Deploying Large Scale VPN with MPLS

Session RST-230

Deploying VPN with MPLS

- Private, connectionless IP VPNs
- Outstanding scalability
- Customer IP addressing freedom
- Multiple QoS classes
- Secure support for intranets and extranets
- Simplified VPN provisioning
- Support over any access or backbone technology

Connection-Oriented VPN Topology

Connectionless VPN Topology
Delivering Value Added IP Services

Multiservice ATM Transport

VPN-Aware Networks

Services and Applications

Multimedia VoIP Hosting Net Commerce Training

New SP Infrastructure

Intranet A Extranet Internet

Frame Relay MPLS-Enabled Network ATM

Agenda

- Deploying MPLS VPN
- Scaling MPLS VPN Network
- Internet Access
- Central and Remote Access
- Network Management and Provisioning
Deploying MPLS VPNs
How It Works, How to Configure It

Agenda

• MPLS-VPN Terminology
• Network Topology
• Enabling the Core
• Step-By-Step Configuration Guideline
  Sample Configuration (VRF, Interfaces)
  PE-CE Routing Protocol Configuration
  (Static,RIPv2, BGP,OSPF)
  MP-BGP Redistribution
What Is a Virtual Private Network?

- VPN is a set of sites which are allowed to communicate with each other
- VPN is defined by a set of administrative policies
  - Policies determine both connectivity and QoS among sites
  - Policies established by VPN customers
  - Policies could be implemented completely by VPN Service Providers using BGP/MPLS VPN mechanisms

VPN Requirements

- Flexible inter-site connectivity
  - Ranging from complete to partial mesh
- Sites may be either within the same or in different organizations
  - VPN can be either Intranet or Extranet
- Site may be in more than one VPN
  - VPNs may overlap
- Not all sites have to be connected to the same service provider
  - VPN can span multiple providers
MPLS VPN Terminology

- **Provider Network (P-Network)**
  The backbone under control of a Service Provider

- **Customer Network (C-Network)**
  Network under customer control

- **CE router**
  Customer Edge router; Part of the C-network and interfaces to a PE router

- **Site**
  Set of (sub)networks part of the C-network and co-located
  A site is connected to the VPN backbone through one or more PE/CE links

- **PE router**
  Provider Edge router; Part of the P-Network and interfaces to CE routers

- **P router**
  Provider (core) router, without knowledge of VPN
MPLS VPN Terminology

- **Route-Target**
  64 bits identifying routers that should receive the route

- **Route Distinguisher**
  Attributes of each route used to uniquely identify prefixes among VPNs (64 bits)
  VRF-based (not VPN-based)

- **VPN-IPv4 addresses**
  Address including the 64 bits Route Distinguisher and the 32 bits IP address

MPLS VPN Terminology

- **MP-BGP**
  Multi-Protocol extensions to BGP

- **VRF**
  VPN Routing and Forwarding Instance
  Routing table and FIB table
  Populated by routing protocol contexts

- **VPN-Aware network**
  A provider backbone where MPLS-VPN is deployed
Building VPNs with MPLS

- Constrained distribution of routing information
  Routes are only communicated to routers that are members of a VPN

- VPN-IP addresses
  Supports overlapping address spaces

- Multiprotocol Label Switching (MPLS)
  Labels used to define VPNs
  Labels used to represent VPN-IP addresses

- Peer model
  Simplifies routing for end customers
MPLS VPN Routes Distribution

Routing Information Distribution

- **Step 1:** From site (CE) to service provider (PE)
  
  E.g., via RIP, or static routing, or BGP

- **Step 2:** Export to provider’s BGP at ingress PE

- **Step 3:** Within/across service provider(s) (among PEs):
  
  Via BGP

- **Step 4:** Import from provider’s BGP at egress PE

- **Step 5:** From service provider (PE) to site (CE)
  
  E.g., via RIP, or static routing, or BGP
Constrained Distribution of Routing Information

- Occurs during steps 2, 3, 4
- Performed by service provider using route filtering based on BGP extended community attribute
  
  BGP community is attached by ingress PE at Step 2
  Per site (per CE), per address prefix granularity
  
  Route filtering based on BGP community is performed by egress PE at step 4
  Per site (per CE), per address prefix granularity

Packet Forwarding

- Forwarding based on extended (VPN-IP) addresses
- MPLS binds VPN-IP routes to label switched paths
- Logically separate forwarding information base (FIB) for each VPN
MPLS VPN Network

Working of MPLS VPN Network
Multiple Forwarding Tables

• PE maintains multiple Forwarding Tables
  One per set of directly attached sites with common VPN membership
  e.g., one for all the directly attached sites that are in just one particular VPN

• Enables (in conjunction with route filtering) per VPN segregation of routing information on PE

Multiple Forwarding Tables

• Each Forwarding Table is populated from:
  Routes received from directly connected CE(s) of the site(s) associated with the Forwarding Table
  Routes receives from other PEs (via BGP) restricted to only the routes of the VPN(s) the site(s) is in via route filtering based on BGP Extended Community Attribute
Multiple Forwarding Tables

- Each customer port on PE is associated with a particular Forwarding Table
  - Via configuration (at provisioning time)
  - Provides PE with per site forwarding information for packets received from CEs
  - Ports on PE could be “logical”
    - E.g., VLAN, FR, ATM, L2F, etc...

VPN-IP Addresses

- New address family: VPN-IP addresses
  - VPN-IP address = Route Distinguisher (RD) + IP address
  - Multiple RT associated with each route
  - RDs are assigned by a service provider
  - RDs are globally unique (by virtue of assignment)
  - Convert non-unique IP addresses into unique VPN-IP addresses
- Reachability information for VPN-IP addresses is carried via multiprotocol extensions to BGP-4
Converting Between IP and VPN-IP Addresses

- Performed by PEs:
  - Ingress PE—exporting route into provider’s BGP:
    - PE is configured with RD(s) for each directly attached site
    - Convert from IP to VPN-IP (by prepending RD) before exporting into BGP
  - Egress PE—importing route from provider’s BGP:
    - Convert from VPN-IP to IP (by stripping RD) before inserting into site’s forwarding table

Happens ONLY in the Control Plane, Not in the Data Plane

MPLS VPN Example: 1—Simple Intranet

Multiple Sites with Full Mesh Connectivity

- One BGP community
- At PE with directly attached site:
  - Exports all site’s routes into provider’s BGP with same route target
  - Imports into the forwarding table associated with the VPN (sites) only routes with same route target
MPLS VPN Example: 2—Hub/Spoke VPN

All Spoke Sites Communicate Through Hub

• PE at the hub site:
  Exports hub site’s routes with community
  Import spokes into the forwarding table associated with the VPN (site) routes

• PE at a spoke sites:
  Export spoke site’s routes with community
  Import hub into the forwarding table associated with the VPN (site) routes

Agenda

• MPLS-VPN Terminology
• Network Topology
• Enabling the Core
• Step-By-Step Configuration Guideline
  Sample Configuration (VRF, Interfaces)
  PE-CE Routing Protocol Configuration (Static, RIPv2, BGP, OSPF)
  MP-BGP Redistribution
Step-By-Step Configuration Guideline

- LDP configuration in MPLS backbone
- MP-BGP between the PE routers
- VPN knowledge is on PE routers
- Adding VPN sites to PE routers
  - VRF and route distinguisher
  - VRF import/export policies (based on route-target)
  - Routing used with CEs
    - (Connected, static, RIPv2, OSPF, BGP)

Step-By-Step Configuration Guideline

- Configure LDP in MPLS backbone
  - On all interfaces in MPLS backbone configure mpls ip
- Verify the configuration
  - Show mpls forwarding
  - Show mpls ldp neighbour
  - Labels for non-BGP routes are created
  - Note: Configuration will be slightly different in future IOS
PE—PE Session to Exchange VPNv4 Routes with MP-BGP

router bgp 100
no bgp default ipv4-unicast
neighbor 7.7.7.7 remote-as 100
neighbor 7.7.7.7 update-source Loop0

address-family vpnv4
neighbor 7.7.7.7 activate
neighbor 7.7.7.7 send-community extended
neighbor 7.7.7.7 next-hop-self exit-address-family

router bgp 100
no bgp default ipv4-unicast
neighbor 6.6.6.6 remote-as 100
neighbor 6.6.6.6 update-source Loop0

address-family vpnv4
neighbor 6.6.6.6 activate
neighbor 6.6.6.6 send-community extended
neighbor 6.6.6.6 next-hop-self exit-address-family

MP-BGP Configuration

• IBGP full mesh between all PEs
• Exchanging VPNv4 addresses
• Flexible control mechanisms with BGP
• Verify the working of MP-BGP

  show ip bgp vpnv4
  all  Display information about all VPNv4 NLRIs
  rd   Display information for a route distinguisher
  vrf  Display information for a VPN Routing/Forwarding instance

  example:
  show ip bgp vpnv4 rd 100:1
Agenda

- MPLS-VPN Terminology
- Network Topology
- Enabling the Core
- Step-By-Step Configuration Guideline
  - Sample Configuration (VRF, Interfaces)
  - PE-CE Routing Protocol Configuration (Static, RIPv2, BGP, OSPF)
  - MP-BGP Redistribution

Adding VPN Site

1—Configure VRF Instance on PE Router

ip vrf <vrf-symbolic-name> (Name of the VPN site)
rd <route-distinguisher-value>
route-target import <Import route-target community>
route-target export <Import route-target community>

example:

ip vrf VPN-A
rd 100:1
route-target export 100:1
route-target import 100:1
Step-By-Step Configuration Guideline

Configure VRF Instance on PE Router

```
rd <route-distinguisher-value>
  You may pick a unique rd for each vrf interface
  Ease in manageability
  Can achieve load sharing using unique rd everywhere
route-target import <Import route-target community>
route-target export <Import route-target community>
  Dictates who will receive the routes
  Inter VPN connectivity is very simple by importing route-target form other VPN
  It can be same value as rd
```

Interface Serial0
ip vrf forwarding VPN-A
ip address 192.168.10.1 255.255.255.0

Verify the configuration

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>VRF</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial0</td>
<td>192.168.10.1</td>
<td>VPN-A</td>
<td>up</td>
</tr>
</tbody>
</table>
Step-By-Step Configuration Guideline

Routing Protocol Between Provider and Customer (PE and CE)

- Supported protocols
  Connected, static, RIPv2, OSPF, eBGP
- Learned routes will populate the VRF associated to the interface where the protocol is configured
- Same routing protocol instance with different routing contexts

Step-By-Step Configuration Guideline

PE-CE Routing Protocol (Static)

Static routes into VRFs need outgoing interface

```
ip vrf VPN-A
rd 100:1
route-target both 100:1
!
Interface Serial0
ip vrf forwarding VPN-A
ip address 192.168.10.1 255.255.255.0

ip route vrf VPN-A 10.0.0.0 255.0.0.0 Serial0 192.168.10.2
```

Verify the configuration

```
sh ip route vrf VPN-A
C 192.168.10.0/24 is directly connected, Serial0
S 10.0.0.0/8 [1/0] via 192.168.10.2, Serial0
```
Step-By-Step Configuration Guideline
PE-CE Routing Protocol (RIPv2)

- Routing contexts are defined within the routing protocol instance
- Follow these steps to configure RIPv2 as The PE-CE routing protocol
  - Configure per-VRF routing for RIPv2
  - Configure redistribution of MP-BGP into RIPv2
  - Configure redistribution of RIPv2 into MP-BGP

Step-By-Step Configuration Guideline
PE-CE Routing Protocol (RIPv2)

- Use RIP with stub sites and when convergence is not an issue
- Address-family router sub-command
  - `Router rip version 2 address-family ipv4 vrf <vrf-symbolic-name> ...
  ... any common router sub-command ...
...`
Step-By-Step Configuration Guideline
PE-CE Routing Protocol (RIPv2)

- **RIPv2/BGP interaction**

  During redistribution,
  
  RIP metric propagated BGP MED
  
  BGP MED automatically propagated into RIP metric
  
  Allows transparency of RIP metric through the MPLS backbone
VPN Site with BGP Configuration
PE-CE Routing (BGP)

Step-By-Step Configuration Guideline
PE-CE Routing Protocol (BGP)

BGP uses same “address-family” command
Router BGP <asn>
...
address-family ipv4 vrf <vrf-symbolic-name>
...
any common router BGP sub-command
...
Configuring OSPF in MPLS VPN Environments (OSPF)

- Follow these steps to configure OSPF as the PE-CE routing protocol
  - Configure per-VRF copy of OSPF
  - Configure redistribution of MP-BGP into OSPF
  - Configure redistribution of OSPF into MP-BGP

Per-VRF OSPF Configuration

```
router(config)#
router ospf process-id vrf name
  ... Standard OSPF parameters ...

- This command starts per-VRF OSPF routing process
- The total number of routing processes per router is limited to 32

router(config-router)#
redistributre bgp as-number subnets

- This command redistributes MP-BGP routes into OSPF; The Subnets keyword is mandatory for proper operation
```
Configuring Route Redistribution

```
router(config)#

router bgp as-number
    address-family ipv4 vrf vrf-name
    redistribute ospf process-id [match [internal] [external 1] [external 2]]
```

- OSPF to BGP route redistribution is configured with the redistribute command under the proper address-family
- Without the OSPF `match` keyword specified, only internal OSPF routes are redistributed into OSPF

Monitoring OSPF in MPLS VPN Environment

```
router#
show ip ospf

This command specifies whether an OSPF process is attached to an MPLS VPN backbone
```

```
router#
show ip ospf database type prefix

This command displays the down bit in the LSA
```

```
router#
show ip bgp vpnv4 vrf name prefix [mask]

This command displays the OSPF-specified extended BGP communities
```
Router#show ip ospf
Routing Process "ospf 250" with ID 10.2.3.4
Supports only single TOS(TOS0) routes
Supports opaque LSA
Connected to MPLS VPN Super backbone
It is an area border and autonomous system
boundary router
Redistributing External Routes from,
bgp 1, includes subnets in redistribution

Final Step: PE Distributing
CE Routes with MP-BGP

router bgp 100
!
address-family ipv4 vrf site2
neighbor 192.168.62.2 remote-as 65502
neighbor 192.168.62.2 activate
redistribute ospf 250
exit-address-family
!
address-family ipv4 vrf site1
neighbor 192.168.61.1 remote-as 65501
neighbor 192.168.61.1 activate
redistribute ospf 250
exit-address-family
!
exit

router bgp 100
!
address-family ipv4 vrf site4
neighbor 192.168.74.4 remote-as 65504
neighbor 192.168.74.4 activate
redistribute ospf 250
exit-address-family
!
address-family ipv4 vrf site3
neighbor 192.168.73.3 remote-as 65503
neighbor 192.168.73.3 activate
redistribute rip metric 2
exit-address-family
!
exit
PE2#sh ip route vrf site3 bgp 100
Show IP BGP VPNv4 VRF Name Prefix

Router#show ip ospf vpnv4 vrf Customer_A 10.0.1.0
BGP routing table entry for 1:10:10.0.1.0/24, version 64
Paths: (1 available, best #1, table Customer_A)
  Advertised to non peer-group peers:
    10.2.3.6
    Local
      10.2.3.4 from 0.0.0.0 (10.2.3.4)
      Origin incomplete, metric 2, localpref 100, weight 32768, valid, sourced, best
      Extended Community: RT:100:27 OSPF RT:0:3:0

MPLS VPN—Configuration Summary

- Identify PE routers
- Enable MPLS in the core routers
- Configure MP-BGP between PEs (Route-Reflector or full-mesh)
- Configure VRF instance for each VPN  
  Design rd and route-target assignments
- Identify Interfaces going to VPN sites  
  Assign interfaces to the VRF instance
- Choose the routing protocol between PE and CE  
  Configure necessary redistribution between MP-BGP and VRF routing protocol
MPLS VPN—Configuration
PE Router Commands

- All show commands are VRF-based
  - `show ip route vrf <vrf-symbolic-name> ...`
  - `show ip protocol vrf <vrf-symbolic-name>`
  - `show ip cef vrf <vrf-symbolic-name> ...
    ...

- PING, Telnet, Traceroute commands are VRF-based
  - `ping vrf <vrf-symbolic-name>`
  - `telnet/vrf <vrf-symbolic-name>`
  - `traceroute vrf <vrf-symbolic-name>`

Scaling MPLS VPN Network
Agenda

- Policy on Route-Target Import and Export
- Maximum Routes in a VRF
- Route Reflectors
- Route Reflector Partitioning
- Outbound Route Filtering
- Carrier Supporting Carrier
- Inter-AS for MPLS VPN

Scaling VPN Network
Requirement/Solution

- Number of route-target imports into VRFs
  Depending on the VPN topology: hub and spoke or full mesh
- Policy on route-target import and export
MPLS/VPN Scaling

- MPLS/VPN architecture is very highly scalable:
  - Architecture supports 100,000+ VPNs, 10,000,000+ sites
- No single BGP router can hold all Internet and all VPN routing information
  - Additional routing information segmentation is essential
  - Partitioned route reflectors improve MPLS/VPN scalability

Policy with Route-Target Import and Export

- Size of the BGP table is proportional to the number of route-target import into VRFs configured on the PE router
- Non-reflecting PE router discards any VPN-IPv4 route that hasn’t a route-target configured to be imported in any of the attached VRFs
- To reduces significantly the amount of information each PE has to store, reduce the number of route-target required for each VPN
Policy with Route-Target Import and Export

- Automatic MP-BGP updates filtering for each VRF-based on policy with route-target extended BGP community
- If route-target in incoming MP-BGP update is equal to any of the import values configured in this PE router, the update is accepted, otherwise it is silently discarded
- The automatic filtering only works for non-reflecting routers—when the first route-reflector client is configured, the update filtering is disabled

Scaling VPN Network Requirement/Solution

- Number of routes in a VRF
- Limit the maximum number of routes allowed for a VRF
Maximum Routes

- Prevent the PE from learning too many routes from a site
- Specify “Maximum routes” limit with an action:
  - Rejects routes or
  - Warn only: issues a SYSLOG error message only
- Applied per VRF
  ip vrf vrf1
  rd 100:1
  route-target import 100:1
  maximum routes 1000 warn-only

Scaling VPN Network Requirement/Solution

- Scalability of full mesh IBGP peering
- Avoid duplicating route advertisement and maintaining session
- Use route reflectors
Route Reflector

- IBGP full mesh between PEs results in flooding all VPNs routes to all PEs
- Existing BGP techniques can be used to scale the route distribution: route reflectors
- Each edge PE router needs only the information for the VPNs it supports
  Only routes for VRFs configured on the PE router
- Route-reflectors are used to distribute VPN routing information

Dedicated VPNv4 Route Reflectors

- Dedicated VPNv4 route-reflectors can be deployed to improve scalability
  PE routers still carry Internet routes and a subset of VPN routes
  Selectively activate IPv4 and VPNv4 sessions on PE routers
- Free the PE from having to maintain full mesh for IBGP and route duplication to all other PEs
Dedicated VPNv4 Route Reflectors

- Dedicated VPNv4 route reflectors are deployed to improve scalability
- Route reflectors for each address family must be redundant to avoid single point-of-failure

Configuration for VPNv4 Route Reflectors

```
router bgp 115
  no bgp default ipv4 unicast
  neighbor 172.16.1.2 remote-as 115 ! IPv4 RR
  neighbor 172.16.1.2 activate
  address-family vpnv4
  neighbor 172.16.1.2 activate
  neighbor 172.16.1.2 send-community extended
```

- Enable IPv4 and VPNv4 sessions with route-reflectors only
Scaling VPN Network
Requirement/Solution

- Number of VPN routes on the network
  Include and routes from all VPNs and global routing table
- Use route reflector partitioning

Route Reflectors Partitioning

- With additional growth of VPN customers, the VPN route-reflectors cannot handle all VPN routes
- Deploy partitioned VPN route-reflectors
  Partition VPN routes based on route target (for example, dedicated RR for large customers) or
  Partition VPN routes based on other BGP attributes (for example, BGP community)
Partitioned VPNv4 Route Reflectors

- No BGP router needs to store all VPN information
- (Optional) PE routers will peer with route-reflectors according to the VPNs that are connected to the PE routers

BGP Route-Reflector Group

```
routet(config-router)#
bgp rr-group extcommunity-access-list
```
- Configures route-target-based inbound filter on a route-reflector
- Easier to configure than an inbound route-map
- Can be transformed into outbound filter at other PE routers through ORF functionality
Partitioned Route Reflector Inbound

- Inbound filters on route-reflectors reduce maintenance costs
  Increase CPU utilization on route-reflectors
- bgp rr-group filter is an optimal solution
  Filter maintenance performed on route-reflector
  Actual filtering process performed on PE router

Scaling VPN Network Requirement/Solution

- Decrease the size of routing updates from RR
- Outbound route filtering
MPLS-VPN Scaling
Outbound Route Filters—ORF

- Non-reflecting PE routers will discard updates with unused route-target
- To optimize resource utilization, these updates should NOT be sent
- Outbound Route Filter (ORF) allows a PE router to tell its neighbors which routes to filter in outbound BGP updates

Scaling VPN Network
Requirement/Solution

- Large number of routes per VPN
- Such as SP as customer
- Use Carrier Supporting Carrier
Carrier Supporting Carrier

- Some VPNs carry large routing information within the sites, including the internet routing table
- With CSC, PE does not learn all routes for a VPN
- PE learn minimal number of routes enough to provide the connectivity between the VPN sites
- PE-CE access is MPLS enabled
- PE-CE advertisement: routes with OSPF/RIP and labels with LDP
- CE establishes label switching paths with other VPN sites and is an MPLS edge

Carrier Supporting Carrier

- Customer’s external routes are IPv4 routes
- IBGP for exchanging customer’s external routes (Internet routes) among (and within) sites
- OSPF/RIP for exchanging customer’s internal routes (routes for BGP Next Hop) between sites and VPN service provider (between CE and PE)
- LDP for exchanging labels with VPN service provider (between CE and PE)
- MPLS forwarding is extended to the customer’s CE routers
Carrier Supporting Carrier

- Partition customer’s routes into internal and external
- Customer’s internal routes are carried by VPN Service Provider(s)
- Customer’s external routes are carried only by the customer’s routers
  - Exchanged via IBGP among sites that belong to the same organization (intranet VPN) or
  - Exchanged via (multi-hop) EBGP among sites that belong to different organizations (extranet VPN)
- Specification described in RFC2457
Scaling VPN Network Requirement/Solution

- VPN crossing multiple BGP domain
- Inter-AS for MPLS VPN

Inter-Autonomous System for MPLS VPN

- Allows a VPN to span service providers and autonomous systems
- Establishes eBGP session between the border edge PE
- Distribute IPv4 routes for the VPNs in the form of VPNv4 addresses
- EBGP border edge router rewrite the next-hop address and new MPLS labels
- Uses MPLS to forward the traffic end-to-end and across the AS’s
Inter-AS MPLS-VPN Backbones

VPNv4 Routes Exchange

Routing Between Autonomous Systems

- VPNs spans across separate autonomous systems in BGP confederation
- Allows confederations to optimize IBGP meshing
- Each AS operates under different administrative control and runs different IGP
- Exchange VPNv4 routing information through EBGP border router
- Each PE assigns labels for the routes to establish connections
Inter-AS MPLS-VPN Backbones VPNv4 Routes Exchange

- Providers exchange route between PE-ASBR routers
- MP-eBGP for VPNv4 addresses between ASBRs
  - Next-hop and labels are re-written by the PE-ASBRs
- Requires PE-ASBRs to store ALL VPN routes that need to be exchanged
- Routes are in the MP-BGP table but not in any routing table
  - PE-ASBRs do not have any VRF
  - MP-eBGP labels are used in LFIB
Agenda

- Deploying MPLS VPN
- Scaling MPLS VPN Network
- Internet Access
- Central and Remote Access Services
- Provisioning

Internet Access

Firewall can be:
- CPE or Network-based
- Dedicated or Shared
- SP Managed or Corp Managed

Ex. Dedicated FW, Managed by Corp but Hosted by SP, Providing Direct Internet Access to All VPN Sites

Bandwidth Control
Internet Access Concepts

• Factors for Service Provider to consider
  
  Customer with no NAT/no firewall requirements
  Customer with NAT, but no firewall requirements
  Customer with firewall, but no NAT requirements
  Customer with NAT and firewall requirements
  Central vs distributed—Who is responsible for these?
  End customer expects a service offering
  Note: Security requirements between Intranet and Internet

Internet Access
Existing Customer Requirements

• What do customers have at the moment?
  
  A secure private network via VPNs or leased lines
  One or more secure connections to the Internet
Internet Access: Possible Implementation Scenarios

- Simple solution
- VPN to Internet via subinterfaces
- Single Router and managed firewall gateway

Internet Access: Simple Solution

- Advantages of the simple solution
Internet Access: Simple Solution

![Diagram of Internet Access: Simple Solution](image)

Internet Access: VPN to Internet Via Subinterfaces

- Sub optimal routing in Service Provider core network
- Full Internet routing table available at central Site CE
- Two logical subinterfaces which might incur additional costs
- Central site needs to differentiate between Internet and VPN traffic
Internet Access: VPN to Internet Via Subinterfaces

Central Site

Outbound Traffic Flow

Internet Transit

MPLS-VPNs

MPLS Core

Central Site

Inbound Traffic Flow

Internet Transit

MPLS-VPNs

Central Site

VPN Traffic Flow
Internet Access: Single Router and Managed Firewall Gateway

- Service Provider supplies managed firewall service
- Only single VPN connection between each customer site and Service Provider network required
- Provides a gateway from the VPN to the global routing table so the first non-VPN router can be any PE router in the MPLS core
- Full Internet routing table available to customers using eBGP multihop peering to external Internet PE router
- Allows for optimal routing with minimum hops through MPLS core
Internet Access: Single Router and Managed Firewall Gateway

Internet Access: Scenario Review

- Simple Solution
  Recommend
- VPN to Internet via Subinterfaces
  Recommend
- Single Router Managed Firewall Gateway
  Recommend
- Different Solutions Appropriate for the individual requirement
Internet Access Summary

- Service Provider opportunity
  - Provide end customer option to buy Internet connectivity for corporate VPN
  - CPE-based Firewall all VPN sites send traffic to a specific customer site where centralized customer or service provider managed firewall is located
  - Network based Firewall all corporate VPNs have direct Internet access via network-based firewall (could be dedicated)
  - Extend value-add for “basic” site-to-site services

Central Services for VPN Service Providers

- New value added services
- Provide connectivity and servers infrastructure
- Application independent: server hosting, security, quality of service guarantees
- Application servers: web, DNS, email POP, AAA
- Specialized servers: database, VoIP dial plan, multicast servers, e-learning
- Benefits both: SP and customers
Server Hosting with VPN Aware POP

- POP or co-location network is VPN aware
- Each VPN is mapped into dedicated VLAN
- PE connect directly to VLAN trunk to Ethernet switch
- PE is conduit into the MPLS VPN backbone
- Servers are intranet or extranet servers
- Dedicated servers per VPN, or shared with application authorization
- Hosted firewall service
- Internet access for VPN sites
- Nearest POP for optimum routing to the servers
Remote Access to MPLS VPN Solution Benefits

- Whole sale dial and DSL solution into VPN
- Removes the need for VPDN (No tunnels required in backbone) and achieves optimal routing
- Customer home gateway is no longer needed and SP can offer managed home gateway Service (virtual home gateway)
- Virtual profiles enables scalability to high density
- Provides management capabilities IP address, AAA, remote access to MPLS VPN

**RA to MPLS VPN Solution**

- **Access Technology Specific Solutions**
  - Dial Access
  - DSL Access
  - Cable Access, DOCSIS
  - Fixed Wireless Access

- **Common Solution Independent of Access Technology**
  - SP AAA Server
  - SP DHCP Server
  - Customer AAA Server
  - Customer DHCP Server
Automation: Just-In-Time Provisioning Mechanism

Create the PE/CE Configlet
- Telnet or SSH to PE
- Upload Current Configuration
- Telnet or SSH to CE
- Upload Current Configuration
- Download and Activate Services

Topology View of VPNs

- MPLS/VPN PE and CE Views
- MPLS/VPN CE to CE Views
VPN Topology Formation

- Formation of routing communities for VPN connectivity
- Allows provisioning of arbitrary mesh without knowledge of BGP
- Auto picks values for route targets once communities are specified
- Hub and spoke and full mesh topology support
- Extranet provisioning

Template Provisioning System

- Allows flexible and smart provisioning of any IOS commands
- Components
  - Template manager GUI
  - Template API
- Template definition language
  - Rich set of data types and expressions
  - Dimensional arrays, strings, float, more...
  - Tied to VPNSC VPN Service request
Example—Templates
Any IOS Command Set

- Template language written used to emulate IOS router configurations
- Data Merged with Template Language to create device configuration

Provisioning MPLS/VPN Services
VPN Solution Center

- Generates VPN IOS commands automatically
- Just in time provisioning
- Manages IP addresses, RD and RT values and VRF’s
- Audits of both configuration and routing to verify VPN connectivity
- Supports managed and unmanaged VPN
- Automatic management VPN provisioning
- Latest hardware support
  Cable, DSL, GSR, ESR, MGX, others…
Summary

• Apply the right tools in the right place helps make the VPN network scale
• Use advanced features for special cases and value added services
• Consider alternatives for Internet access based on requirements
• Test and understand before you implement
• Use network management tools to automate provisioning and monitoring
Other Networkers MPLS Sessions

- RST-130: Introduction to MPLS
- RST-231: Deploying MPLS for Traffic Engineering
- ISP-231: Deploying QoS in SP Networks
- RST-330: Troubleshooting MPLS for Traffic Engineering
- RST-331: Troubleshooting ATM MPLS Networks
- RST-430: Advanced Developments and Concepts in MPLS
- PS-542: MPLS-Technology Options and Applications

Useful Information

- CCO MPLS page
  http://www.cisco.com/go/mpls
- Cisco IOS 12.0ST Documentation
- “MPLS and VPN Architectures” book
Deploying Large Scale VPN with MPLS

Session RST-230

Please Complete Your Evaluation Form

Session RST-230