per single physical interface (UNI)
- Ideal for voice, video, and real-time data

E-LAN (Point-to-Multipoint)

- Offers point to multipoint for any-to-any connectivity
- Transparent to VLANs and Layer 2 control protocols
- 4 or 6 classes of QoS support
- Ideal for LAN-to-LAN bulk data

MPLS (L3VPN) vs. Metro Ethernet (L2VPN)

MPLS Layer 3 Service

- Routing protocol dependent on the carrier
- Layer 3 capability depends on carrier offering
  - QoS (4 classes/6 classes)
  - IPv6 adoption
- Transport IP protocol only
- Peering with carrier for routing protocol adjacency

MetroE Layer 2 Service

- Routing protocol independent of the carrier
- Customer manages layer 3 QoS
- Capable of transport IP and none-IP traffic.
- Routing protocol scalability in point-to-multipoint topology

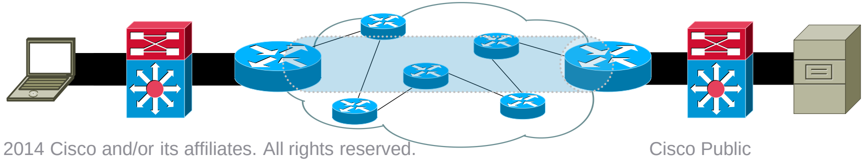
Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

Tunnelling Technologies

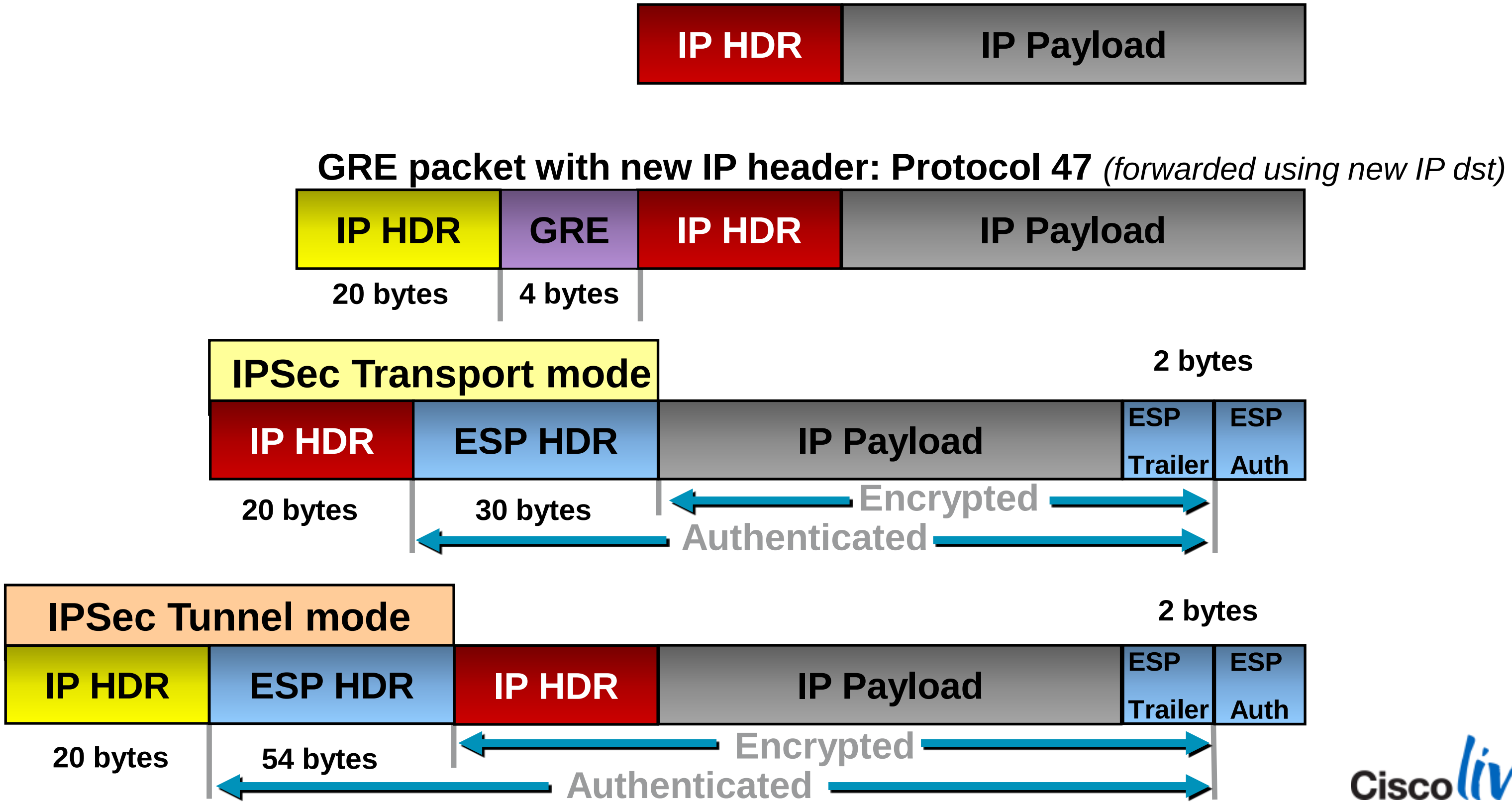
Packet Encapsulation over IP

- IPSec—Encapsulating Security Payload (ESP)
  - Strong encryption
  - IP Unicast only
- Generic Routing Encapsulation (GRE)
  - IP Unicast, Multicast, Broadcast
  - Multiprotocol support
- Layer 2 Tunnelling Protocol—Version 3 (L2TPv3)
  - Layer 2 payloads (Ethernet, Serial,…)
  - Pseudowire capable
- Other Tunnelling Technologies – L3VPNomGRE, OTV, VxLAN, LISP, OTP



Tunnelling

GRE and IPSec Transport and Tunnel Modes



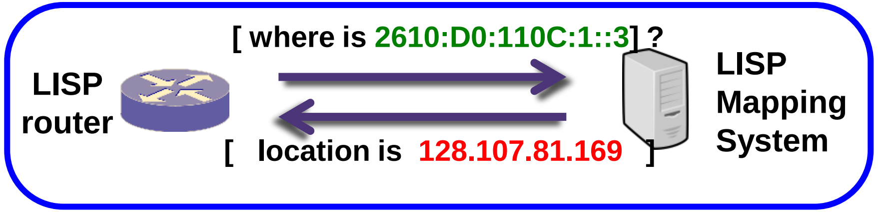
Locator/Identifier Separation Protocol (LISP)

Dynamic Tunnelling Analogous to a DNS but for Network Infrastructure

- DNS resolves IP addresses for URLs

DNS
URL Resolution

- LISP resolves locators for queried identities



LISP
Identity-to-location
Map Resolution

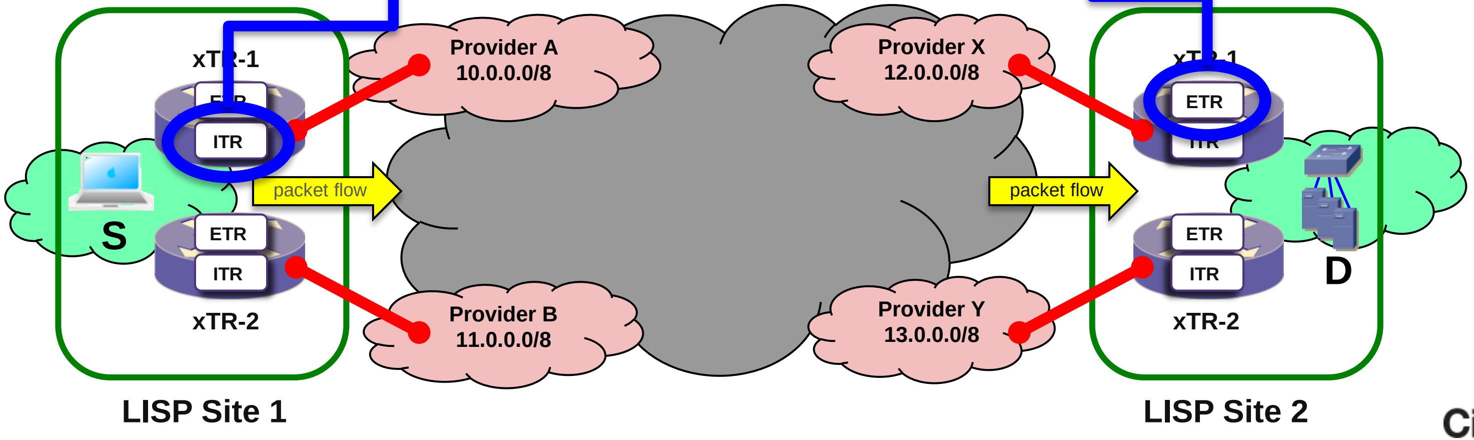
This Topic Is Covered in Detail in BRKRST-3045

LISP Overview - Terminologies

- **EID (Endpoint Identifier)** is the IP address of a host – just as it is today
- **RLOC (Routing Locator)** is the IP address of the LISP router for the host
- **EID-to-RLOC mapping** is the distributed architecture that maps **EIDs** to **RLOCs**

ITR – Ingress Tunnel Router
- Receives packets from site-facing interfaces
- Encap to remote LISP sites, or native-fwd to non-LISP sites

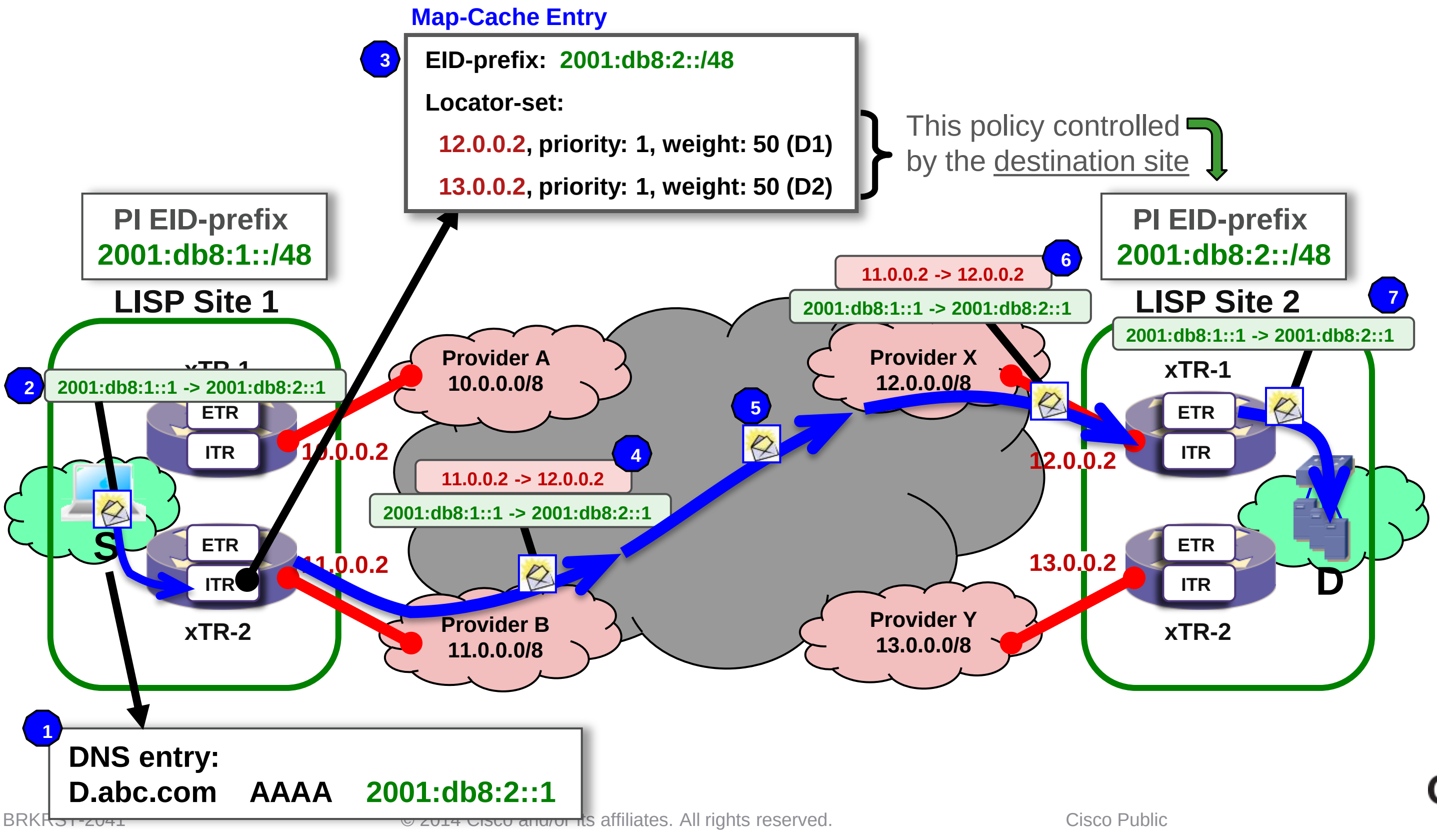
ETR – Egress Tunnel Router
- Receives packets from core-facing interfaces
- De-cap, deliver packets to local **EIDs** at site



Cisco live!

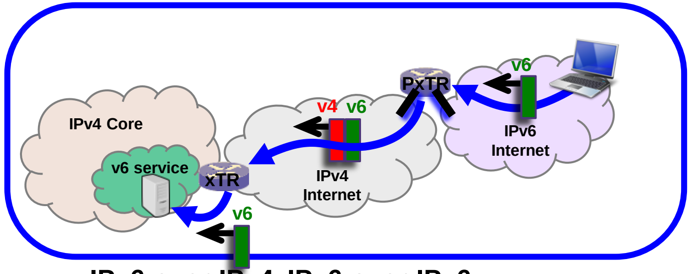
LISP Operation Example

LISP Data Plane - Unicast Packet Forwarding



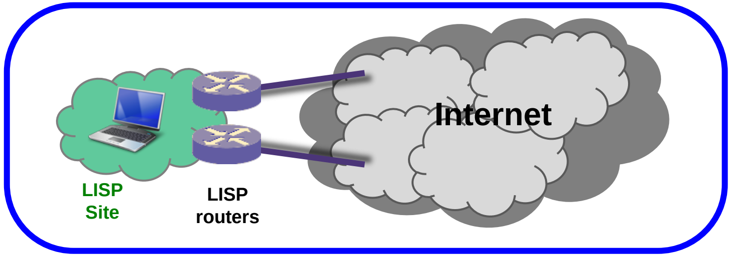
LISP Use Cases

IPv6 Transition



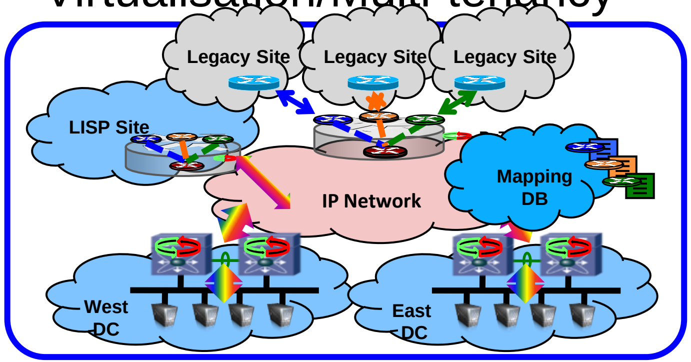
- IPv6-over-IPv4, IPv6-over-IPv6
- IPv4-over-IPv6, IPv4-over-IPv4

Efficient Multi-Homing



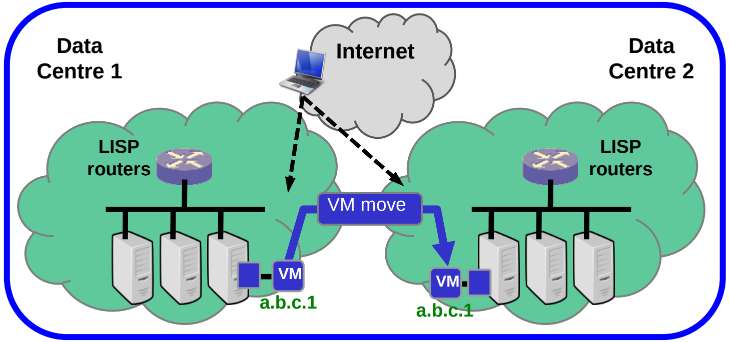
- IP Portability
- Ingress Traffic Engineering Without BGP

Virtualisation/Multi-tenancy



- Large Scale Segmentation

Data Centre/ VM Mobility

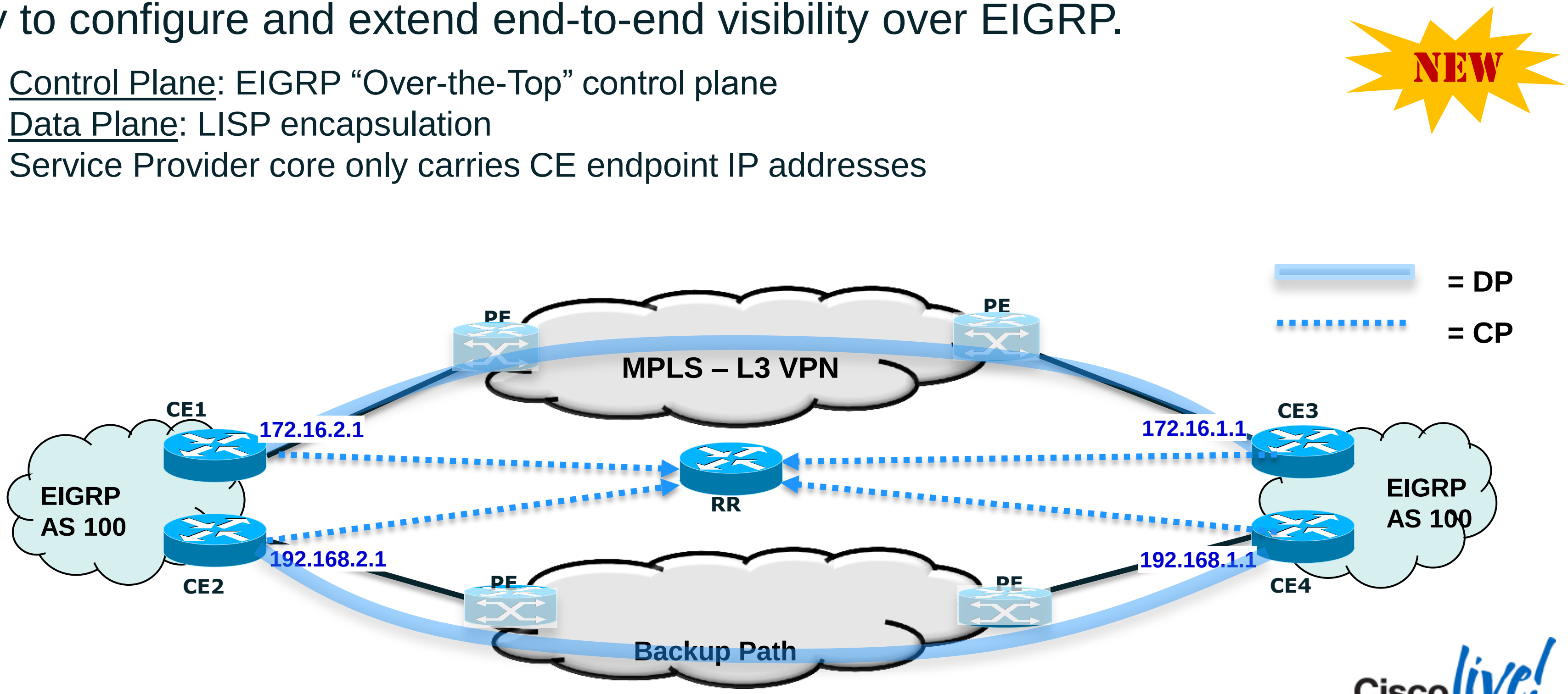


- Cloud / Layer 3 VM Move

EIGRP OTP Solution Overview

EIGRP Over-the-Top (OTP) is a highly scalable overlay network architecture that is easy to configure and extend end-to-end visibility over EIGRP.

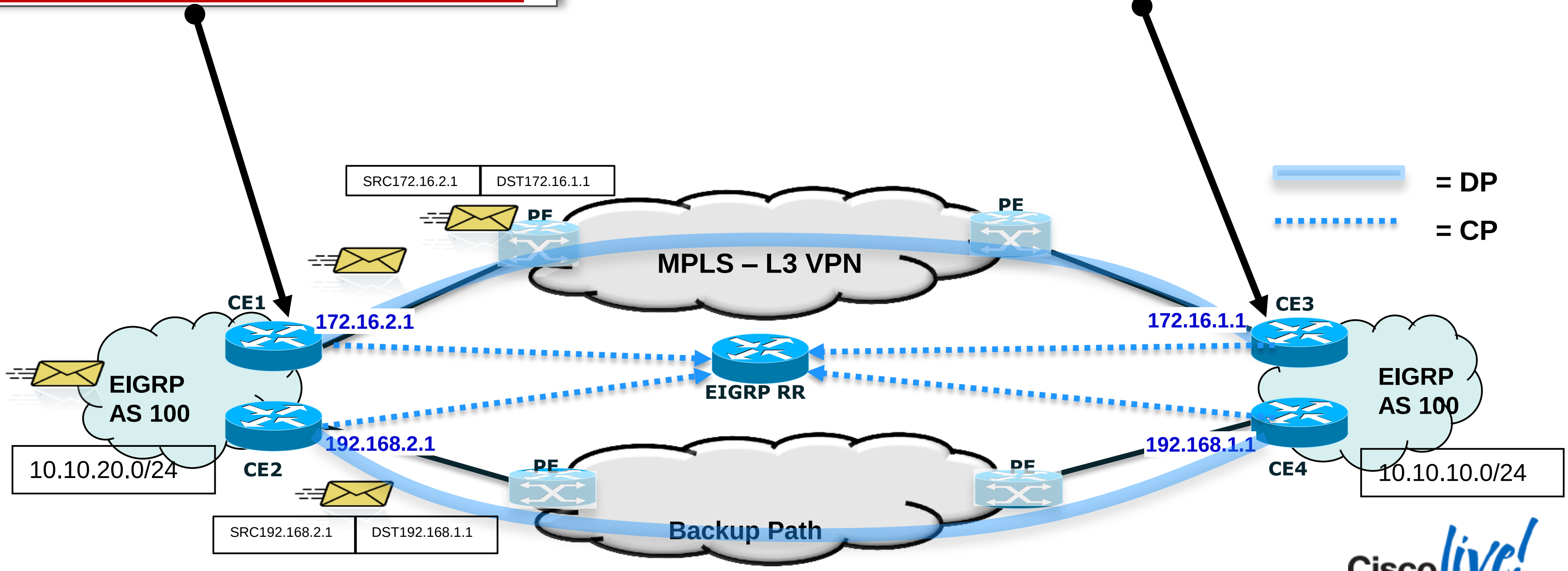
- Control Plane: EIGRP “Over-the-Top” control plane
- Data Plane: LISP encapsulation
- Service Provider core only carries CE endpoint IP addresses



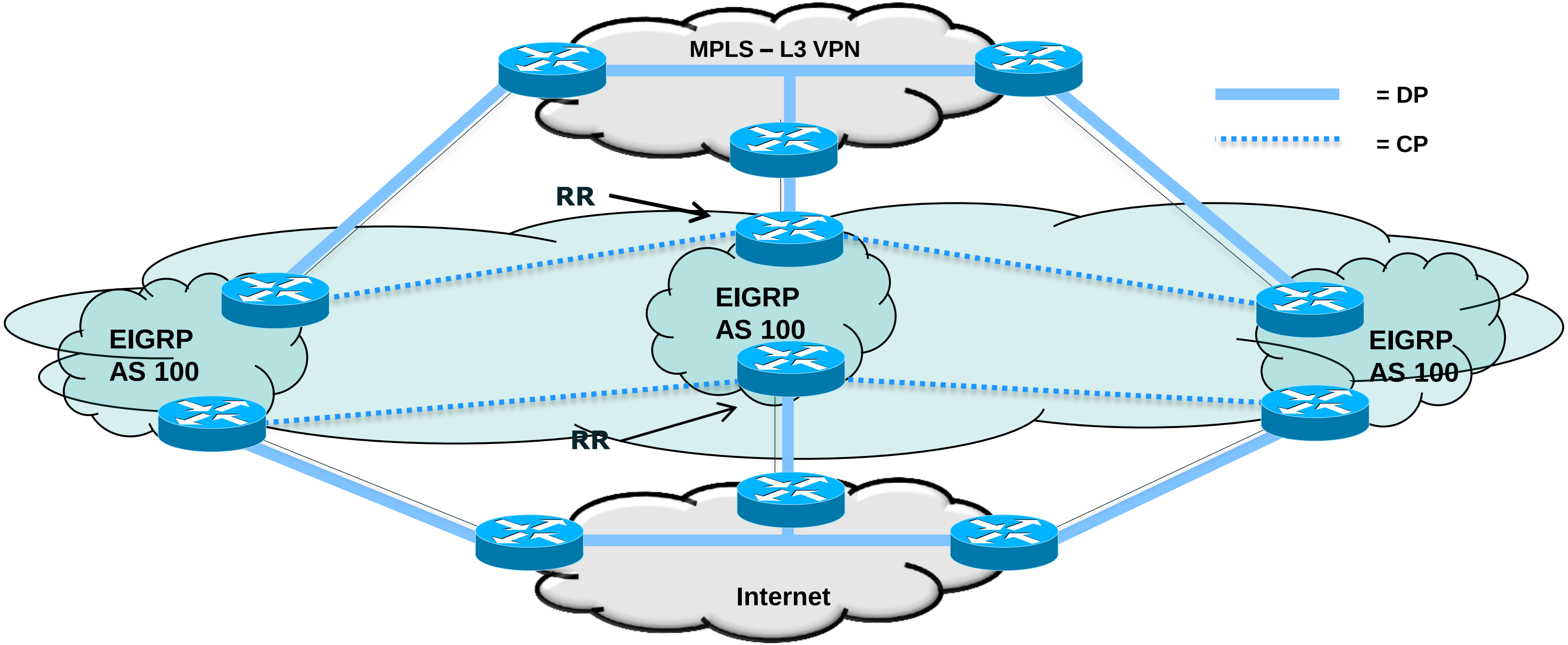
EIGRP OTP Operation

Routing Table
10.10.10.0/24 next-hop 172.16.1.1, metric 100
10.10.10.0/24 next-hop 192.168.1.1, metric 200

Routing Table
10.10.20.0/24 next-hop 172.16.2.1 metric 100
10.10.20.0/24 next-hop 192.168.2.1 metric 200

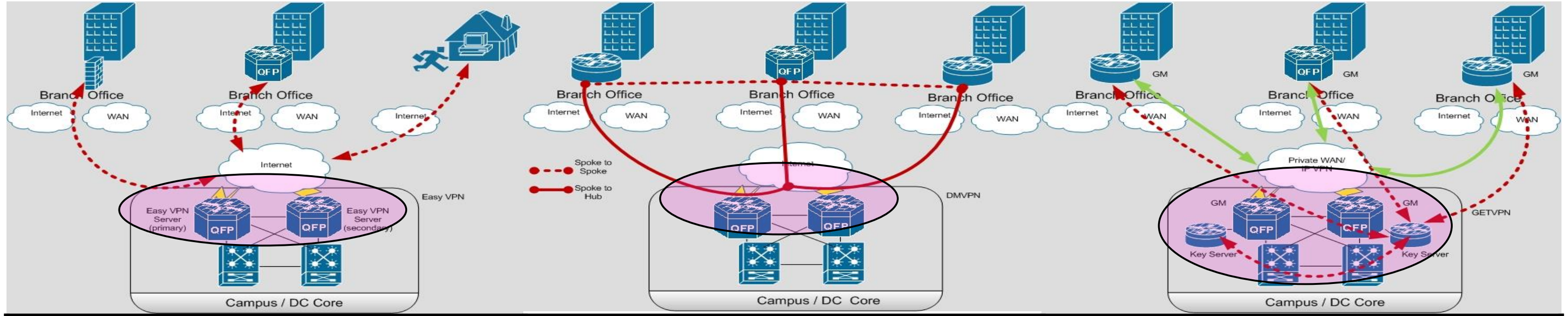


EIGRP OTP Enables Transport Agnostic Design



- Select one CE per provider to function as RR “Route Reflector” (simplifies deployment)
- EIGRP-RR for advertising CE Next-Hops, prefixes and metrics to other CE’s
- EIGRP on CE Routers configured to peer with EIGRP-RR,
- Easy to add additional site, as EIGRP-RR does not require config changes

VPN Technology
Positioning EzVPN, DMVPN, GETVPN



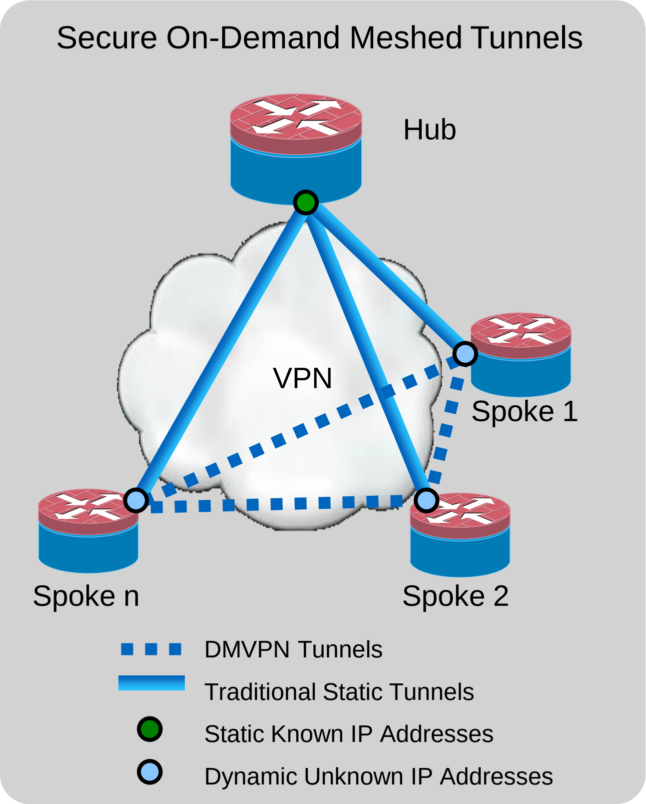
EzVPN	DMVPN	GETVPN
• LAN-like Encrypted VPN experience for a diverse set of VPN client including software clients • Enhances interoperability by consolidating tunnels from teleworkers, retail stores, or branch offices • Centralised policy and management control	• On-demand point to multipoint Encrypted VPNs • Simplified branch to branch connectivity solutions • OPEX reduction using zero-touch deployment • Resilient VPN solution combining both crypto and routing control plane	• Tunnel-less Encrypted VPNs • Any-to-Any VPN connectivity suitable for IP VPNs • No overlay routing • Simplified QoS integration with Crypto • Reduced latency and jitter due to direct communication with no central hub • Eliminates P2P IKE relationship with Group Encryption Keys

VPN Technology Comparison

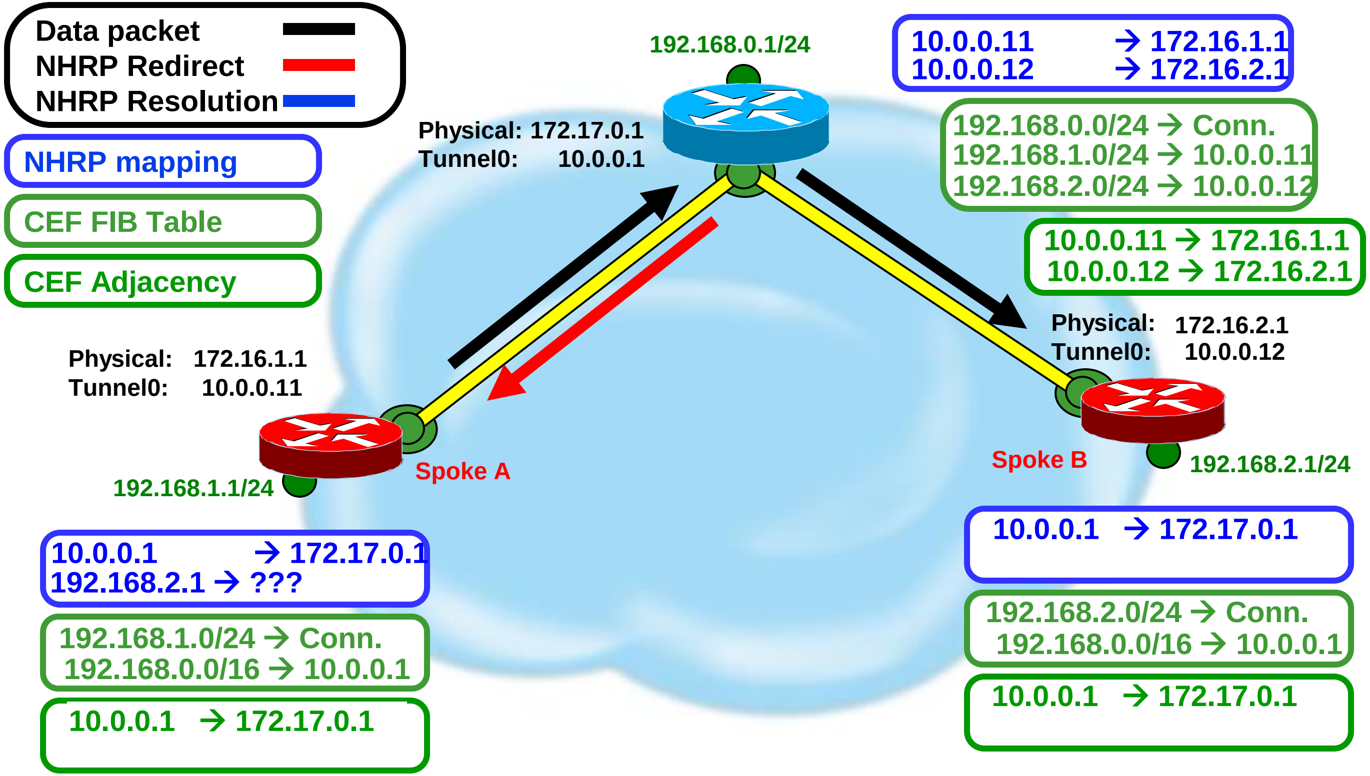
	EzVPN	DMVPN	GETVPN
Infrastructure Network	▪ Public Internet Transport	▪ Private & Public Internet Transport	▪ Private IP Transport
Network Style	▪ Hub-Spoke; (Client to Site)	▪ Hub-Spoke and Spoke-to-Spoke; (Site-to-Site)	▪ Any-to-Any; (Site-to-Site)
Routing	▪ Reverse-route Injection	▪ Dynamic routing on tunnels	▪ Dynamic routing on IP WAN
Failover Redundancy	▪ Stateful Hub Crypto Failover	▪ Route Distribution Model	▪ Route Distribution Model + Stateful
Encryption Style	▪ Peer-to-Peer Protection	▪ Peer-to-Peer Protection	▪ Group Protection
IP Multicast	▪ Multicast replication at hub	▪ Multicast replication at hub	▪ Multicast replication in IP WAN network
Scalability	▪ Unlimited ▪ 3000+ Client/Srv	▪ Unilimit ▪ 3000+ Client/Srv	▪ 3000 GM total ▪ 1000 GM/KS

Dynamic Multipoint VPN

- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel

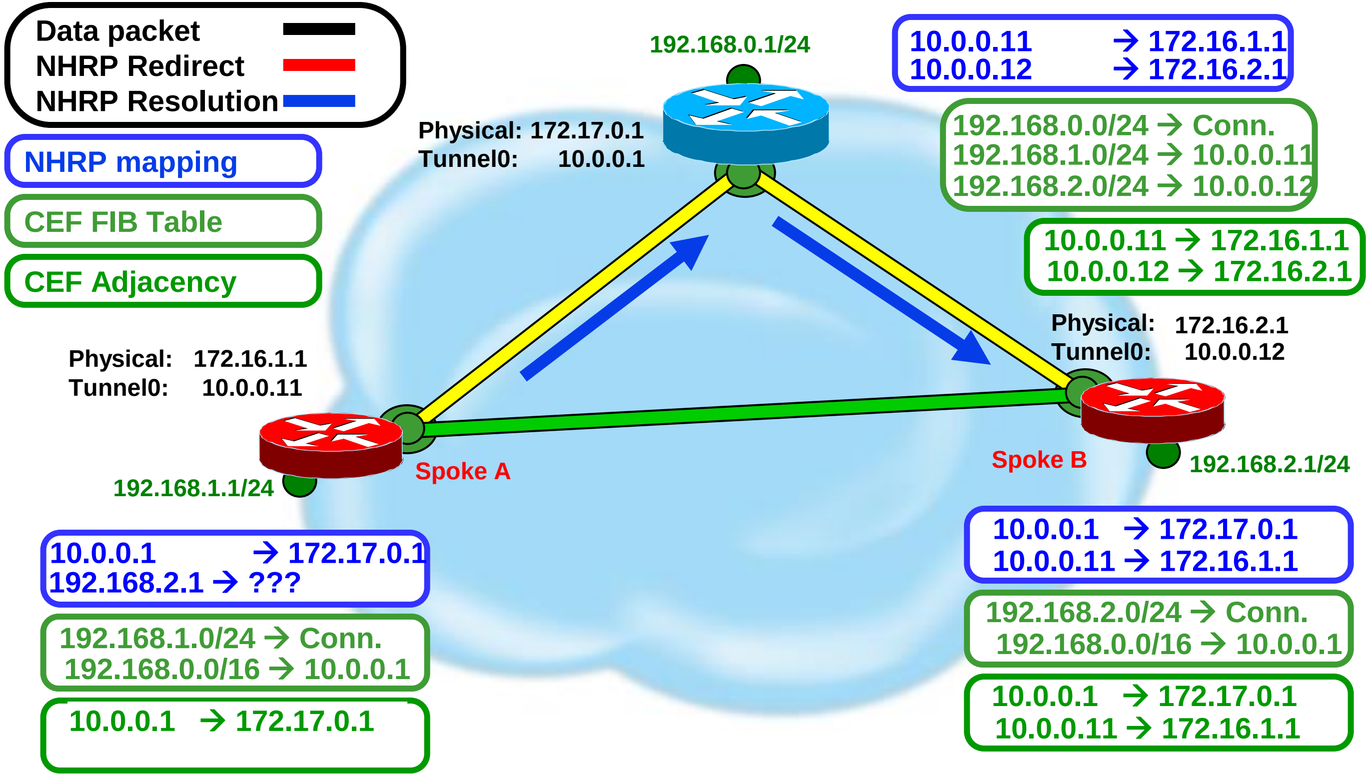


Dynamic Multipoint VPN (DMVPN)
Operational Example

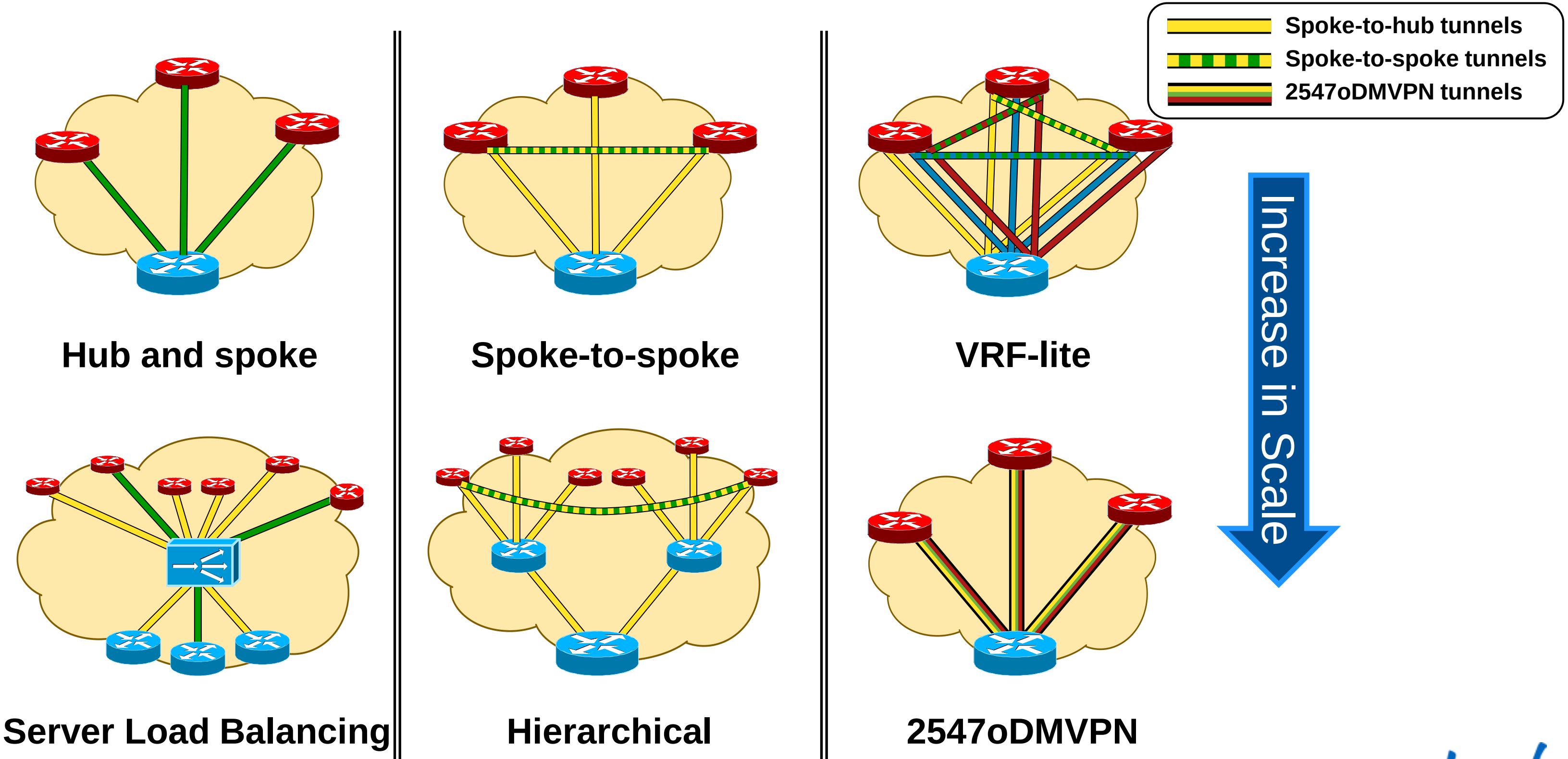


Dynamic Multipoint VPN (DMVPN)

Operational Example (cont.)



Network Designs

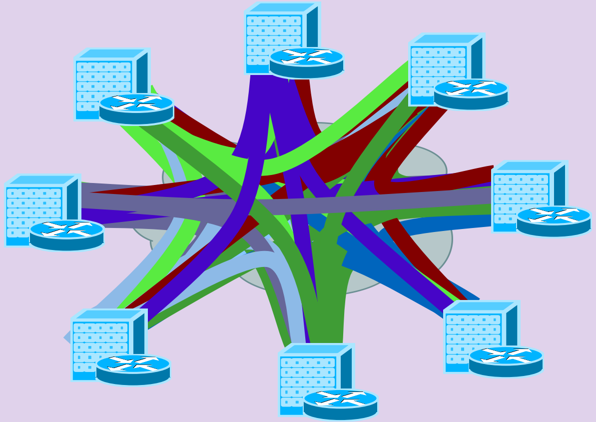


Any-to-Any Encryption

Before and After GETVPN

Public/Private WAN

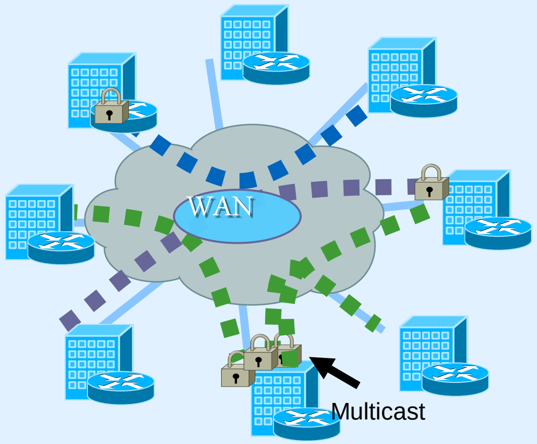
Before: IPSec P2P Tunnels



- Scalability—an issue (N^2 problem)
- Overlay routing
- Any-to-any instant connectivity can't be done to scale
- Limited QoS
- Inefficient Multicast replication

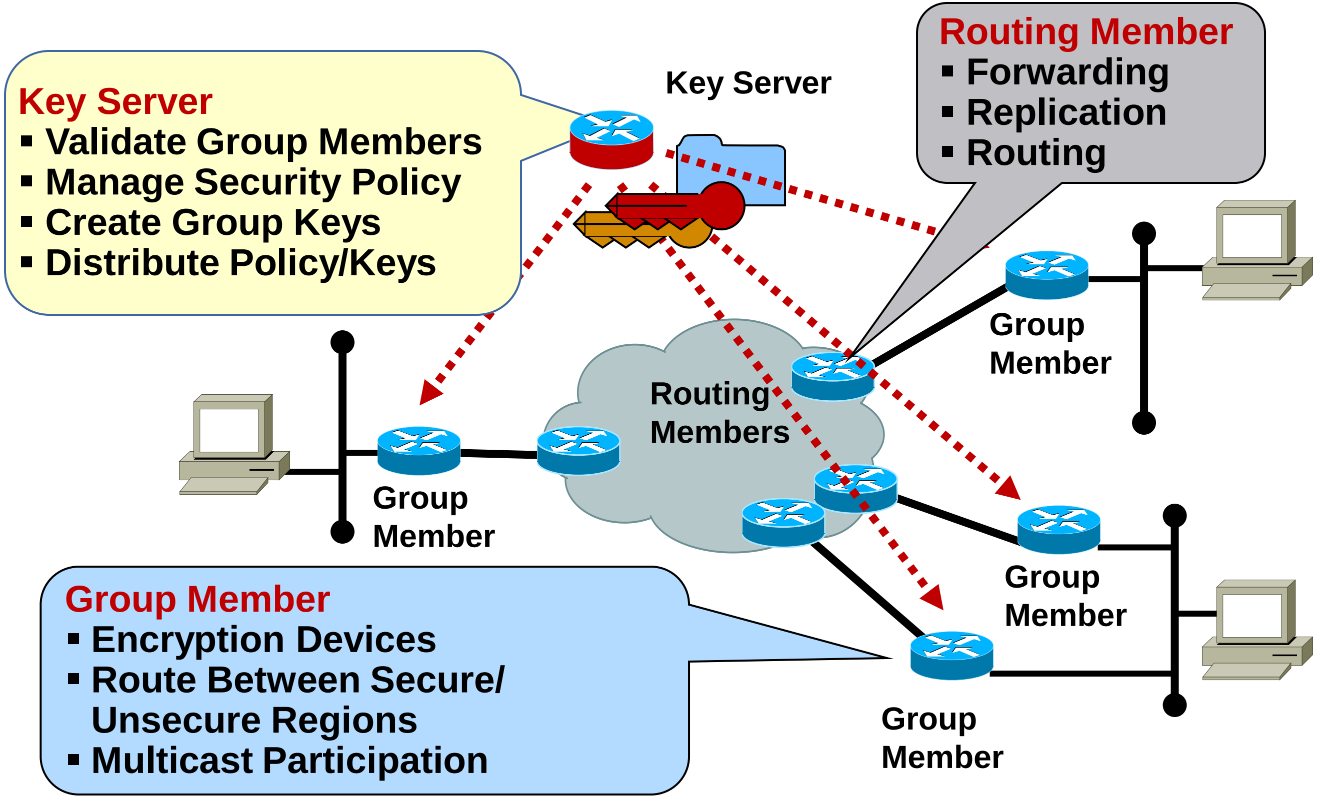
Private WAN

After: Tunnel-Less VPN

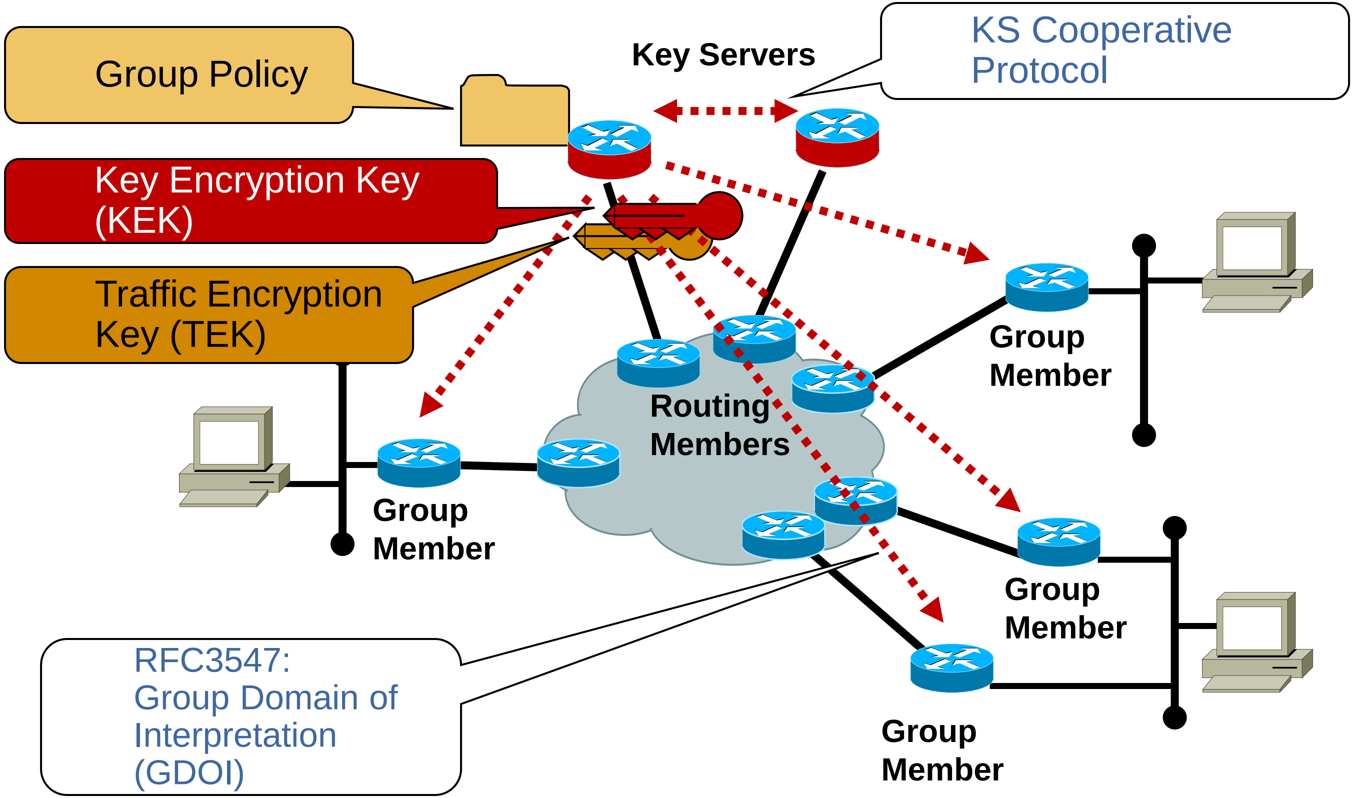


- Scalable architecture for any-to-any connectivity and encryption
- No overlays—native routing
- Any-to-any instant connectivity
- Enhanced QoS
- Efficient Multicast replication

Group Security Functions



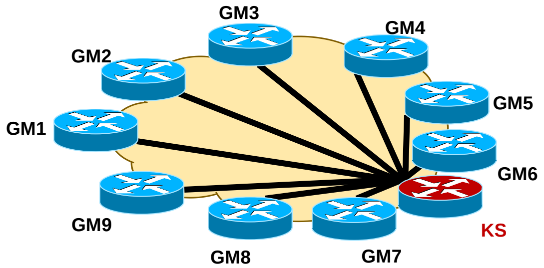
Group Security Elements



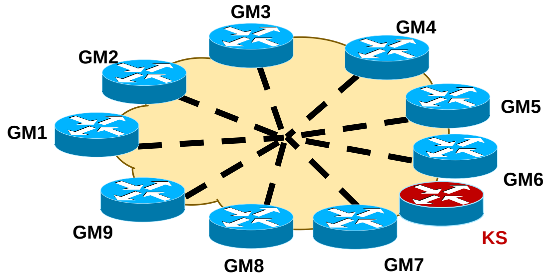
GETVPN - Group Key Technology

Operation Example

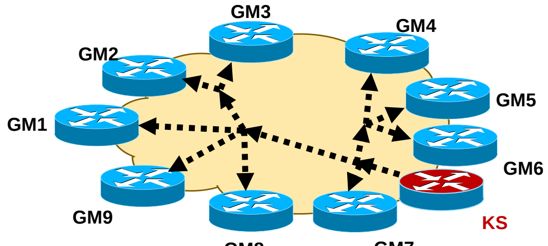
- **Step 1**: Group Members (GM) "register" via GDOI (IKE) with the Key Server (KS)
  - KS authenticates and authorises the GM
  - KS returns a set of IPsec SAs for the GM to use



- **Step 2**: Data Plane Encryption
  - GM exchange encrypted traffic using the group keys
  - The traffic uses IPSec Tunnel Mode with "address preservation"

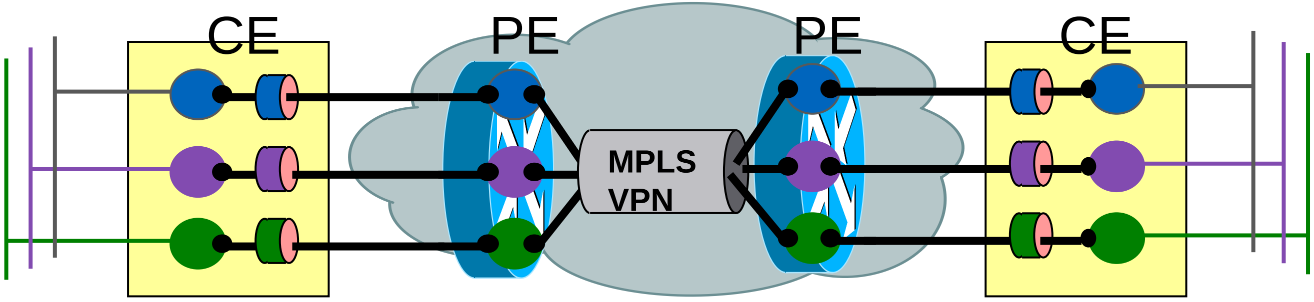


- **Step 3**: Periodic Rekey of Keys
  - KS pushes out replacement IPsec keys before current IPsec keys expire; This is called a "rekey"

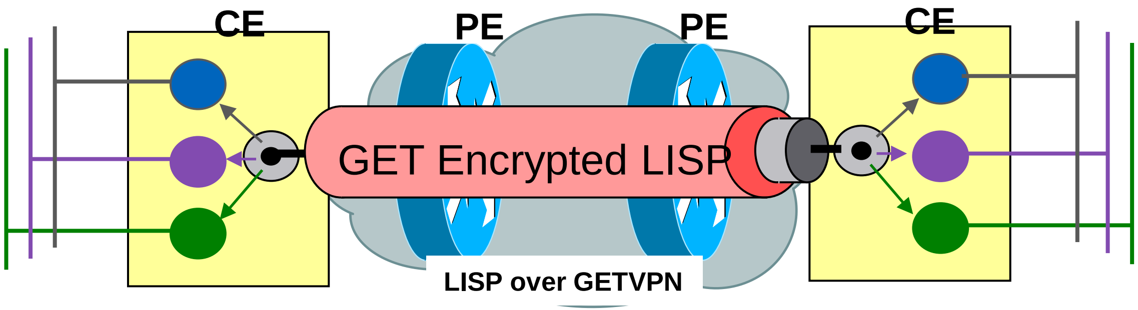


GETVPN Virtualisation Deployment Model

GETVPN Segmented WAN



LISP with GETVPN

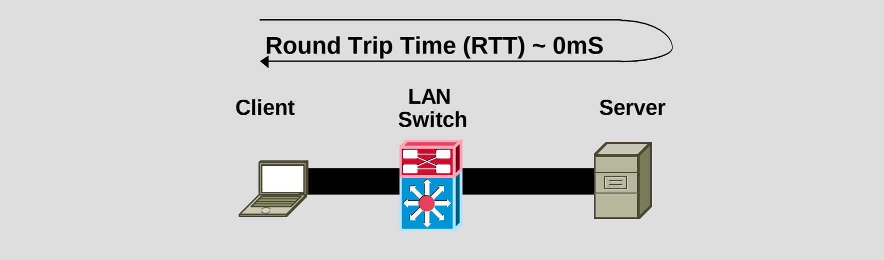


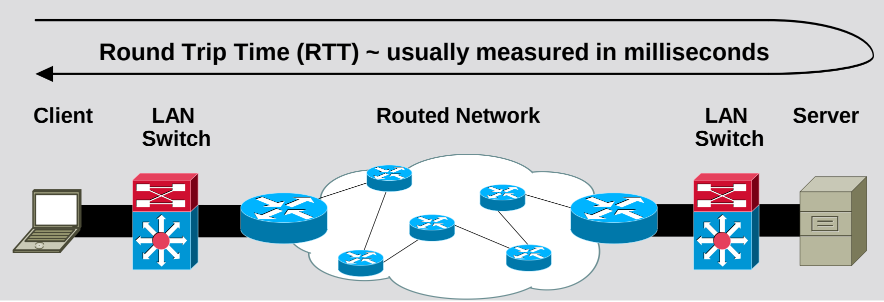
Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

The WAN Is the Barrier to Branch
Application Performance

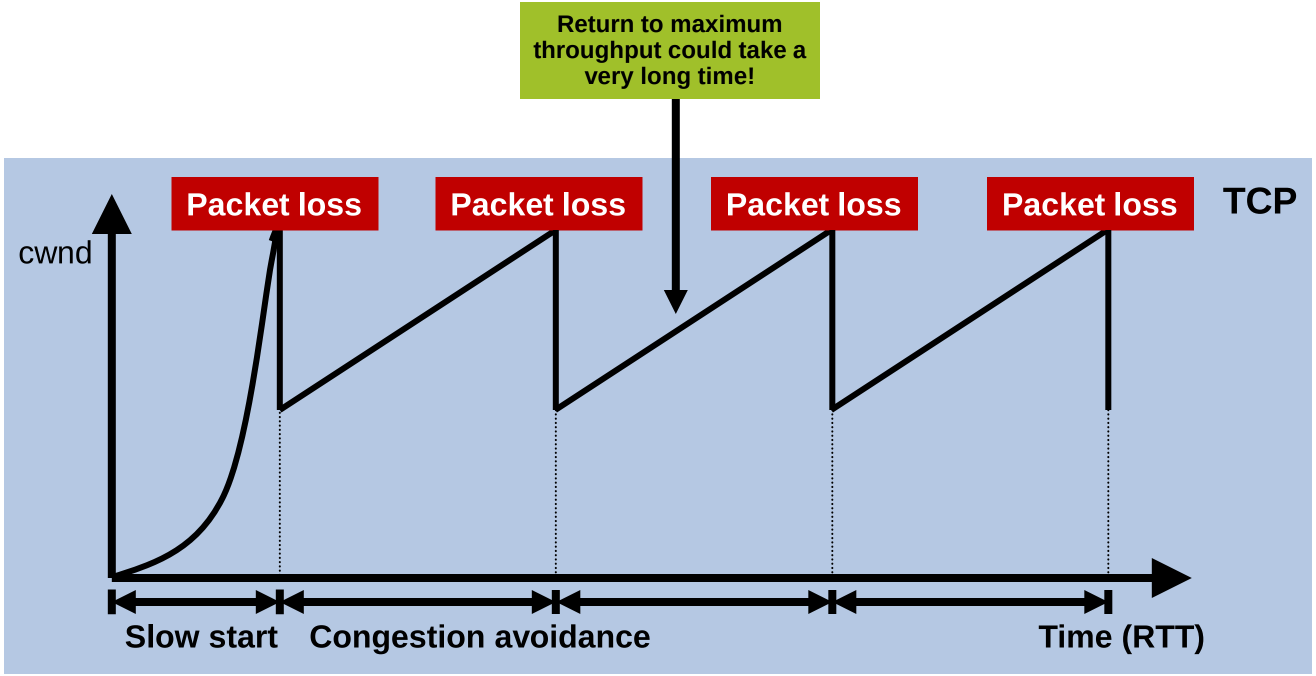
- Applications are designed to work well on LAN's
  - High bandwidth
  - Low latency
  - Reliability
- WANs have opposite characteristics
  - Low bandwidth
  - High latency
  - Packet loss





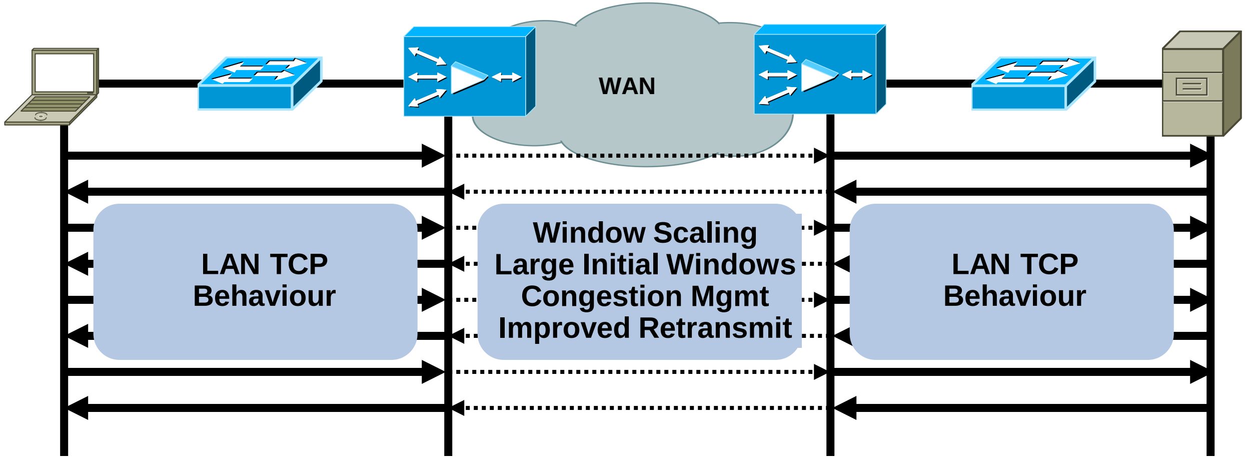
WAN Packet Loss and Latency =
Slow Application Performance =
Keep and manage servers in branch offices ($$$)

TCP Behaviour



WAAS - TCP Performance Improvement

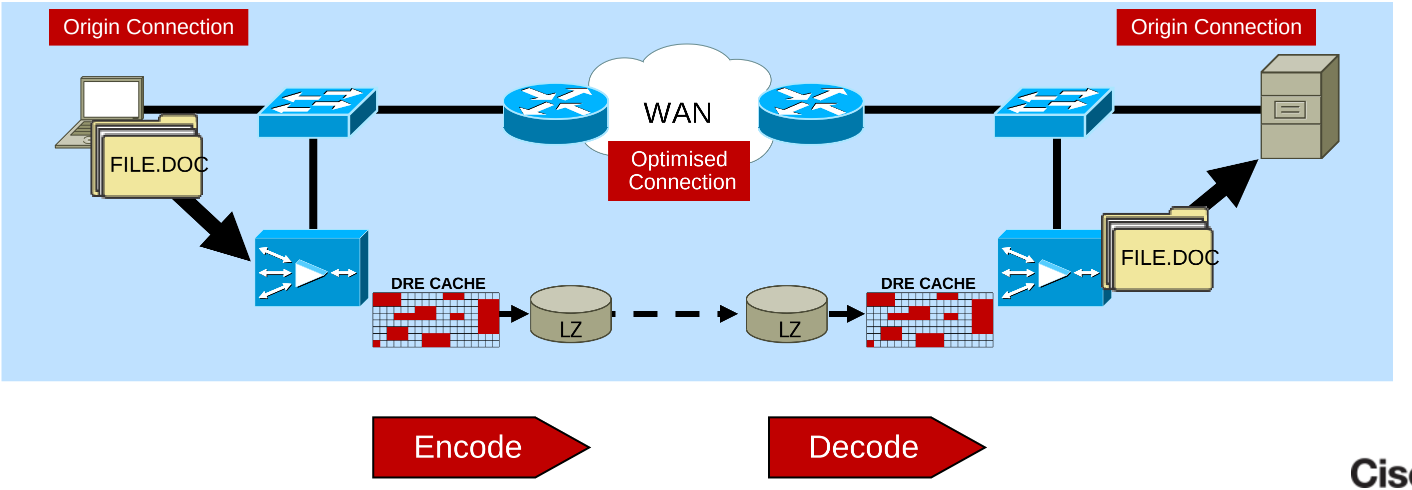
- Transport Flow Optimisation (TFO) overcomes TCP and WAN bottlenecks
- Shields nodes connections from WAN conditions
  - Clients experience fast acknowledgement
  - Minimise perceived packet loss
  - Eliminate need to use inefficient congestion handling



WAAS Overview

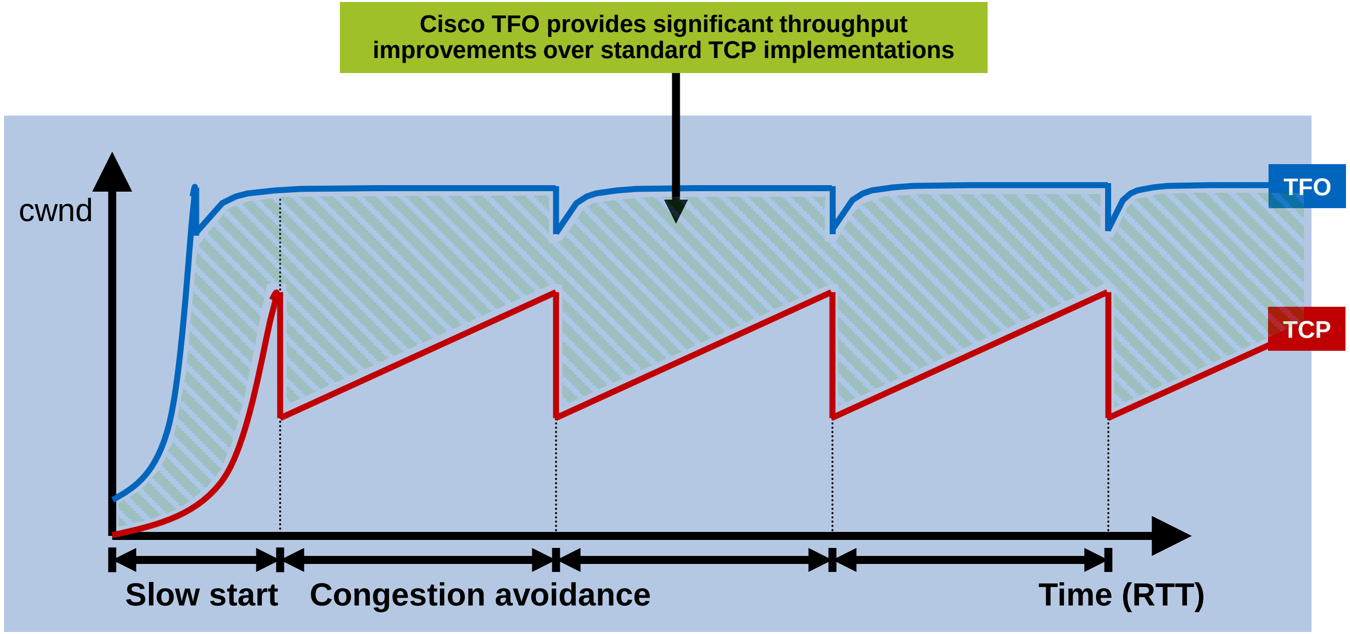
DRE and LZ Manage Bandwidth Utilisation

- Data Redundancy Elimination (DRE) provides advanced compression to eliminate redundancy from network flows regardless of application
- LZ compression provides generic compression for all traffic

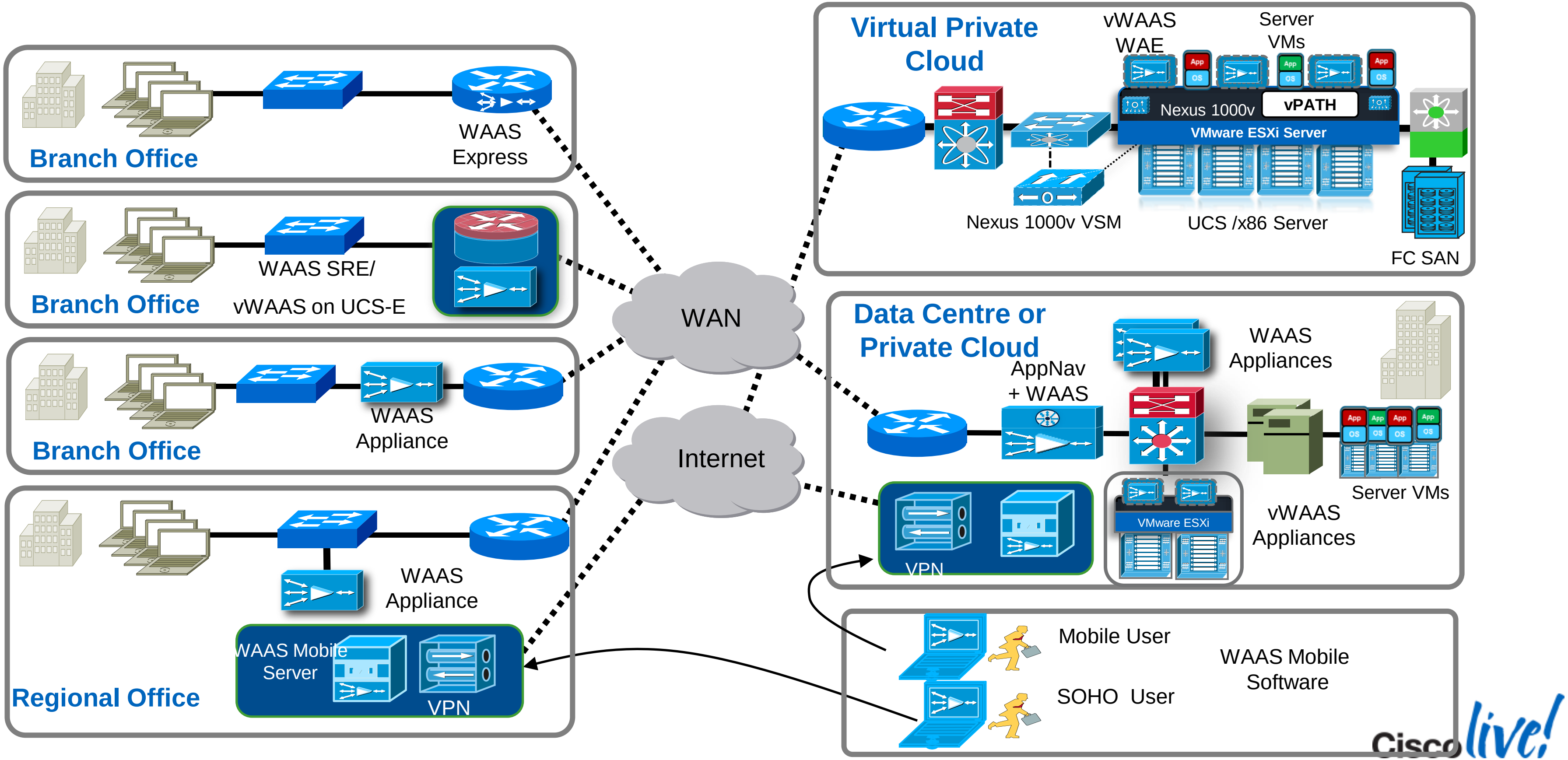


Comparing TCP and Transport

Flow Optimisation



Cisco WAAS Deployment Options for Branch



Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

Quality of Service Operations

How Does It Work and Essential Elements

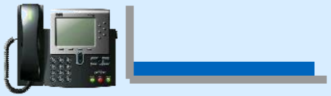
Classification and Marking	Queuing and Dropping	Post-Queuing Operations
IDENTIFY & PRIORITIZE	MANAGE & SORT	PROCESS & SEND

- **Classification and Marking:**
  - The first element to a QoS policy is to classify/identify the traffic that is to be treated differently. Following classification, marking tools can set an attribute of a frame or packet to a specific value.
- **Policing:**
  - Determine whether packets are conforming to administratively-defined traffic rates and take action accordingly. Such action could include marking, remarking or dropping a packet.
- **Scheduling (including Queuing and Dropping):**
  - Scheduling tools determine how a frame/packet exits a device. Queuing algorithms are activated only when a device is experiencing congestion and are deactivated when the congestion clears.

Enabling QoS in the WAN

Traffic Profiles and Requirements

Voice



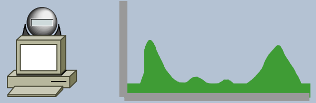
- Smooth
- Benign
- Drop sensitive
- Delay sensitive
- UDP priority

Bandwidth per Call Depends on Codec, Sampling-Rate, and Layer 2 Media

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 1%
- Bandwidth (30-128Kbps)

One-Way Requirements

SD Video Conf



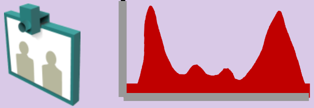
- Bursty
- Greedy
- Drop sensitive
- Delay sensitive
- UDP priority

SD/VC has the Same Requirements as VoIP, but Has Radically Different Traffic Patterns (BW Varies Greatly)

- Latency ≤ 150 ms
- Jitter ≤ 30 ms
- Loss ≤ 0.05%
- Bandwidth (1Mbps)

One-Way Requirements

Telepresence



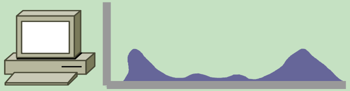
- Bursty
- Drop sensitive
- Delay sensitive
- Jitter sensitive
- UDP priority

HD/VC has Tighter Requirements than VoIP in terms of jitter, and BW varies based on the resolutions

- Latency ≤ 200 ms
- Jitter ≤ 20 ms
- Loss ≤ 0.10%
- Bandwidth (5.5-16Mbps)

One-Way Requirements

Data



- Smooth/bursty
- Benign/greedy
- Drop insensitive
- Delay insensitive
- TCP retransmits

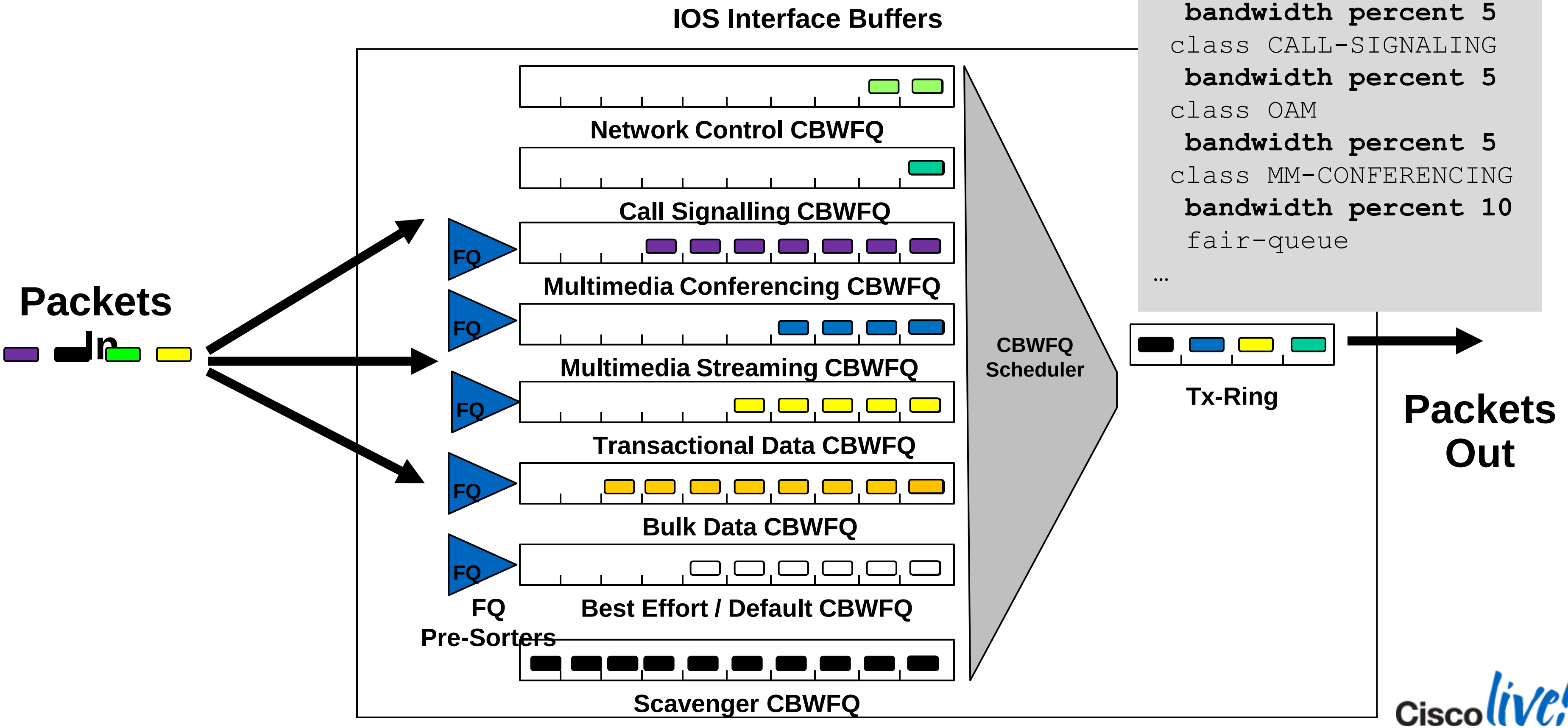
Traffic patterns for Data Vary Among Applications

- Data Classes:
- Mission-Critical Apps
- Transactional/Interactive Apps
- Bulk Data Apps
- Best Effort Apps (Default)

Scheduling Tools

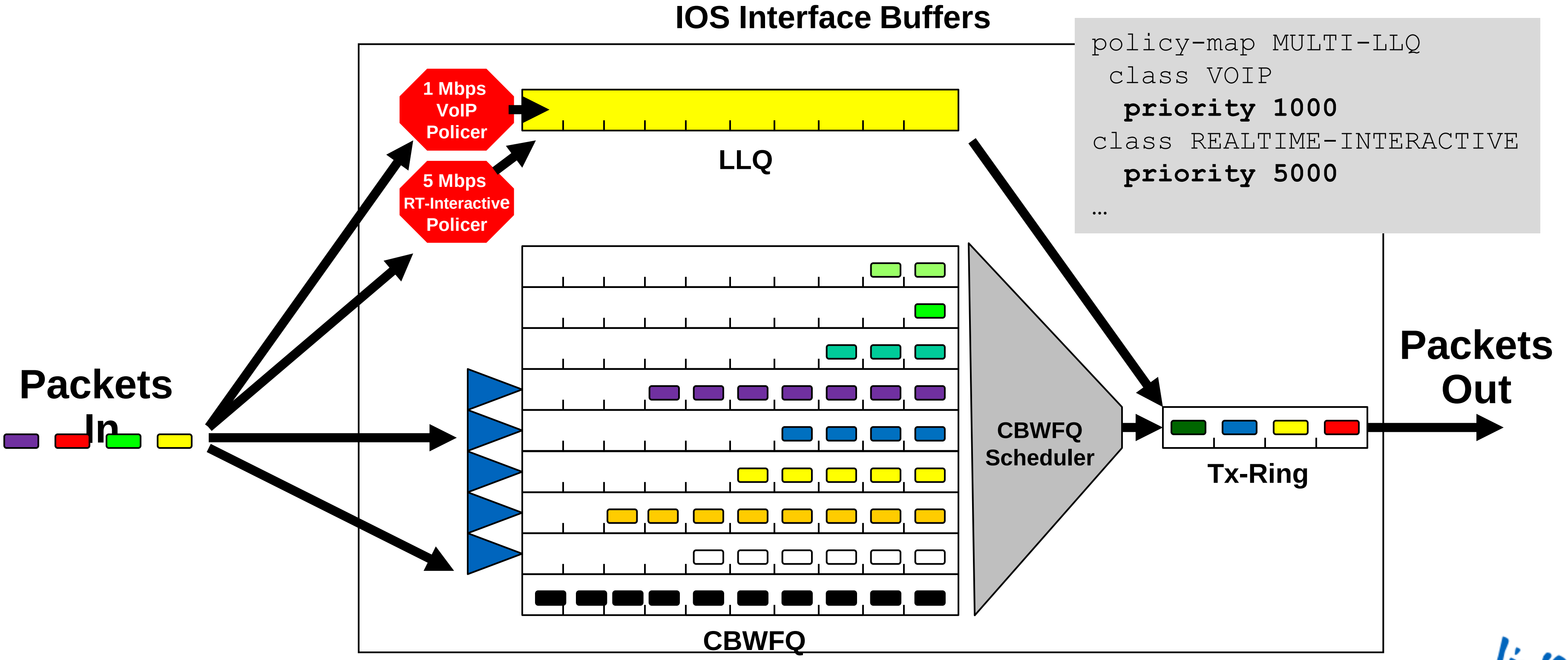
LLQ/CBWFQ Subsystems

```
policy-map CBWFQ
 class NETWORK-CONTROL
  bandwidth percent 5
 class CALL-SIGNALING
  bandwidth percent 5
 class OAM
  bandwidth percent 5
 class MM-CONFERENCING
  bandwidth percent 10
  fair-queue
…
```



Scheduling Tools

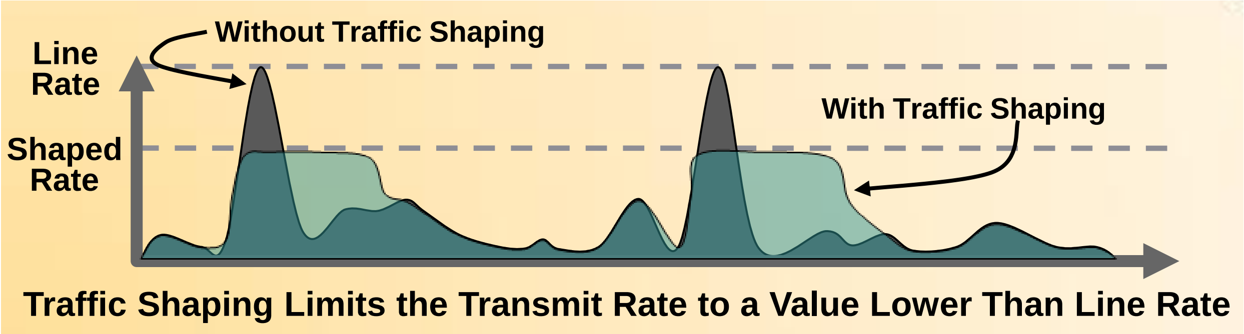
LLQ/CBWFQ Subsystems




```
policy-map MULTI-LLQ
 class VOIP
  priority 1000
class REALTIME-INTERACTIVE
  priority 5000
…
```

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSWAN_40.html#wp129469

Traffic Shaping



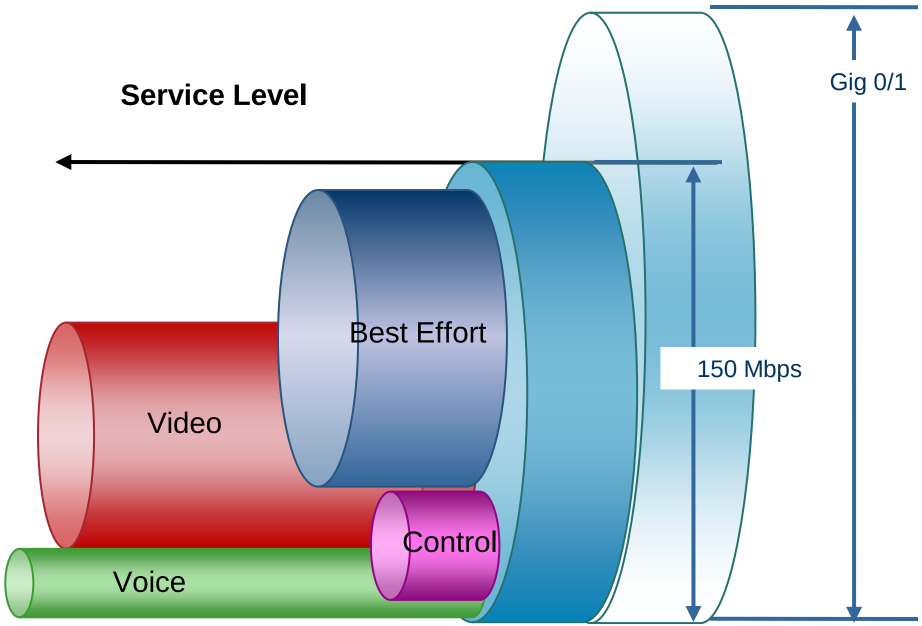
- Policers typically drop traffic
- Shapers typically delay excess traffic, smoothing bursts and preventing unnecessary drops
- Very common with Ethernet WAN, as well as Non-Broadcast Multiple-Access (NBMA) network topologies such as Frame-Relay and ATM

Hierarchical QoS For Subrate Service

H-QoS Policy on WAN Interface, Shaper = CIR

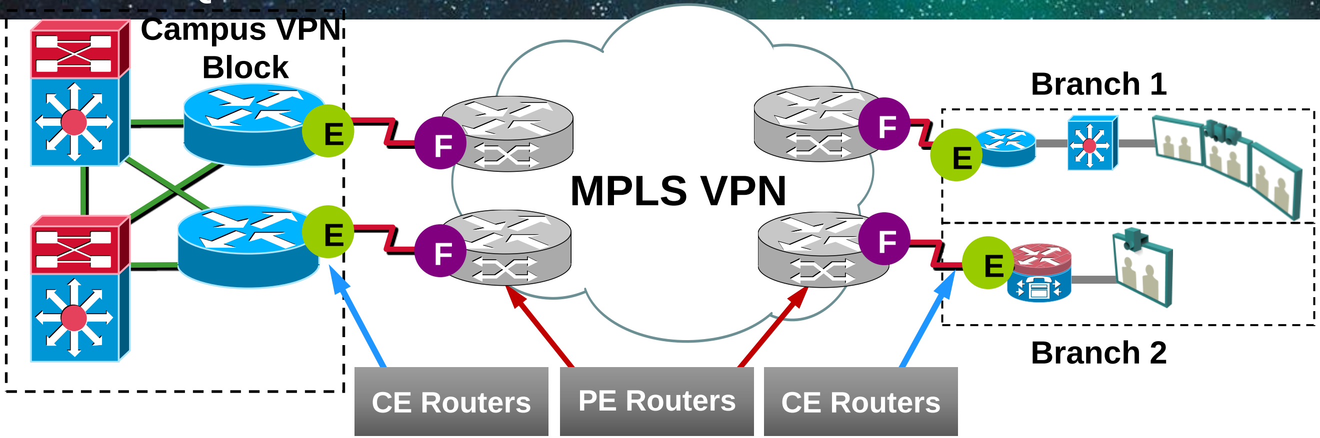
Two Levels MQC

```
Policy-map PARENT
   class class-default
    shape average 150000000
    service-policy output CHILD

Policy-map CHILD
    class Voice
      police cir percent 10
      priority level 1
    class Video
      police cir percent 20
      priority level 2
    class Control
      bandwidth remaining ration 1
    class class-default
     bandwidth remaining ratio 9

Interface gigabitethernet 0/1
  service-policy output PARENT
```



MPLS VPN QoS Considerations

MPLS VPN Port QoS Roles



Enterprise Subscriber (Unmanaged CE Routers)

E **Outbound Policies:**

HQoS Shaper (if required)

≤ 33% of BW {
+ LLQ for VoIP (EF)
+ LLQ or CBWFQ for RT-Interactive (CS4)

+ Remark RTI (if necessary)
+ CBWFQ for Signaling (CS3)
+ Remark Signaling (if necessary)

Inbound Policies:

Trust DSCP

+ Restore RT-Interactive to CS4 (if necessary)

+ Restore Signaling to CS3 (if necessary)

Service Provider:

F **Outbound Policies:**

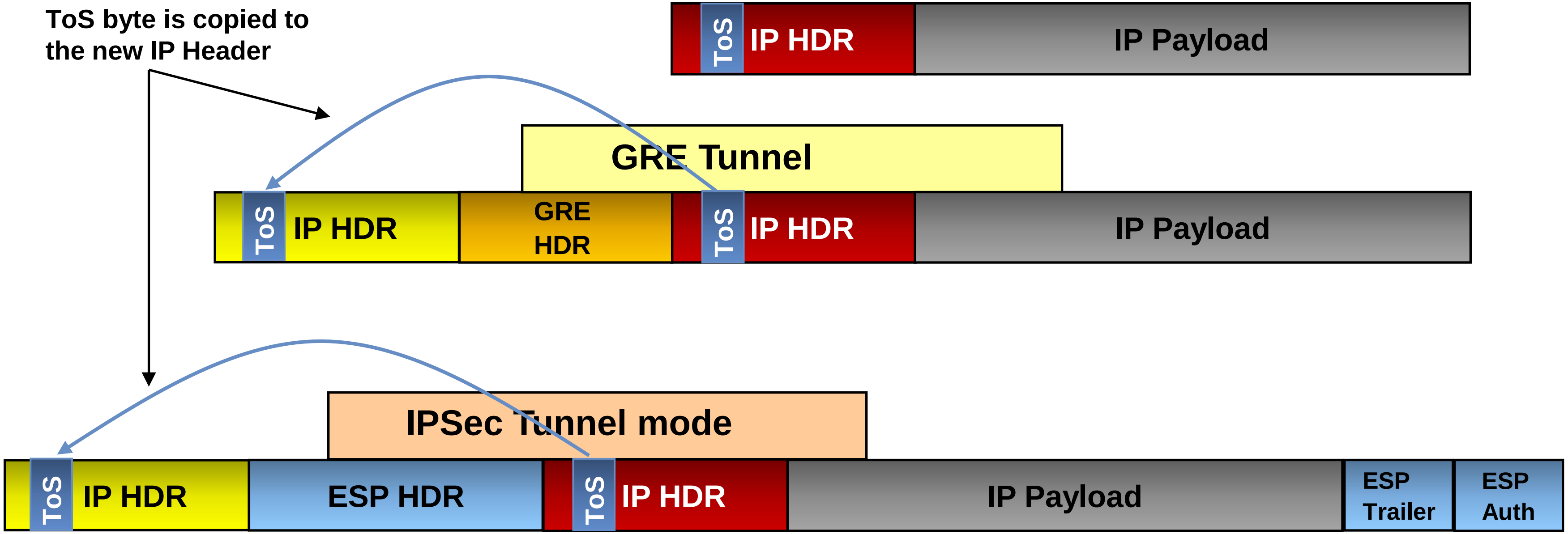
+ LLQ for Real-Time
+ CBWFQ for Critical Data

Inbound Policies:

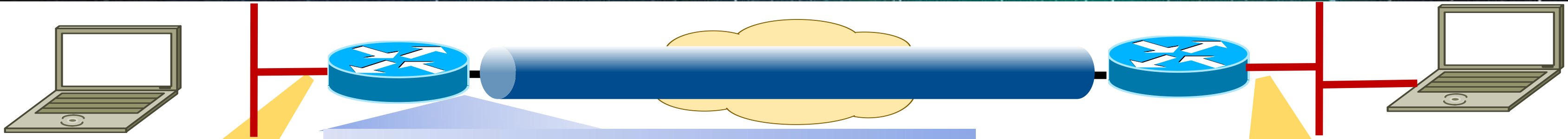
Trust DSCP
Police on a per-Class Basis

GRE/IPSec QoS Consideration

ToS Byte Preservation



GRE/IPSec Network QoS Design



DSCP AF41

Packet Initially Marked to DSCP AF41

DSCP AF41	DSCP CS5
DSCP AF41	DSCP AF41
By Default ToS Values is Copied To IPSec Header	Top-Most ToS is Rewrote on egress

DSCP AF41

Packet decapsulated To reveal the original ToS Byte

Direction of Packet Flow

Remarks the DSCP value on the encrypted/encapsulated header on egress interface

```
policy-map WAN-SP-CLASS-OUTPUT
 class VOICE
  priority percent 10
 class VIDEO-INTERACTIVE
  priority percent 23
  set ip dscp cs5
 class NETWORK-MGMT
  bandwidth percent 5
  service-policy MARK-BGP
 class class-default
  bandwidth percent 25
  random-detect
!
policy-map Int-Gig-Agg-HE
 class class-default
  shape average 1000000000
  service-policy WAN-Out
```

Per Site Traffic Shaping to Avoid Overruns

DMVPN Per-Tunnel QoS

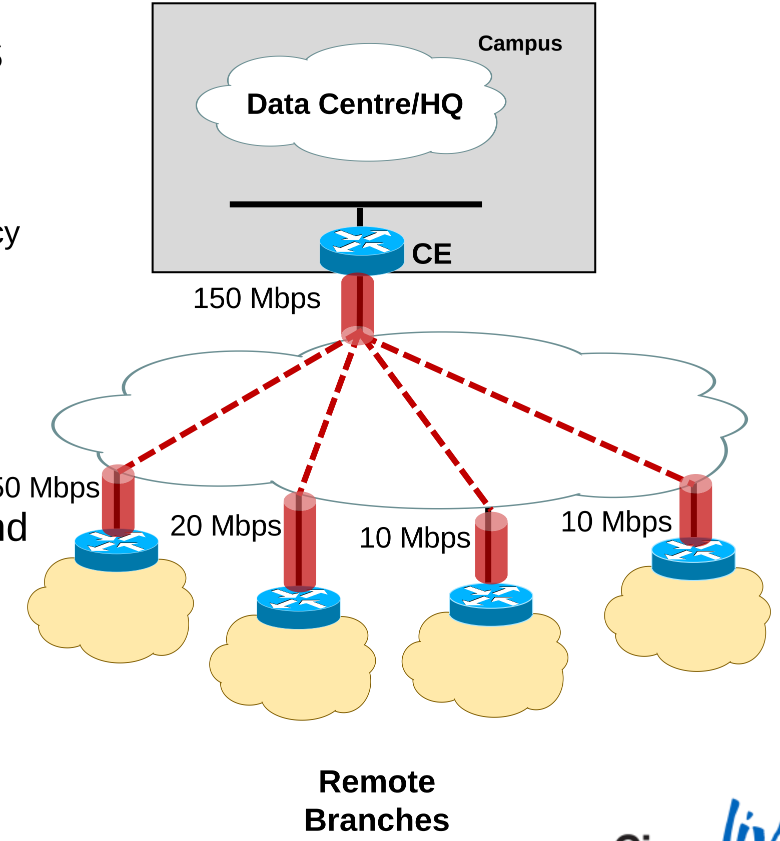
- User NHRP group to dynamically provision HQoS policy on a DMVPN hub per-spoke basis

    Spoke: Configure NHRP group name

    Hub: NHRP group name mapped to QoS template policy

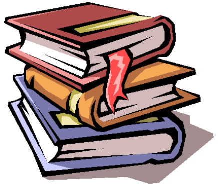
  Multiple spokes with same NHRP group mapped to individual instances of same QoS template policy

- GRE ,IPsec &L2 header are included in calculations for shaping and bandwidth.
- Queuing and shaping is performed at the outbound physical interface
- Can be used with DMVPN with or without IPSec.
- 7200/ISR G1/G2 – 12.4(22)T or later
- ASR1000 – IOS XE RLS 3.6



IOS Configuration Reference for Per-Tunnel QoS for DMVPN:
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_per_tunnel_qos.html

Per-tunnel QoS
Configurations



Hub

```
class-map match-all typeA_voice
  match access-group 100
class-map match-all typeB_voice
  match access-group 100
class-map match-all typeA_Routing
  match ip precedence 6
class-map match-all typeB_Routing
  match ip precedence 6

policy-map typeA
  class typeA_voice
    priority 1000
  class typeA_Routing
    bandwidth percent 20

policy-map typeB
  class typeB_voice
    priority percent 20
  class typeB_Routing
    bandwidth percent 10

policy-map typeA_parent
  class class-default
    shape average 3000000
    service-policy typeA

policy-map typeB_parent
  class class-default
    shape average 2000000
    service-policy typeB
```

Hub (cont)

```
interface Tunnel0
  ip address 10.0.0.1 255.255.255.0
  …
  ip nhrp map group typeA service-policy output typeA_parent
  ip nhrp map group typeB service-policy output typeB_parent
  …
  ip nhrp redirect
  no ip split-horizon eigrp 100
  ip summary-address eigrp 100 192.168.0.0 255.255.192.0 5
  …
```

Spoke1

```
interface Tunnel0
  ip address 10.0.0.11 255.255.255.0
  …
  ip nhrp group typeA
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
  …
```

Spoke2

```
interface Tunnel0
  ip address 10.0.0.12 255.255.255.0
  …
  ip nhrp group typeB
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
  …
```

Spoke3

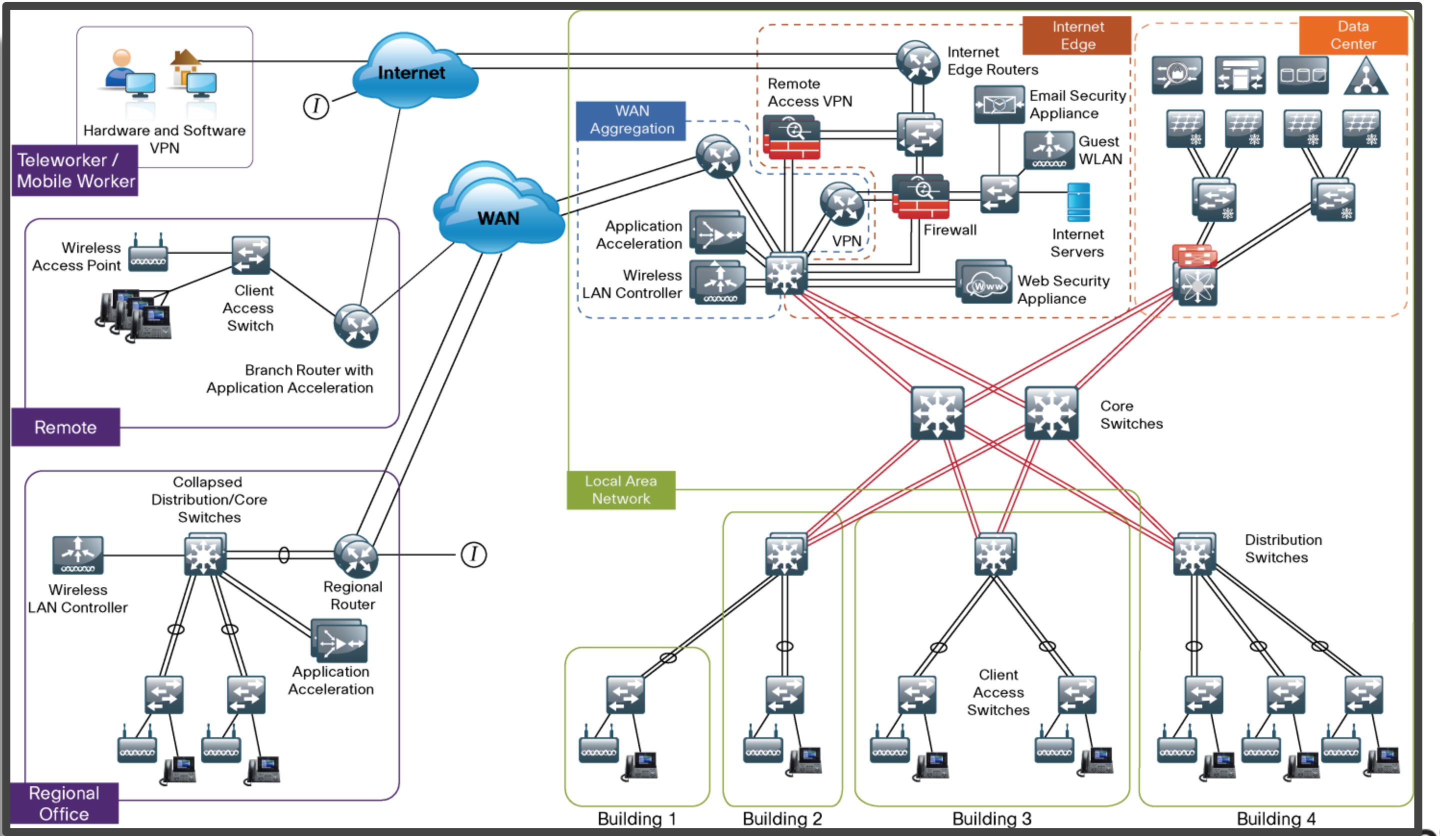
```
interface Tunnel0
  ip address 10.0.0.13 255.255.255.0
  …
  ip nhrp group typeA
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp nhs 10.0.0.1
  …
```

Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

Cisco Validate Design

MPLS WAN Technology Design Guide

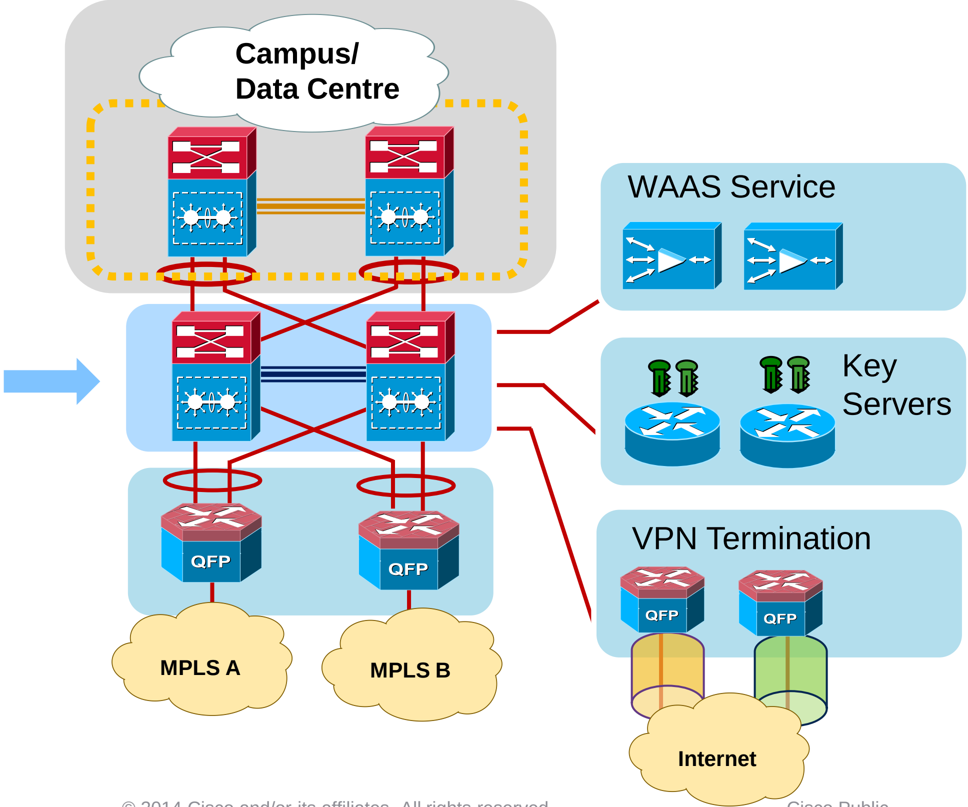


WAN Aggregation Reference Design

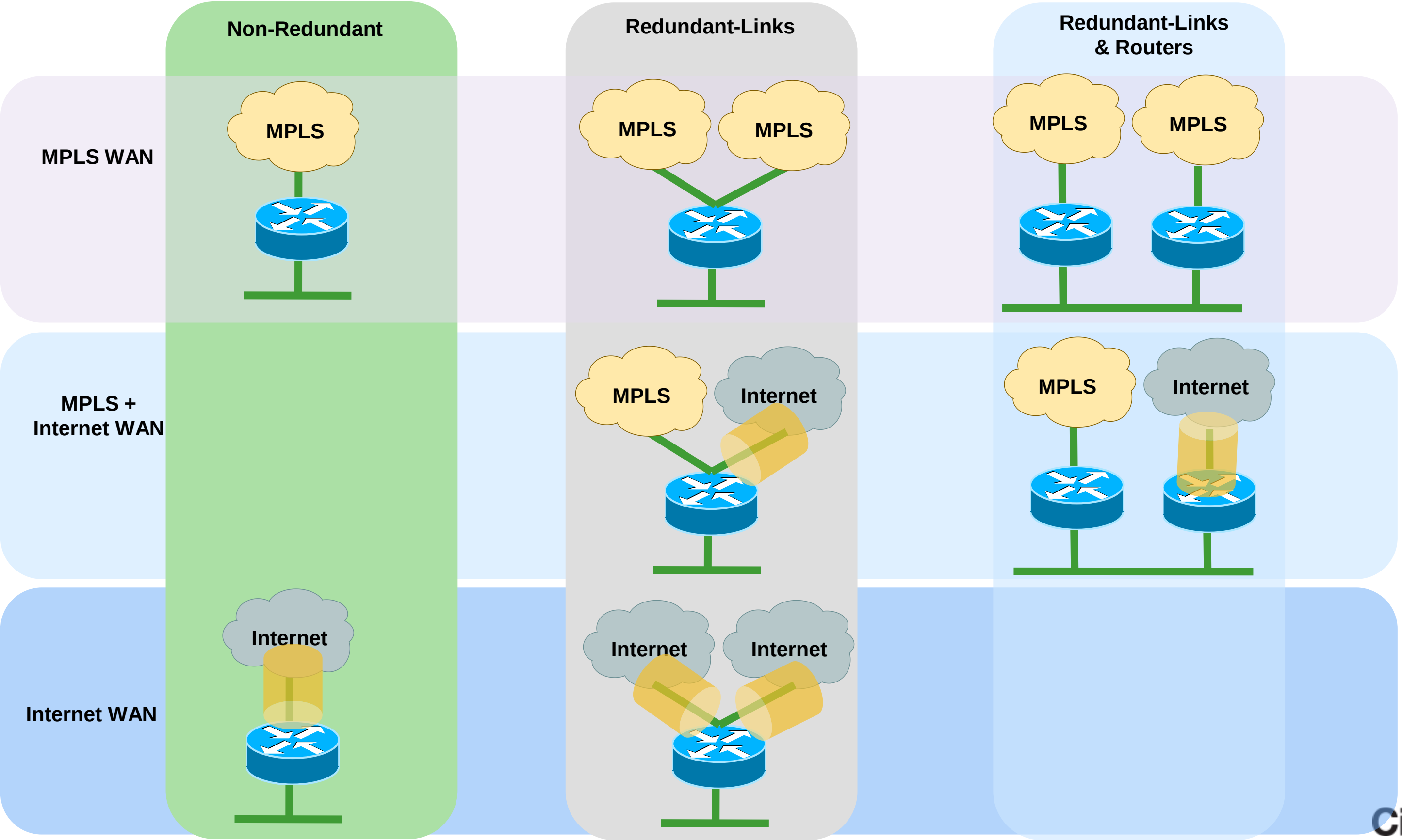
Data Centre/ Campus

WAN Services/ Distribution

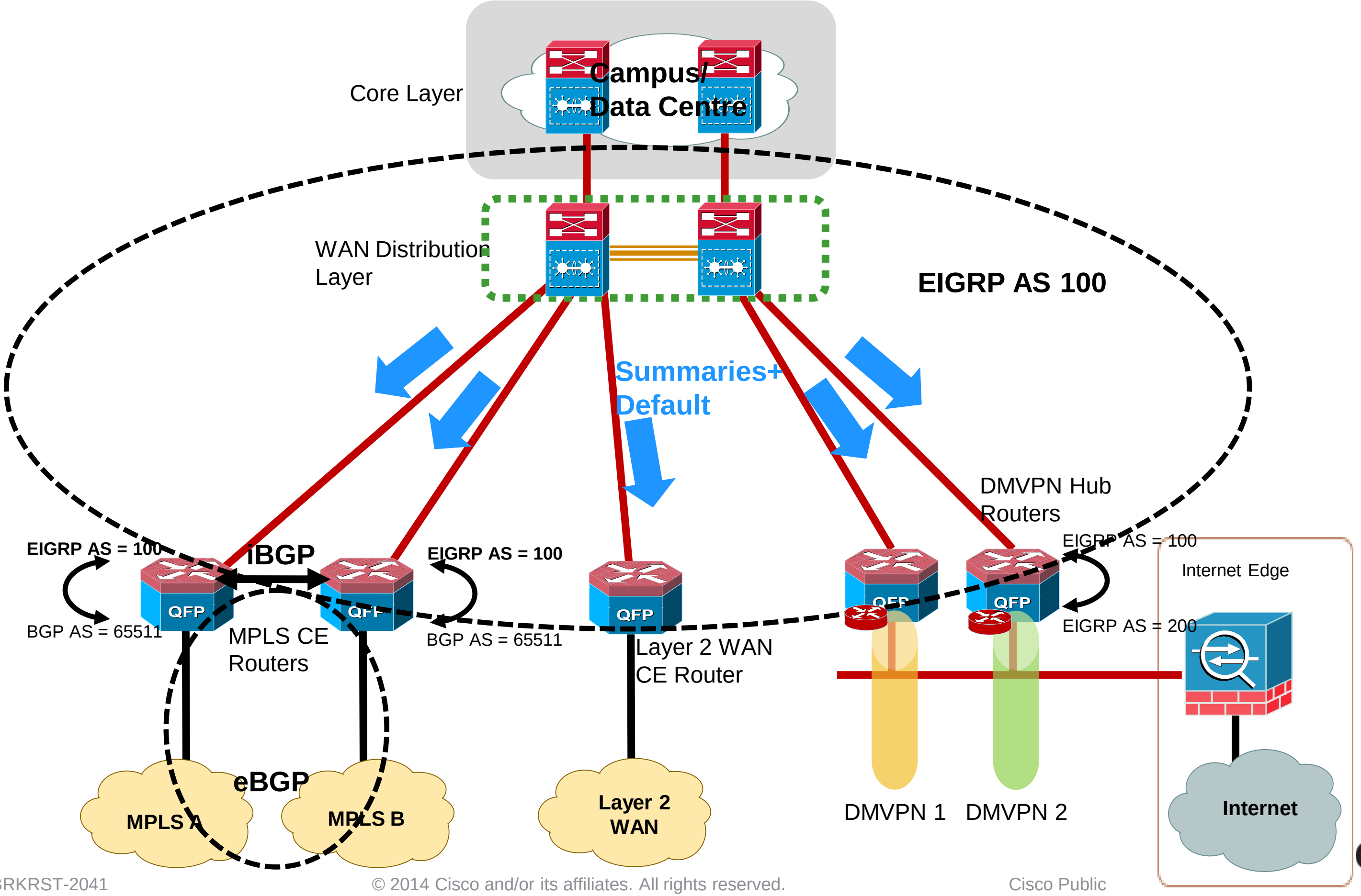
WAN Edge



Remote Branch
Transport & Redundancy Options

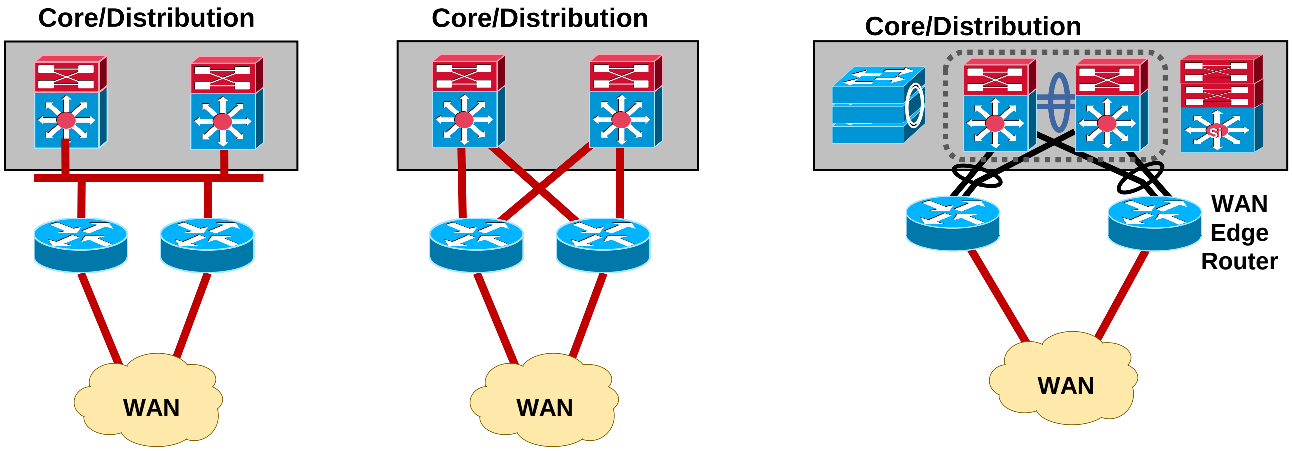


Routing Topology at WAN Aggregation



WAN Edge
Connection Methods Compared

Recommended

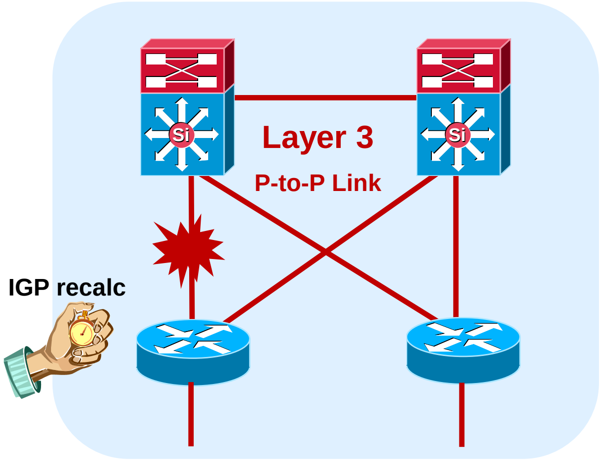


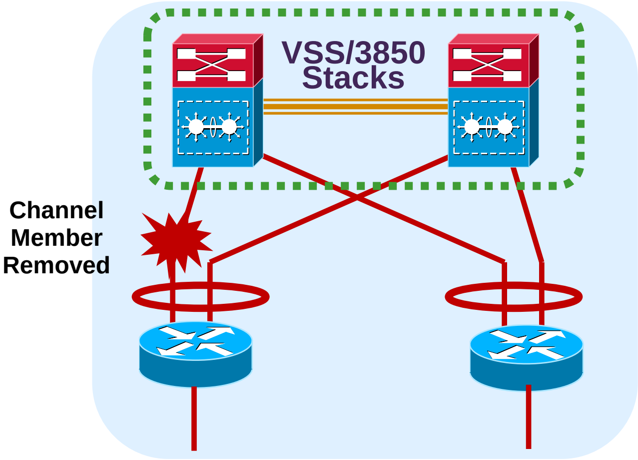
- All:
  - No static routes
  - No FHRPs

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

Optimise Convergence and Redundancy

Multichassis EtherChannel





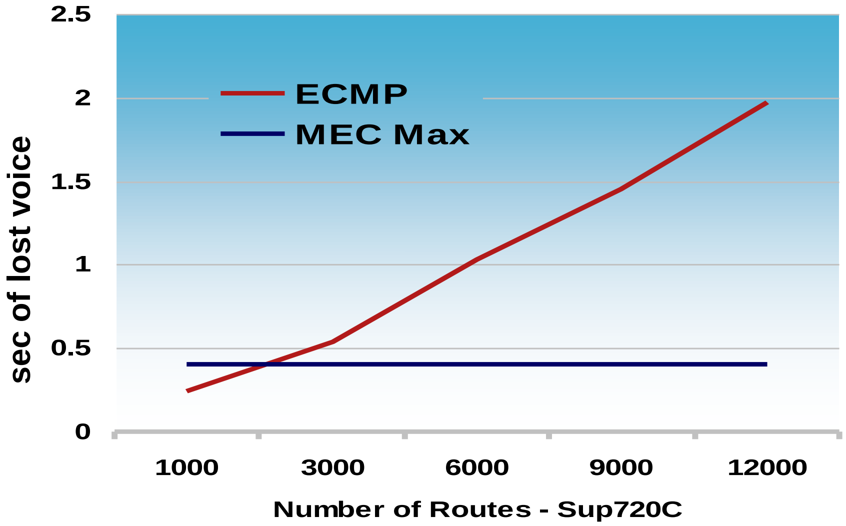
- Link redundancy achieved through redundant L3 paths
- Flow based load-balancing through CEF forwarding across
- Routing protocol reconvergence when uplink failed
- Convergence time may depends on routing protocol used and the size of routing entries

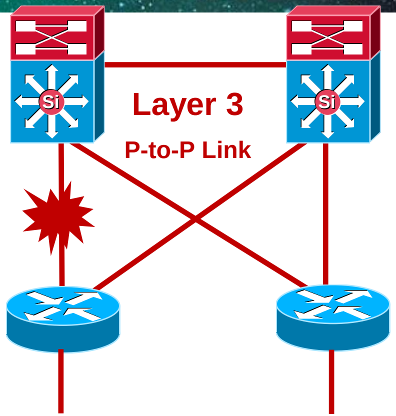
- Provide Link Redundancy and reduce peering complexity
- Tune L3/L4 load-balancing hash to achieve maximum utilisation
- No L3 reconvergence required when member link failed
- No individual flow can go faster than the speed of an individual member of the link

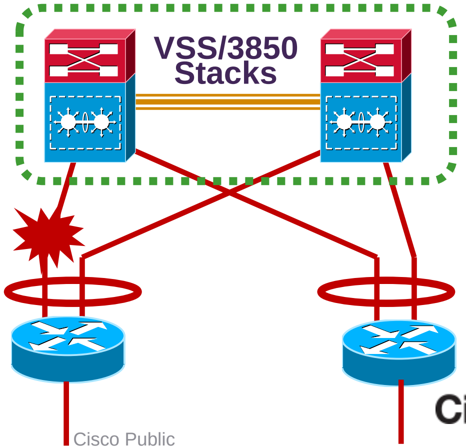
Link Recovery Comparison

ECMP vs. Multichassis EtherChannel

- ECMP convergence is dependent on the number of routes
- MEC convergence is consistent, independent of the number of routes



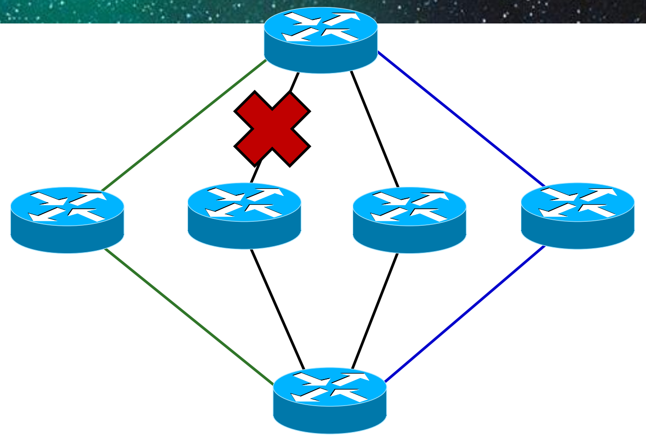


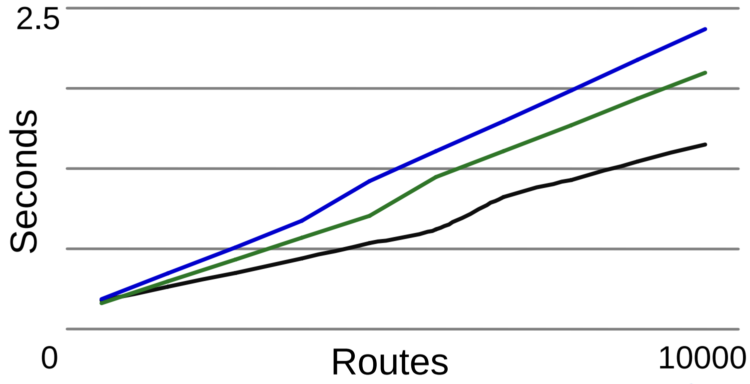


Redundancy vs. Convergence Time

More Is Not Always Better

- In principle, redundancy is easy
- Any system with more parallel paths through the system will fail less often
- The problem is a network isn't really a single system but a group of interacting systems
- Increasing parallelism increases routing complexity, therefore increasing convergence times
  - two parallel paths convergence takes 1.2 seconds
  - three parallel paths convergence takes 2.1 seconds
  - four parallel paths convergence takes 2.4 seconds

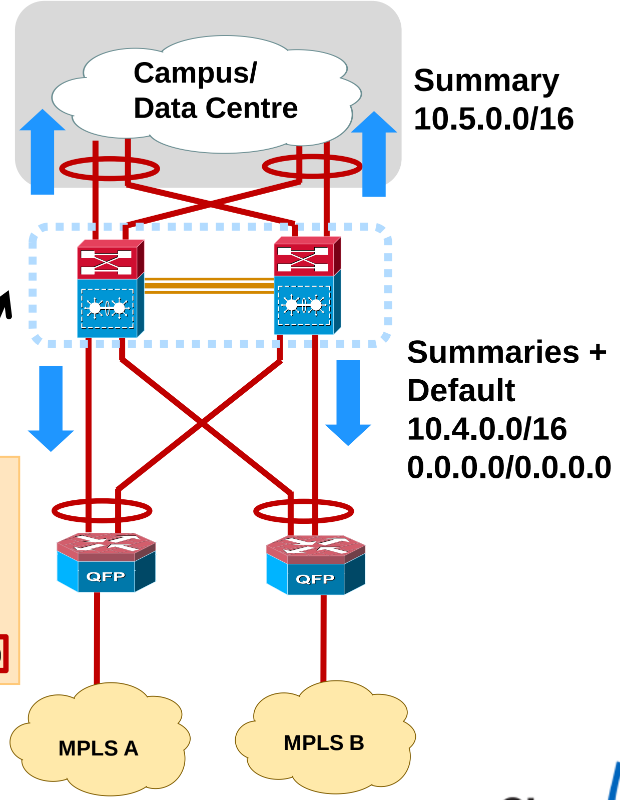




Best Practice
Summarise at Service Distribution

- It is important to force summarisation at the distribution towards WAN Edge and towards campus & data centre
- Summarisation provides topology change isolation.
- Summarisation reduce routing table size.

```
interface Port-channel1
 description Interface to MPLS-A-CE
 no switchport
 ip address 10.4.128.1 255.255.255.252
 ip pim sparse-mode
 ip summary-address eigrp 100 10.5.0.0 255.255.0.0
```

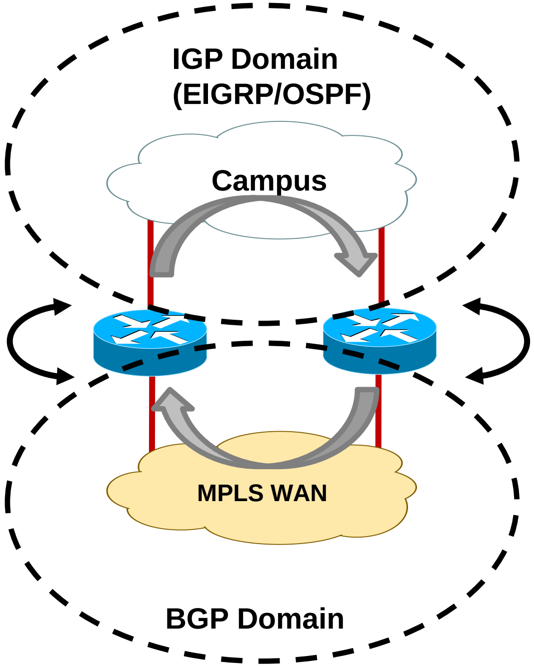


Best Practice

Preventing Routing Loops with Route Tag and Filter

- Mutual route redistribution between protocols can cause routing loops without preventative measures
- Use route-map to set tags and then redistribute based on the tags
- Routes are implicitly tagged when distributed from eBGP to EIGRP/OSPF with carrier AS
- Use route-map to block re-learning of WAN routes via the distribution layer (already known via iBGP)

```
router eigrp 100
 distribute-list route-map BLOCK-TAGGED-ROUTES in
 default-metric [BW] 100 255 1 1500
 redistribute bgp 65500

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

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

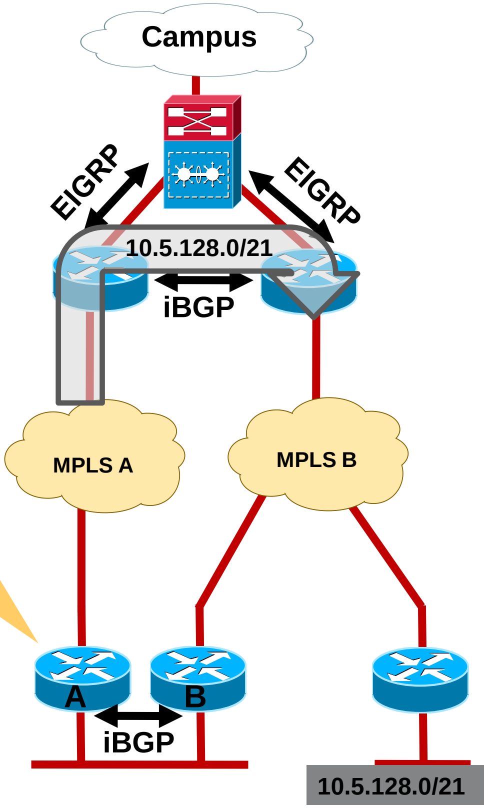


Dual Carriers with BGP as CE-PE Protocol

Use iBGP for Intelligent Path Selection

- Run iBGP between the CE routers to exchange prefixes associated with each carrier
- CE routers will use only BGP path selection information to select both the primary and secondary preferences for any destinations announced by the IGP and BGP
- Use IGP (OSPF/EIGRP) for prefix re-advertisement will result in equal-cost paths at remote-site

```
bn-br200-3945-1# sh ip bgp 10.5.128.0/21
BGP routing table entry for 10.5.128.0/21, version 71
Paths: (2 available, best #2, table default, RIB-failure(17))
  Not advertised to any peer
  65401 65402  (aggregated by 65511 10.5.128.254)
    10.4.142.26 from 10.4.142.26 (192.168.100.3)
      Origin IGP, localpref 100, valid, external, atomic-
aggregate
  65402  (aggregated by 65511 10.5.128.254)
    10.4.143.26 (metric 51456) from 10.5.0.10 (10.5.0.253)
      Origin IGP, metric 0, localpref 100, valid, internal,
atomic-aggregate, best
```

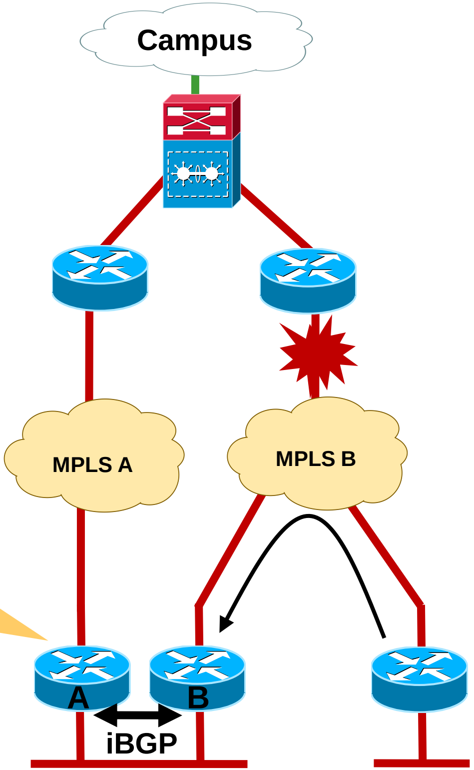


Best Practice - Implement AS-Path Filter

Prevent Branch Site Becoming Transit Network

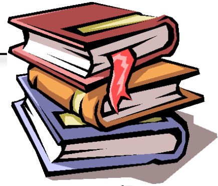
- Dual carrier sites can unintentionally become transit network during network failure event and causing network congestion due to transit traffic
- Design the network so that transit path between two carriers only occurs at sites with enough bandwidth
- Implement AS-Path filter to allow only locally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

```
router bgp 65511
 neighbor 10.4.142.26 route-map NO-TRANSIT-AS out
!
ip as-path access-list 10 permit ^$
!
route-map NO-TRANSIT-AS permit 10
 match as-path 10
```



Golden Rules

Route Preference for EIGRP & OSPF



EIGRP

- – Internal EIGRP – Admin Dist. 90
- – External EIGRP – Admin Dist. 170

- Metric Calculation

  metric = bandwidth + delay

  - – Bandwidth (in kb/s)
  - – Delay (in microseconds)

OSPF

- – Admin Dist. 110

- Route Preference
  1. Intra-Area
  2. Inter-Area
  3. External E1 (Internal + External Cost)
  4. External E2 (External Cost)

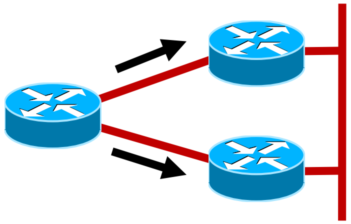
- Cost Calculation

  Cost= Reference BW / Interface BW

  Default Reference BW = 100Mbps

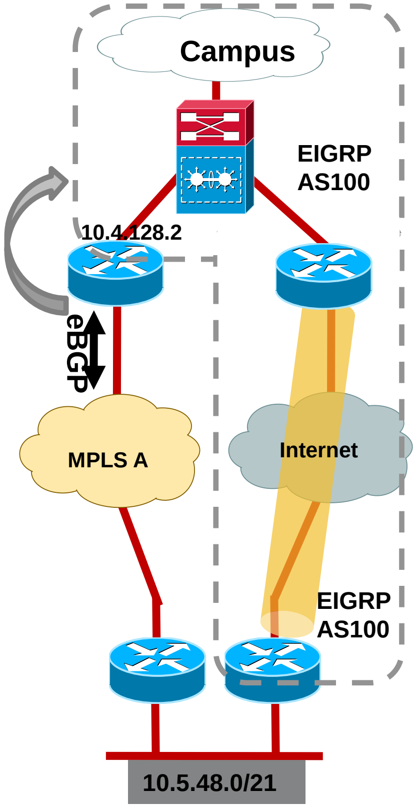
Best Practice
Use Delay Parameter to Influence EIGRP Path Selection

- EIGRP uses the minimum bandwidth along the path and the total delay to compute routing metrics
- Does anything else use these values?
  - EIGRP also uses interface Bandwidth parameter to avoid congestion by pacing routing updates (default is 50% of bandwidth)
  - Interface Bandwidth parameter is also used for QoS policy calculation
  - Performance Routing (PfR) leverages Bandwidth parameter for traffic load sharing
- **Delay parameter should always be used to influence EIGRP routing decision**



MPLS + Internet WAN

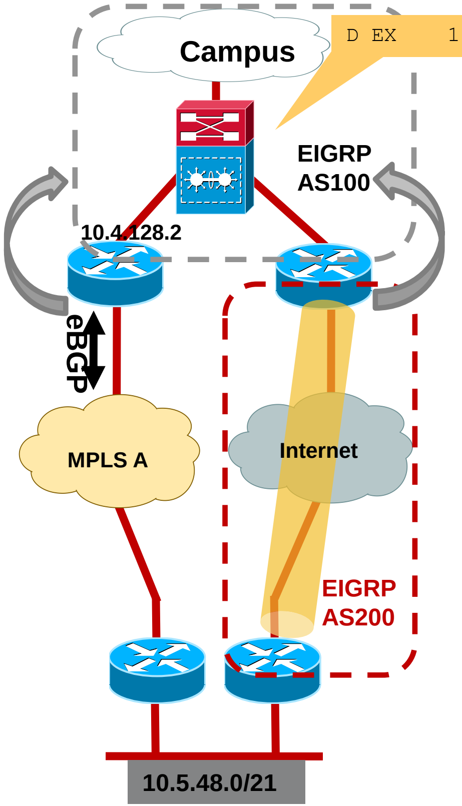
Prefer the MPLS Path over Internet



- eBGP routes are redistributed into EIGRP 100 as external routes with default Admin Distance 170
- Running same EIGRP AS for both campus and DMVPN network would result in Internet path preferred over MPLS path
- Multiple EIGRP AS processes can be used to provide control of the routing
  - EIGRP 100 is used in campus location
    EIGRP 200 over DMVPN tunnels
  - Routes from EIGRP 200 redistributed into EIGRP 100 appear as external route (distance = 170)
- Routes from both WAN sources are equal-cost paths. To prefer MPLS path over DMVPN use eigrp delay to modify path preference

MPLS + Internet WAN

Use Autonomous System for IGP Path Differentiation

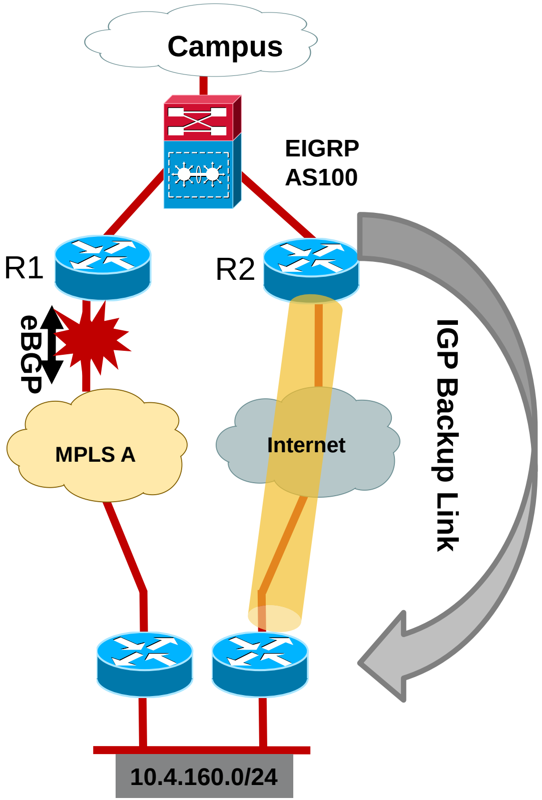


- eBGP routes are redistributed into EIGRP 100 as external routes with default Admin Distance 170
- Running same EIGRP AS for both campus and DMVPN network would result in Internet path preferred over MPLS path
- Multiple EIGRP AS processes can be used to provide control of the routing
  - EIGRP 100 is used in campus location EIGRP 200 over DMVPN tunnels
  - Routes from EIGRP 200 redistributed into EIGRP 100 appear as external route (distance = 170)
- Routes from both WAN sources are equal-cost paths. To prefer MPLS path over DMVPN use eigrp delay to modify path preference

```
MPLS CE router#

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

MPLS VPN BGP Path with IGP Backdoor Path

- eBGP as the PE-CE Routing Protocol
- MPLS VPN as preferred path learned via eBGP
- Secondary path via backdoor IGP link (EIGRP or OSPF) over tunneled connection (DMVPN over Internet)
- Default configuration the failover to backup path works as expected



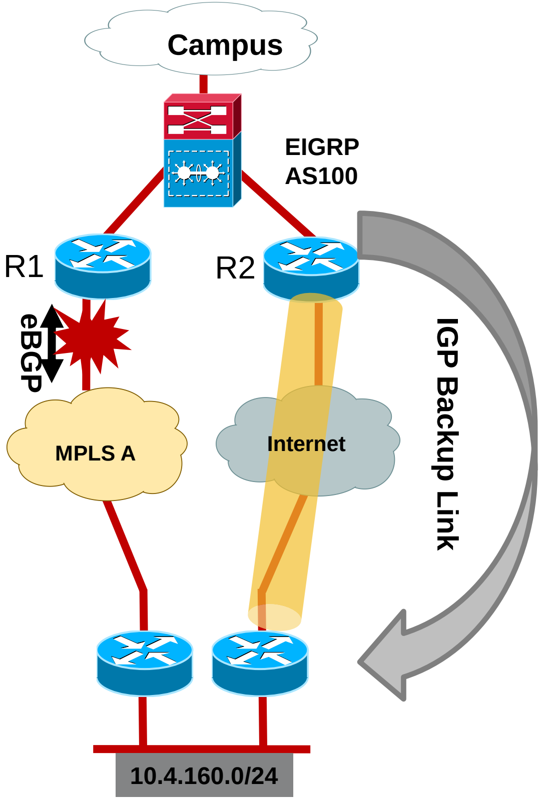
MPLS VPN BGP Path with IGP Backdoor Path

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

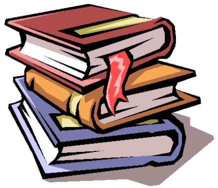
```
D EX 10.4.160.0/24 [170/3584]....
```

```
R1# show ip route
B     10.4.144.0/24 [20/0] via 10.4.142.2, 01:30:06
B     10.4.145.0/24 [20/0] via 10.4.142.2, 01:30:06
```

```
B     10.4.160.0/24 [20/0]....
```



BGP Route Selection Algorithm



BGP Prefers Path with:

1. Highest Weight
2. Highest Local Preference
3. Locally originated (via network or aggregate BGP)
4. Shortest AS_PATH
5. Lowest Origin type
   IGP>EGP>INCOMPLETE (redistributed into BGP)
6. Lowest Multi-Exit Discriminator (MED)
7. Prefer Externals (eBGP over iBGP paths)
8. Lowest IGP metric to BGP next hop (exit point)
9. Lowest Router ID for exit point

BGP Prefers Path with Highest Weight

- Routes redistributed into BGP are considered locally originated and get a default weight of 32768
- The eBGP learned prefix has default weight of 0
- Path with *highest* weight is selected

```
 ASR1004-1#show ip bgp 10.4.160.0 255.255.255.0
BGP routing table entry for 10.4.160.0/24, version 22
Paths: (3 available, best #3, table default)
  Advertised to update-groups:
     4           5
  65401 65401
    10.4.142.2 from 10.4.142.2 (192.168.100.3)
      Origin IGP, localpref 200, valid, external
Local
    10.4.128.1 from 0.0.0.0 (10.4.142.1)
      Origin incomplete, metric 26883072, localpref 100, weight 32768, valid, sourced, best
```

Prefer the eBGP Path over IGP

Set the eBGP weight > 32768

- To resolve this issue set the weights on route learned via eBGP peer higher than 32768

neighbor 10.4.142.2 weight 35000

```
ASR1004-1#show ip bgp 10.4.160.0 255.255.255.0
BGP routing table entry for 10.4.160.0/24, version 22
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  65401 65401
    10.4.142.2 from 10.4.142.2 (192.168.100.3)
      Origin IGP, metric 0, localpref 100, weight 35000, valid, external, best
```

```
ASR1004-1#show ip route
....
B    10.4.160.0/24 [20/0] via 10.4.142.2, 05:00:06
```

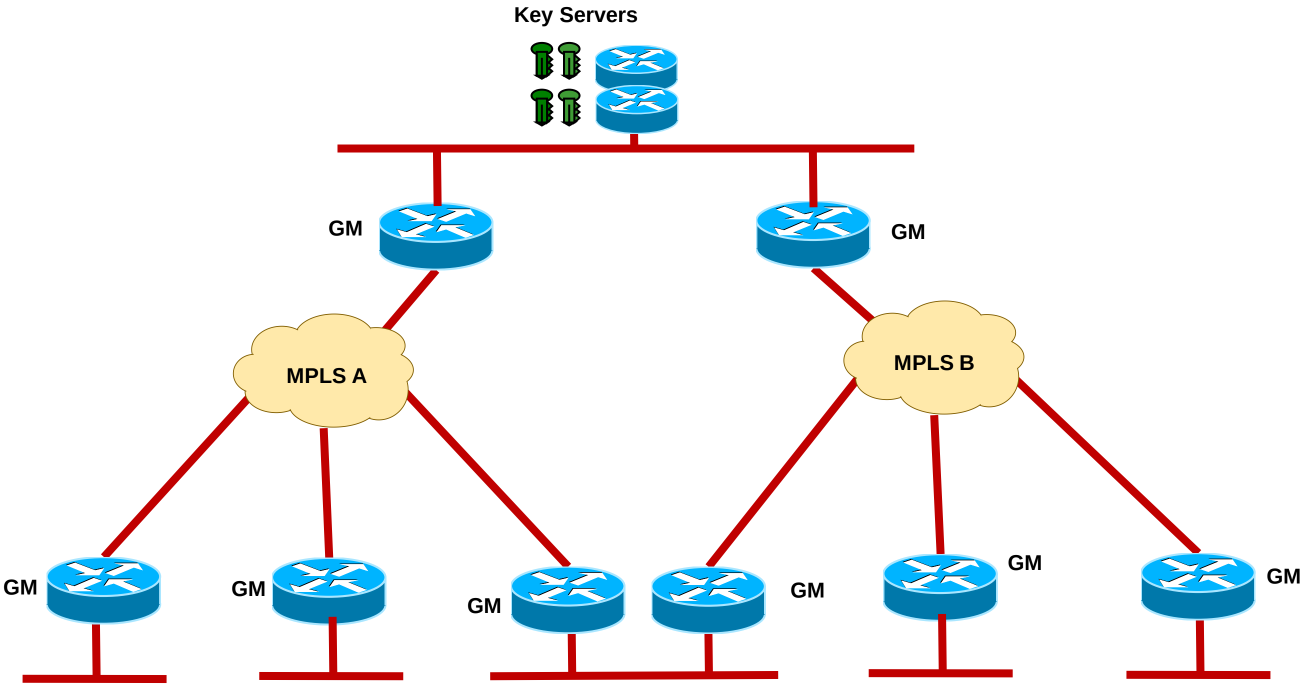

Cisco live!

Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

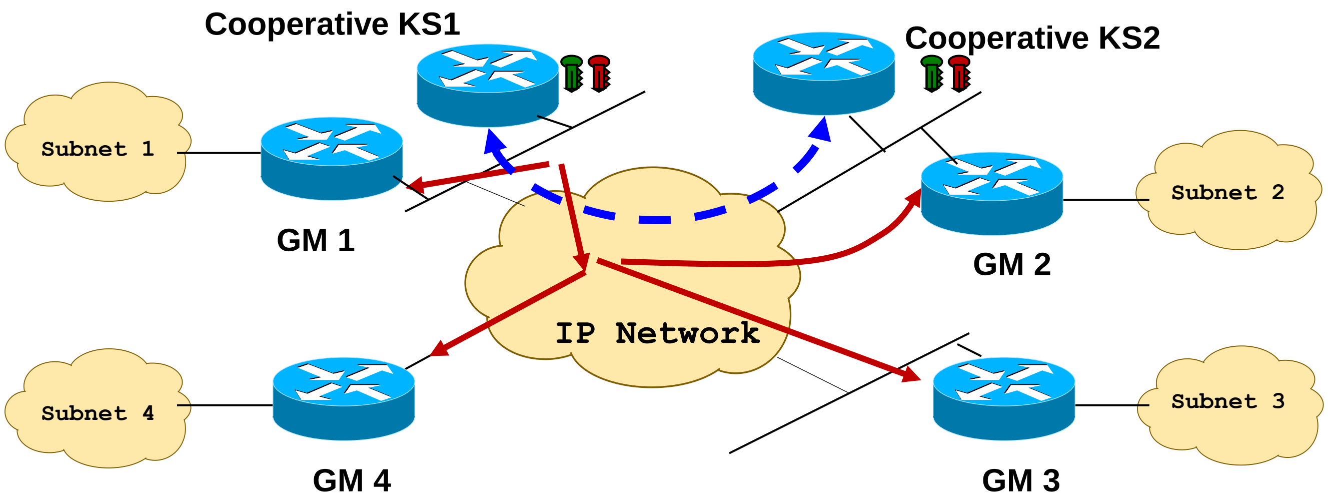
GETVPN Topology

COOP Key Server

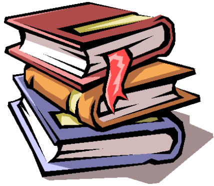


Best Practice - High Availability with Cooperative Key Servers

- Two or more KSs known as COOP KSs manage a common set of keys and security policies for GETVPN group members
- Group members can register to any one of the available KSs
- Cooperative KSs periodically exchange and synchronise group's database, policy and keys
- Primary KS is responsible to generate and distribute group keys



Best Practice - Key Server Recommendations

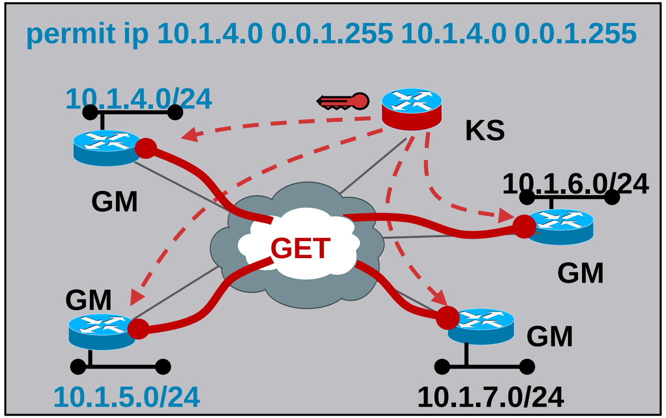


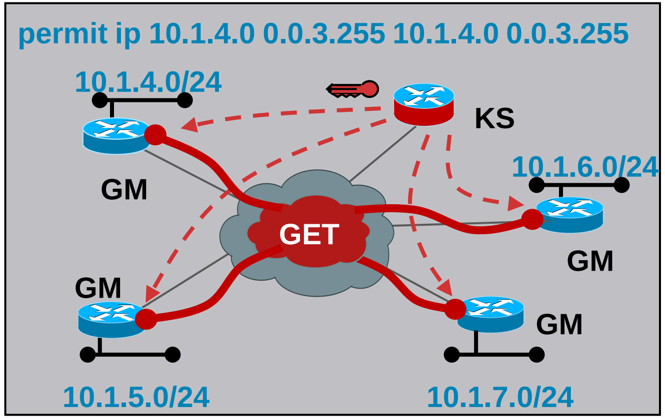
- Maintain reliable KS communication:
  - –Insure multiple routing paths exist between all KS
  - –Use loopback interface for KS registration and Cooperative KS protocol Use IKE keep-alive for KS-KS communication
- Use only globally applicable policies in KS proxy identifiers:
  - –Site specific policies should be applied at the GM
  - –Goal is to create symmetric policies on KS
  - –Exception policy development should be done on GM, not KS
- Use sufficiently long key lifetimes to minimise key transitions:
  - –TEK > 3600 sec, KEK > 86400 sec
- Insure rekey interval extends longer than routing convergence time

Transition from Clear-text to GETVPN

SA Receive-Only Method

- Goal
  - –Incrementally deploy infrastructure without encryption
  - –Immediate transition to encryption controlled by KS
- Method
  - –Deploy KS with Receive-only SA's (don't encrypt, allow decryption)
  - –Deploy GM throughout infrastructure and monitor rekey processes
  - –Transition KS to Normal SA (encrypt, decrypt)
- Assessment
  - –Pro: Simple transition to network-wide encryption
  - –Con: Correct policies imperative
  - –Con: Deferred encryption until all CE are capable of GM functions





Group Member

Secured Group Member Interface

```
interface Serial0/0
ip address 192.168.1.14 255.255.255.252
  crypto map svn                              <- WAN ENCRYPTION
  access-group pack-filter out                <- ALLOW IPsec and Control
```

Packet filter (after encryption)

```
ip access-list extended pack-filter
   permit esp any any                                <- ALLOW IPsec
   permit ip host 192.168.1.14 host 192.168.1.13     <- ALLOW ROUTE ADJACENCY
   permit tcp host 192.168.1.14 eq ssh any           <- ALLOW SECURE SHELL
```

Crypto Map Association to Group Security

```
crypto map svn 10 gdoi<- GROUP CRYPTO MAP ENTRY
  set group secure-wan                        <- GROUP MEMBERSHIP
  match address control_plane                 <- LOCAL POLICY (EXCLUDE)
```

Group Member Policy Exceptions

```
ip access-list extended control_plane           <- CONTROL PLANE PROTOCOLS
   deny ip host 192.168.1.14 host 192.168.1.13 <- PE-CE LINK (BGP, ICMP)
   deny tcp host 192.168.1.14 eq ssh any        <- MANAGEMENT SECURE SHELL
```

Group Member Association

```
crypto gdoi group secure-wan                  <- GROUP ENCRYPTION
   identity number 3333                       <- MEMBER'S GROUP IDENTITY
   server address ipv4 <ks1_address>          <- KS ADDRESS TO REGISTER
   server address ipv4 <ks2_address>          <- ALTERNATE KS REGISTRATION
```

Key Server

```
crypto gdoi group secure-wan
     identity number 3333                          <- GROUP ID
     server local                                  <- KEY SERVER
     rekey retransmit 40 number 3                  <- REKEY RETRANSMITS
     rekey authentication mypubkey rsa my_rsa      <- KS MSG AUTHENTICATION
     rekey transport unicast                       <- Unicast Rekey
     saipsec 10                                    <- SECURITY ASSOCIATION
     profile GETVPN-GDOI-PROFILE                   <- CRYPTO ATTRIBUTES SELECTION
     match address ipv4ipsec-policy                <- ENCRYPTION POLICY
     no replay                                     <- NO ANTI-REPLAY
     address ipv4 <ks_address>                     <- KS ADDRESS
```

Crypto Attributes

```
crypto ipsec profile GETVPN-GDOI-PROFILE
  set security-association lifetime seconds 7200
  set transform-set AES256/SHA                       <- AES256 for Encryption and SHA for Hash
```

Encryption IPsec Proxy ID's (mandatory)

```
ip access-list extended ipv4ipsec-policy                            <- ENCRYPTION POLICY
   deny udp any eq 848 any eq 848                                   <- ALLOW GDOI
   permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255          <- UNICAST
   permit ip 10.0.0.0 0.255.255.255 232.0.0.0 0.255.255.255         <- MULTICAST
```

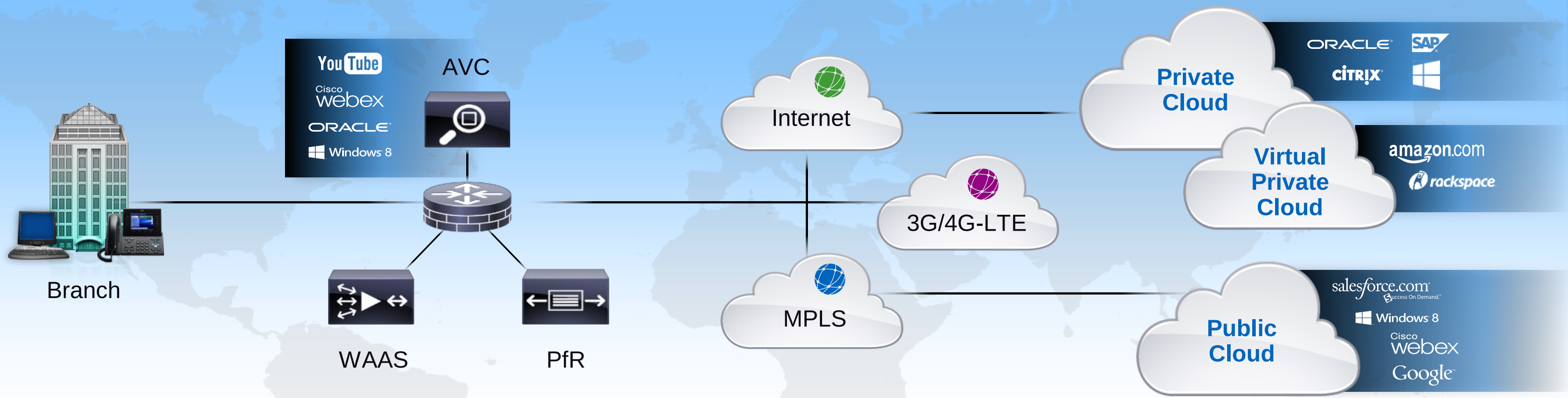
Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

Internet Becoming an Extension of Enterprise WAN

- Commodity Transports Viable Now
- Dramatic Bandwidth, Price Performance Benefits
- Higher Network Availability
- Improved Performance Over Internet

Intelligent WAN Solution Components



Transport Independent

- Consistent operational model
- Simple provider migrations
- Scalable and modular design
- IPsec routing overlay design

Intelligent Path Control

- Dynamic Application best path based on policy
- Load balancing for full utilisation of bandwidth
- Improved network availability

Application Optimisation

- Application visibility with performance monitoring
- Application acceleration and bandwidth optimisation

Secure Connectivity

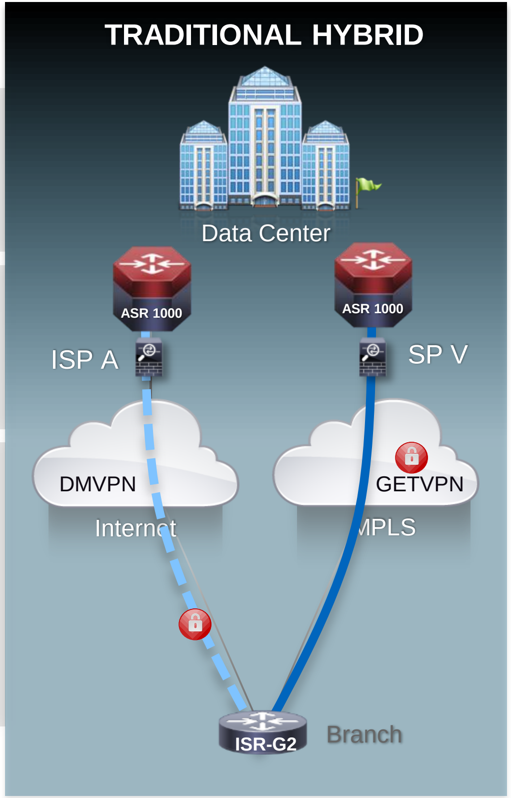
- Certified strong encryption
- Comprehensive threat defence
- Cloud Web Security for secure direct Internet access

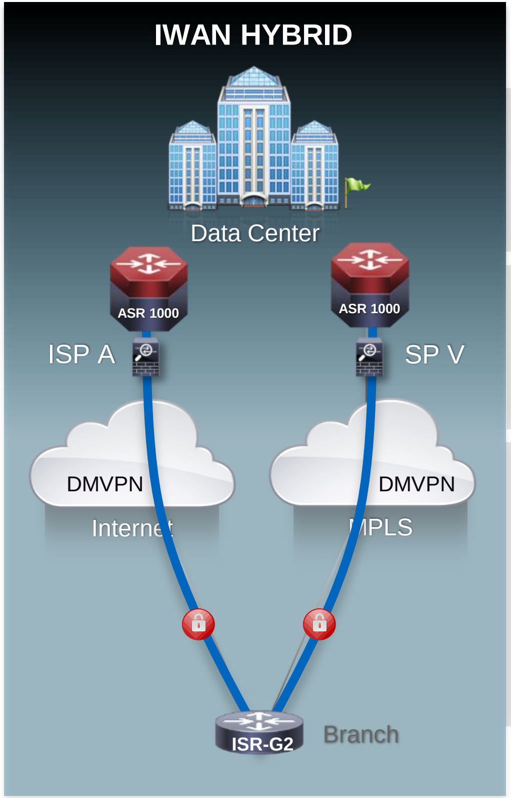
Hybrid WAN Designs
Traditional and IWAN

Active/Standby
WAN Paths
Primary With Backup

Two IPsec Technologies
GETVPN/MPLS
DMVPN/Internet

Two WAN Routing Domains
MPLS: eBGP or Static
Internet: iBGP, EIGRP or OSPF
Route Redistribution
Route Filtering Loop Prevention





Active/Active
WAN Paths

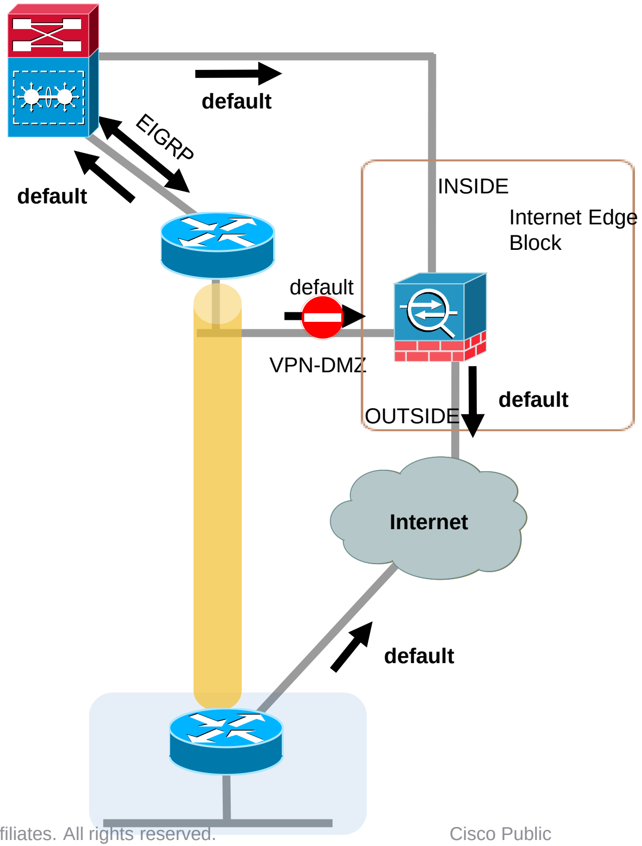
One IPsec Overlay
DMVPN

One WAN Routing Domain
iBGP, EIGRP, or OSPF

DMVPN Deployment over Internet

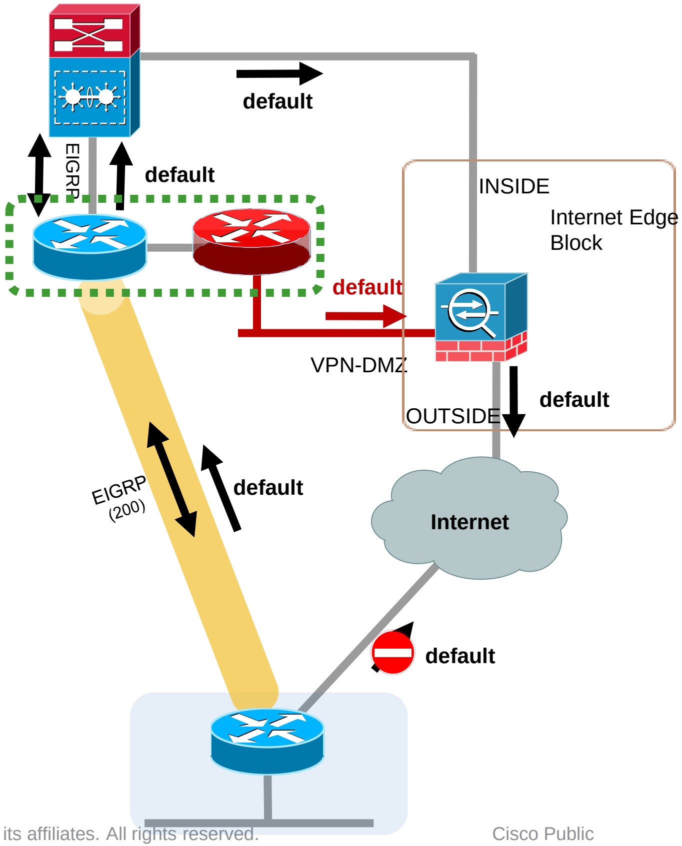
Multiple Default Routes for VPN Headend

- VPN Headend has a default route to ASA firewall's VPN-DMZ interface to reach Internet
- Remote site policy requires centralised Internet access
- Enable EIGRP between VPN headend & Campus core to propagate default to remote
- Static default (admin dist=0) remains active,
- VPN-DMZ is wrong firewall interface for user traffic
- Adjust admin distance so EIGRP route installed (to core)
- VPN tunnel drops



DMVPN Deployment over Internet

- Enable FVRF with DMVPN to separate out the two default routes
- The RED-VRF contains the default route to VPN-DMZ Interface needed for Tunnel Establishment
- A 2^{nd} default route exist on the Global Routing Table used by the user data traffic to reach Internet
- To prevent split tunnelling the default route is advertised to spokes via Tunnel
- Spoke's tunnel drops due to 2^{nd} default route conflict with the one learned from ISP

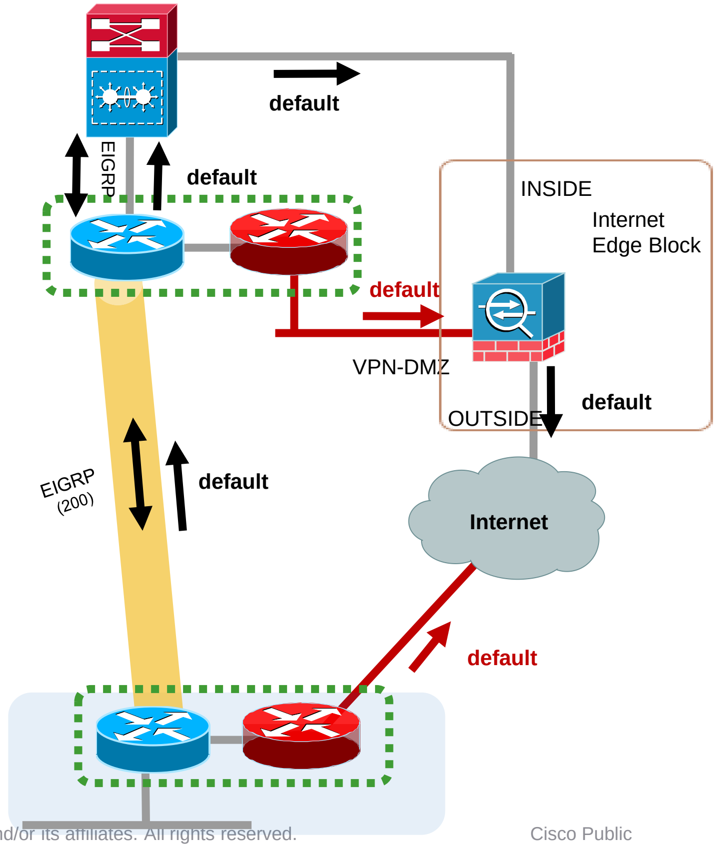


Best Practice – VRF-aware DMVPN

Keeping the Default Routes in Separate VRFs

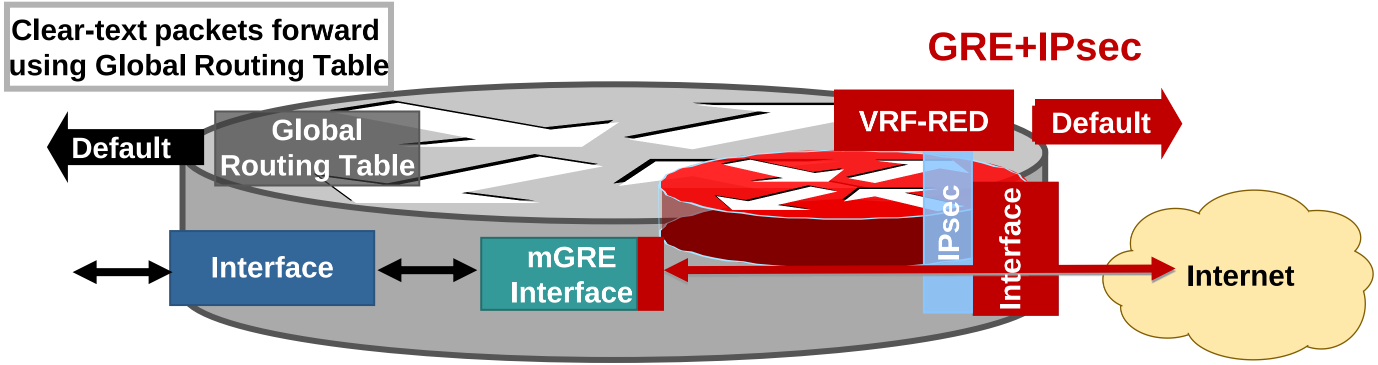
No Split Tunnelling at Branch location

- Enable FVRF DMVPN on the Spokes
- Allow the ISP learned Default Route in the RED-VRF and used for tunnel establishment
- Global VRF contains Default Route learned via tunnel. User data traffic follow Tunnel to INSIDE interface on firewall
- Allow for consistency for implementing corporate security policy for all users



DMVPN and FVRF

Configuration Example




```
ip vrf RED
 rd 65512:1
!
crypto keyring DMVPN-KEYRING vrf RED
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp keepalive 30 5
!
crypto isakmp profile FVRF-ISAKMP-RED
   keyring DMVPN-KEYRING
   match identity address 0.0.0.0 RED
!
```

```
interface GigabitEthernet0/1
 ip vrf forwarding RED
 ip address dhcp
!
interface Tunnel10
 ip address 10.4.132.201 255.255.254.0
 ….
 tunnel mode gre multipoint
 tunnel vrf RED
 tunnel protection ipsec profile DMVPN-PROFILE
!
router eigrp 200
 network 10.4.132.0 0.0.0.255
 network 10.4.163.0 0.0.0.127
 eigrp router-id 10.4.132.201
```

IWAN Intelligent Path Control

Solution Overview

1. Policies:

    Voice/Video: Delay < 200ms, Jitter < 30ms, Preferred Path = FTTH

    Data: Load Balance, max link utilisation 90%

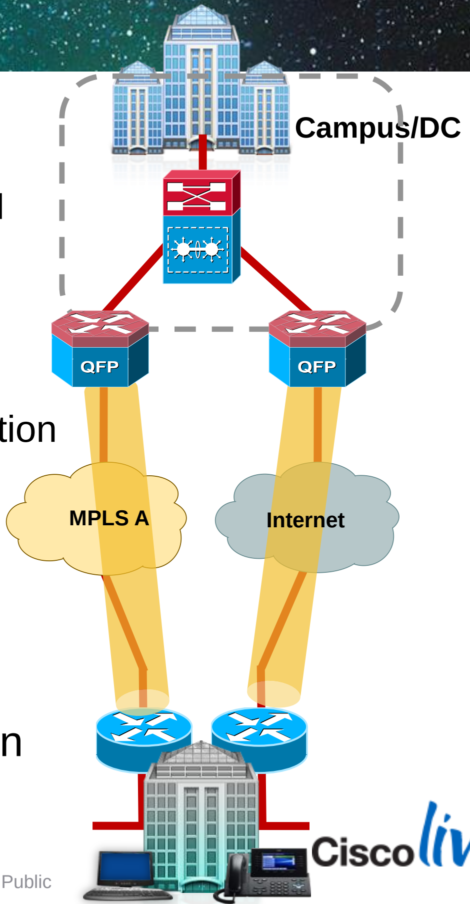
2. DMVPN for secure IPsec transport independent design

    Per-tunnel QOS at hub to minimise branch bandwidth oversubscription

    Site to site dynamic tunnels to reduce latency for multimedia applications

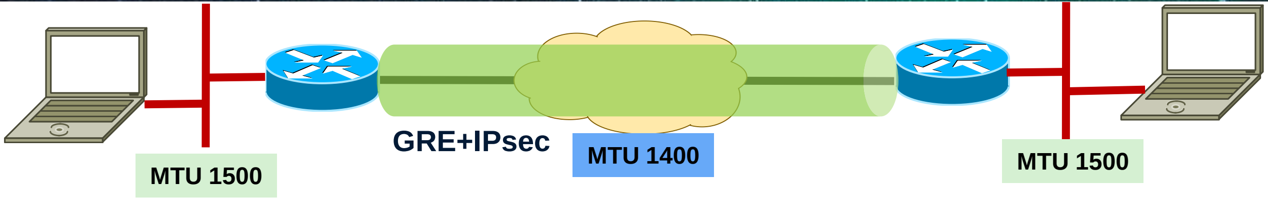
3. Performance Routing (PfR) to protect multimedia apps and maximise bandwidth

4. Advanced QoS to prioritise critical applications during congestion



Best Practices

Avoid Fragmentation with IPSec VPN



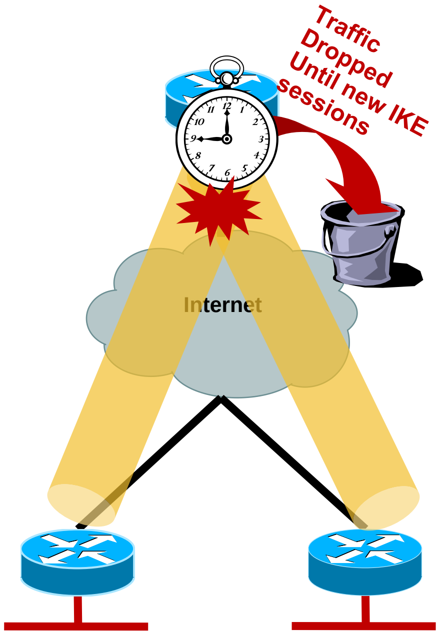
Tunnel Setting (AES256+SHA)	Minimum MTU	Recommended MTU
GRE/IPSec (Tunnel Mode)	1414 bytes	1400 bytes
GRE/IPSec (Transport Mode)	1434 bytes	1400 bytes

- IP fragmentation will cause CPU and memory overhead and resulting in lowering throughput performance
- When one fragment of a datagram is dropped, the entire original IP datagram will have to be resent
- Use '`mode transport`' on transform-set
  - NHRP needs for NAT support and saves 20 bytes
- Avoid MTU issues with the following best practices
  - `ip mtu 1400`
  - `ip tcp adjust-mss 1360`

Best Practices - Enable Dead Peer Detection (DPD)

Improve DMVPN Network Convergence

- Dead Peer Detection (DPD) is a mechanism for detecting unreachable IKE peers
- Each peer's DPD state is independent of the others
- Without DPD spoke routers will continue to encrypt traffic using old SPI which would be dropped at the hub. May take up to 60 minutes for spokes to reconverge
- Use ISAKMP keepalives on spokes
  - `crypto isakmp keepalives <initial> <retry>`
  - – ISAKMP invalid-SPI-recovery is not useful with DMVPN
  - – ISAKMP keepalive timeout should be greater than routing protocol hellos
- Not recommended for Hub routers – may cause an increase of CPU overhead with large number of peers



Informational RFC 3706

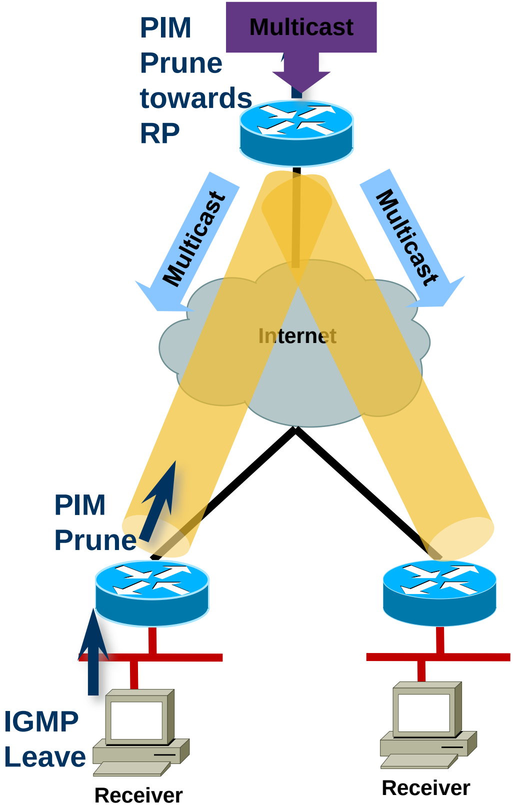
Best Practices — Enable PIM NBMA-Mode

Multicast over DMVPN

- By default router uses OIL to correlate multicast group join to interface
- This causes problem when hub is connected to multiple spokes over NBMA network
- Any spoke that leaves a multicast group would case all the spokes to be pruned off the multicast group
- Enable PIM NBMA mode under tunnel interface on hubs and spokes

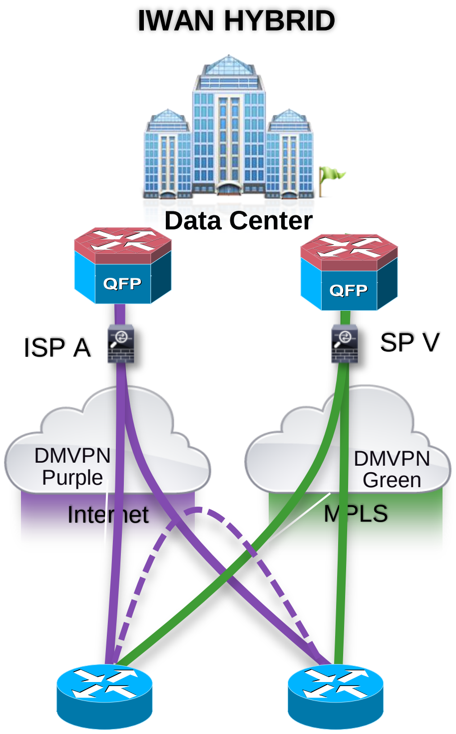
```
ip pim nbma-mode
```

  - Allows the router to track multicast joins based on IP address instead of interface
  - Applies only to PIM sparse-mode
- Router treats NBMA network as a collection of point-to-point circuits, allowing remote sites to be pruned off traffic flows



IWAN Transport Best Practices

- **Private peering with Internet providers**
  - Use same Internet provider for hub and spoke sites
  - Avoids Internet Exchange bottlenecks between providers
  - Reduces round trip latency
- **DMVPN**
  - DMVPN Phase 2 for dynamic tunnels with PfR
  - Separate DMVPN network per provider for path diversity
  - Per tunnel QOS
- **Transport settings**
  - Use the same MTU size on all WAN paths
  - Bandwidth settings should match offered rate
  - Use a front-side VRF to separate Internet and internal default routes
- **Internet security**
  - Firewalls or Access Lists to only permit DMVPN tunnel traffic
  - Hub Tunnel IP address should not be registered in DNS to hide it
- **Routing Overlay**
  - iBGP or EIGRP for high scale (1000+ sites)
  - Single routing process, simplified operations



Agenda

- WAN Technologies & Solutions
  - WAN Transport Technologies
  - WAN Overlay Technologies
  - WAN Optimisation
  - Wide Area Network Quality of Service
- WAN Architecture Design Considerations
  - WAN Design and Best Practices
  - Secure WAN Communication with GETVPN
  - Intelligent WAN Deployment
- Summary

Key Takeaways

- Understand how WAN characteristics can affect your applications
  - Bandwidth, latency, loss
- Dual carrier designs can provide resiliency but have unique design considerations
- A QoS-enabled, highly-available network infrastructure is the foundation layer of the WAN architecture
- Encryption is a foundation component of all WAN designs and can be deployed transparently
- Understand how to build wide area network leveraging Internet transport with Intelligent WAN




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™