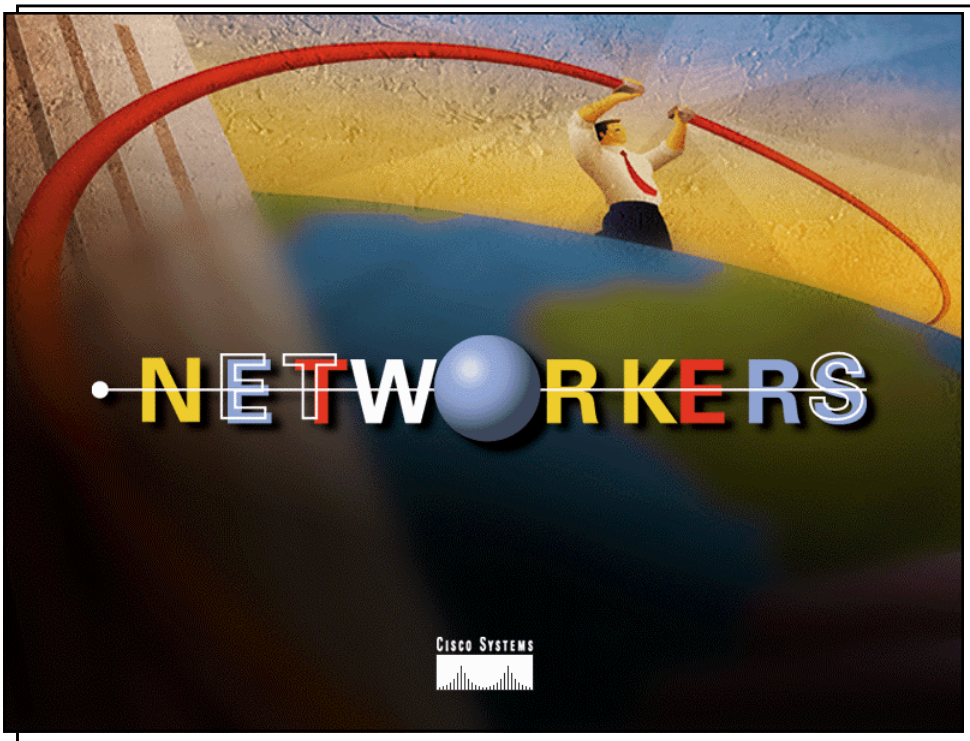
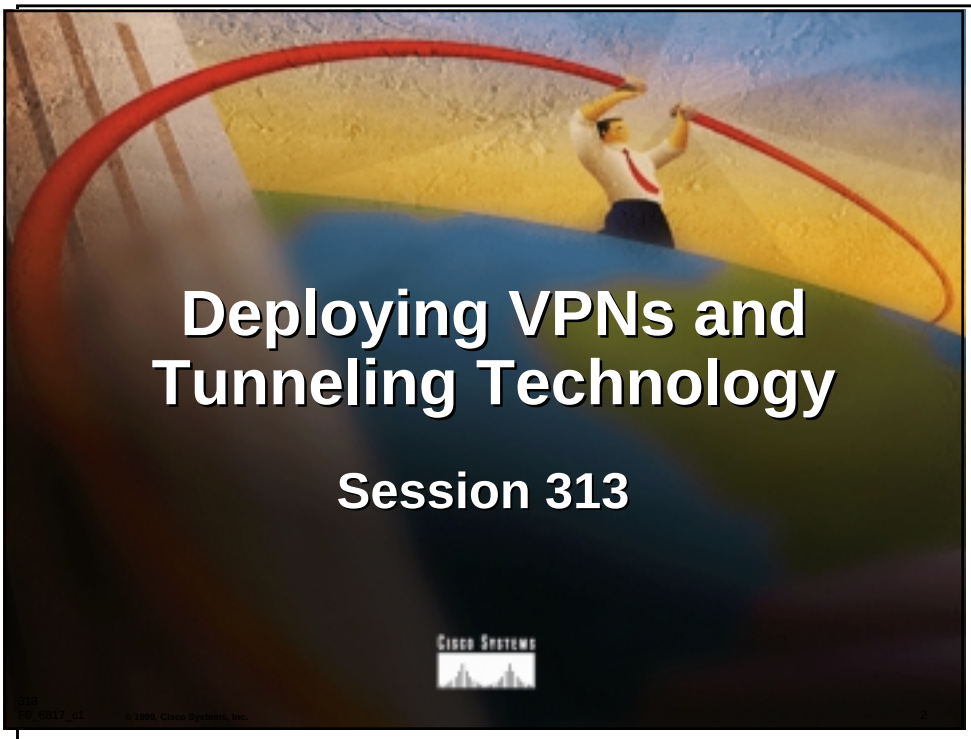




Agenda

- Scope of the Session
- VPN Overview
- Enterprise Dial/Access VPNs
- Enterprise Intranet/Extranet VPNs
- Service Provider VPNs
- Next Generation VPN Solutions

Scope of this Session

- A VPN survey with design guidelines, service options, and configuration examples
- For in-depth IPSec coverage, attend “Advanced Security Technology Concepts”
- For in-depth coverage of network management issues, attend “Evolution of Network Management Technologies”
- For in-depth coverage of QoS issues, attend “Deploying Traffic Management (QoS) Technology”
- For a survey of enterprise QoS, security, monitoring and provisioning products, attend “New Developments for the Enterprise Virtual Private Network”

Virtual Private Network (VPN) Defined

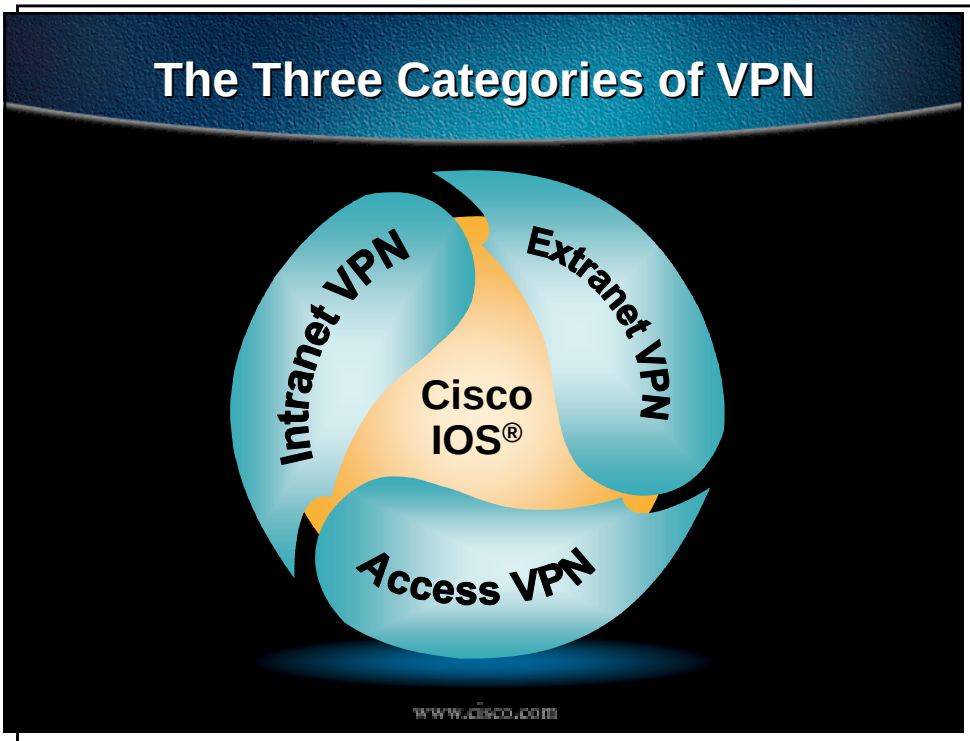
"A Virtual Private Network Carries Private Traffic Over a Public Network"

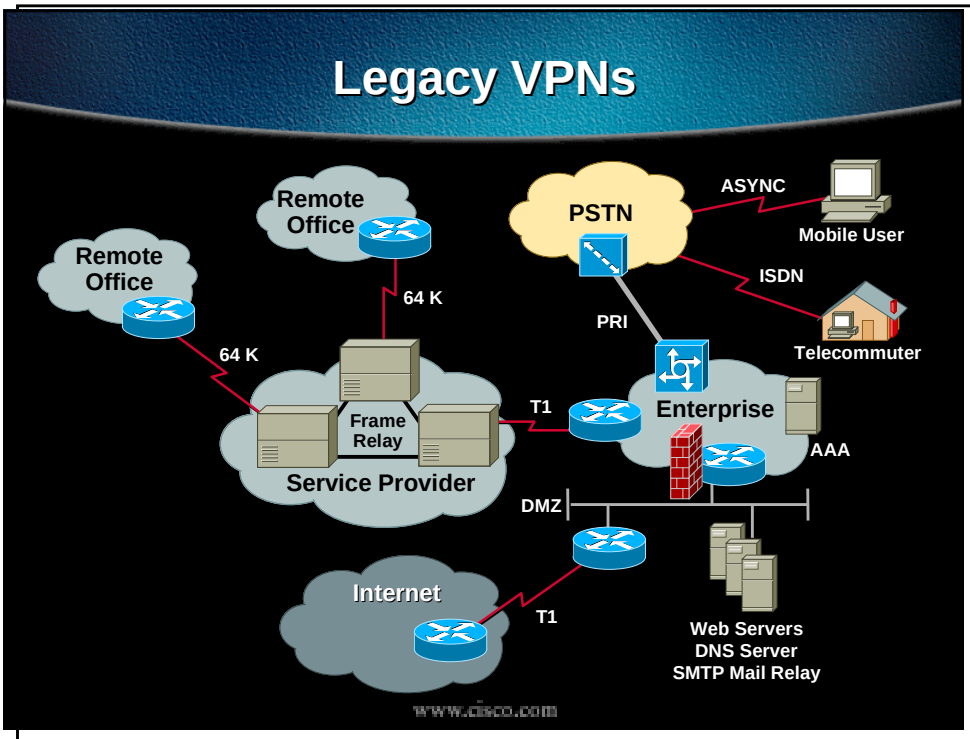
www.cisco.com

What Is a "Public" Network?

- In this context, any network **shared** among different administrative domains
- A shared network such as the Internet
- A privately owned network which services many customers, such as a long distance telephone network

www.cisco.com



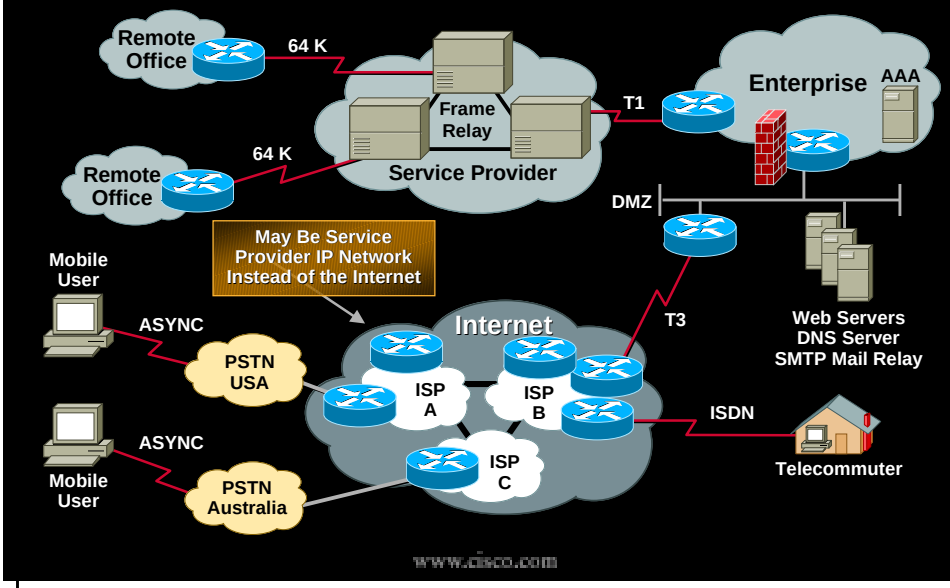


Agenda

- Scope of the Session
- VPN Overview
- **Enterprise Dial/Access VPNs**
- Enterprise Intranet/Extranet VPNs
- Service Provider VPNs
- Next Generation VPN Solutions

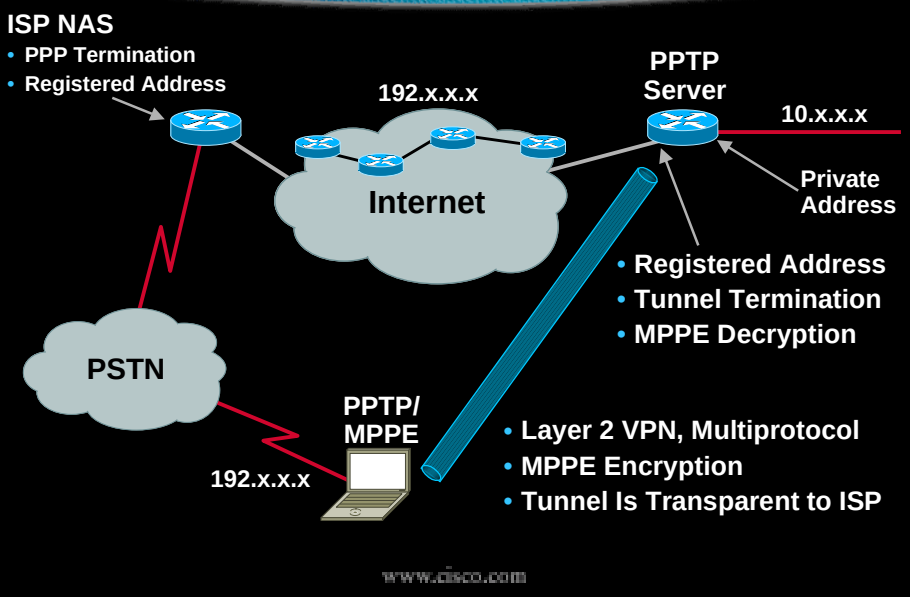
www.cisco.com

Enterprise Dial Outsourcing



www.cisco.com

PPTP/MPPE (Voluntary Tunneling)

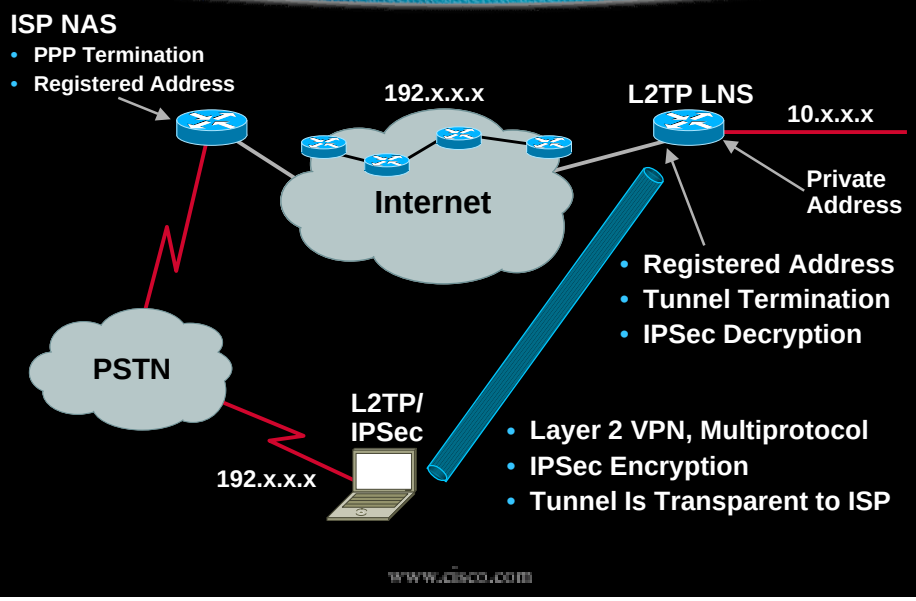


PPTP/MPPE Considerations

- PPTP/MPPE is built into Windows dial-up networking
- Stateful MPPE encryption changes the key every 255 packets, flow control is useful in this case
- Stateless MPPE encryption generates a new key for every packet
- Stateless MPPE is only supported in recent versions of Dial Up Networking

www.cisco.com

L2TP/IPSec (Client Mode L2TP with Transport Mode ESP)

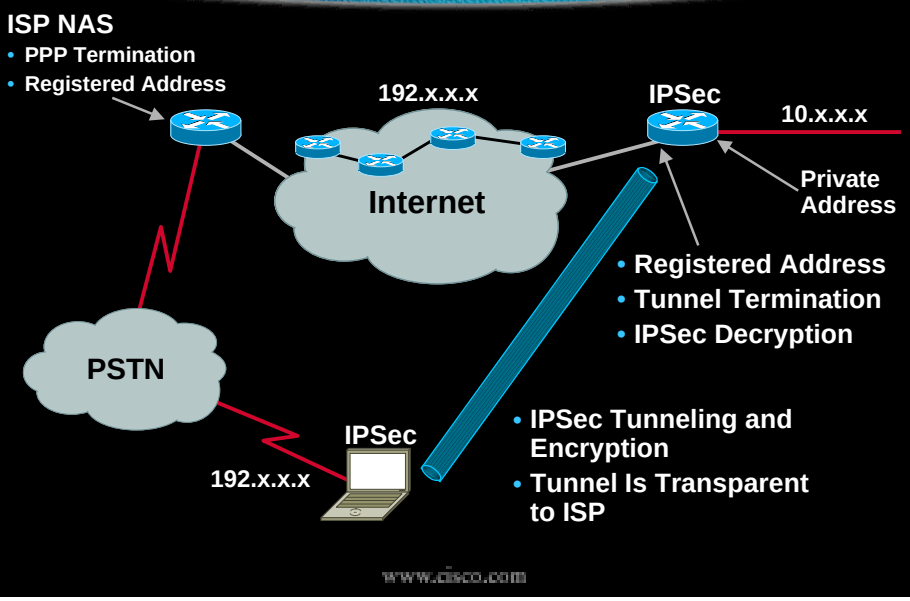


L2TP/IPSec Considerations

- Need client software, bundled into Windows 2000
- Multivendor, multiprotocol, standards track
- Most robust security solution
- Scales with certificate authority support

www.cisco.com

IPSec Alone (Tunnel Mode with ESP)



IPSec Alone Considerations

- Client software need not support L2TP
- Open standards client
- Layer 3 VPN, so IP only
- IKE extensions provide AAA
- Scales with certificate authority support

www.cisco.com

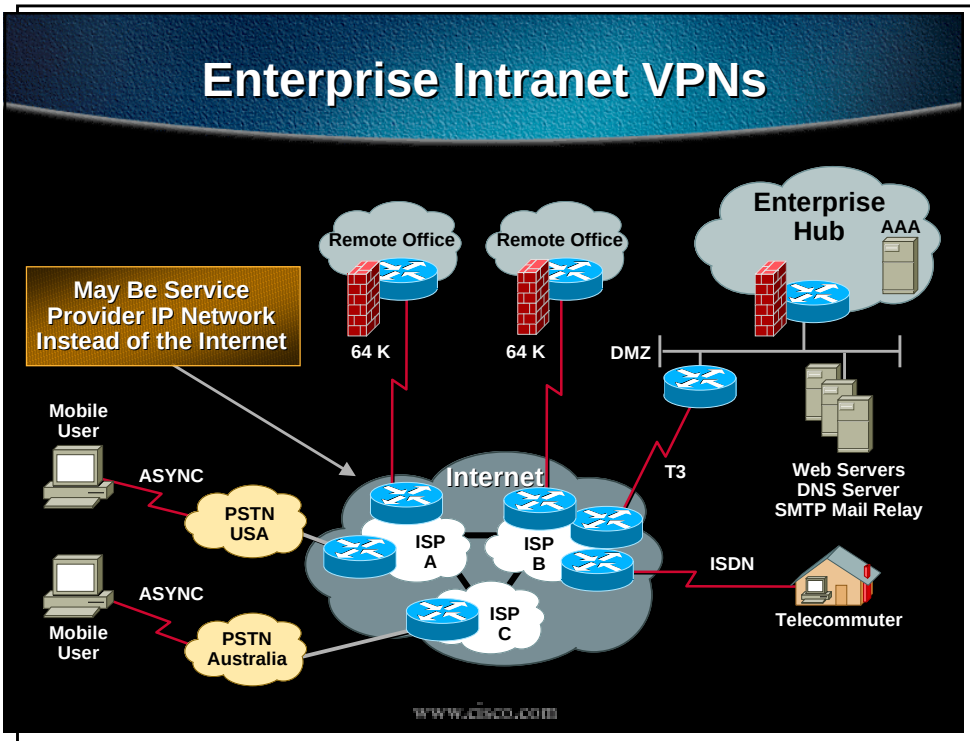
Enterprise Dial/Access VPN Summary

Pro	• Service Provider Independent • Reduced Cost for Enterprises • No Long Distance Phone Charges
Con	• No Resource Availability Guarantees • No Quality of Service Guarantees • Performance Dictated by Weakest Link in the Internet • Must Manage Client Software

Agenda

- Scope of the Session
- VPN Overview
- Enterprise Dial/Access VPNs
- **Enterprise Intranet/Extranet VPNs**
- Service Provider VPNs
- Next Generation VPN Solutions

Enterprise Intranet VPNs



Enterprise Intranet VPN Technologies

- Routing variants
- IP in IP
- L2TP router to router
- GRE tunneling
- IPSec in tunnel mode

Routing Variants

- VPNs through obscurity (per customer ACLs)
- Policy routing

www.cisco.com

IP in IP

- Used mainly by mobile users, mobile LAN, dial, wireless, packet radio
- RFC 1853s, 2003
- IETF mobile IP working group
- Similar to GRE

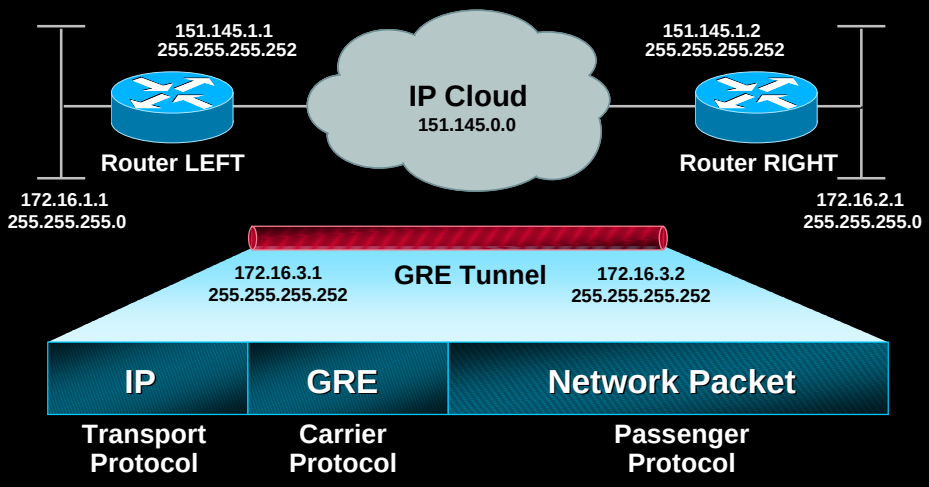
www.cisco.com

L2TP LAN to LAN

- L2TP dynamic tunneling for LAN-based clients
- Useful for remote LANs that may need to connect to one of many sites
- Similar to GRE

www.cisco.com

Generic Route Encapsulation (GRE)



www.cisco.com

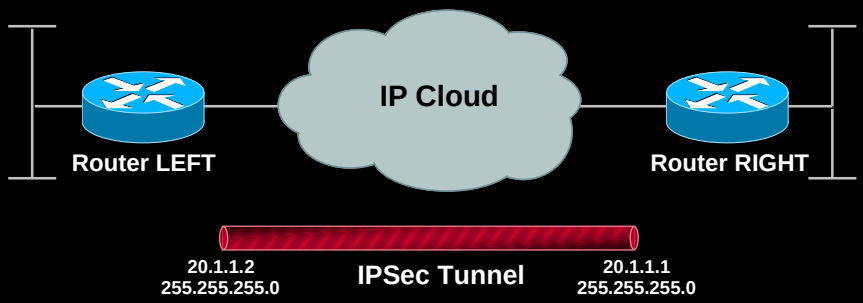
GRE Configuration
Router LEFT Configuration

- Network 151.145.x.x is in publicly routable address space (routable over the Internet or other shared network)
- Routes for 151.145.x.x are not propagated in private network 172.16.x.x
- Serial interfaces are point-to-point connections across the public network
- May be designed as a hub and spoke, the configuration is the same except the hub has tunnels to each spoke

```
Interface Ethernet 0
  ip address 172.16.1.1 255.255.255.0

Interface Serial 0
  ip address 151.145.1.1 255.255.255.0

Interface Tunnel 0
  ip address 172.16.3.1 255.255.255.252
  tunnel source Serial 0
  tunnel destination 151.145.1.2

router eigrp
  network 172.16.0.0
  no auto-summary

ip route 151.145.0.0 255.255.0.0 Serial 0
```

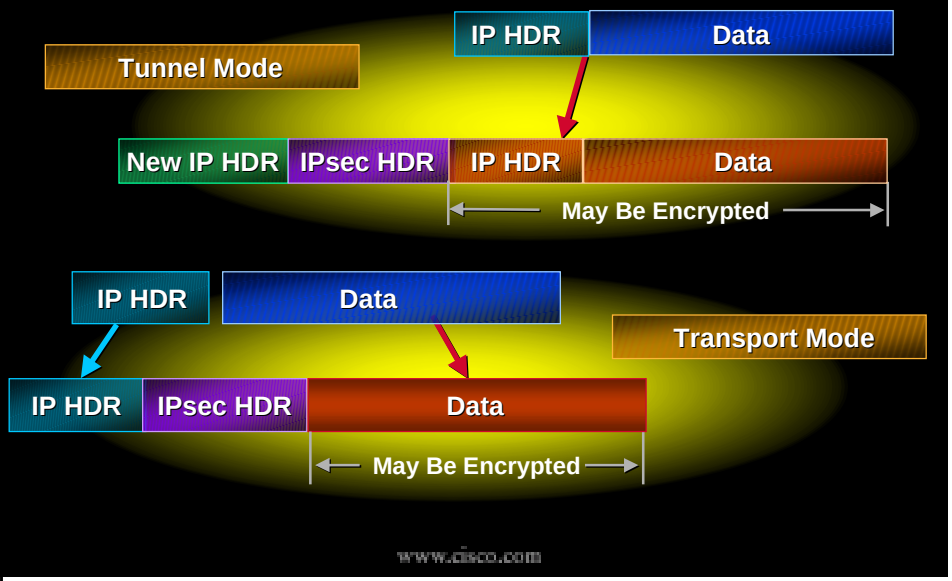
www.cisco.com

IPSec



www.cisco.com

IPSec Modes



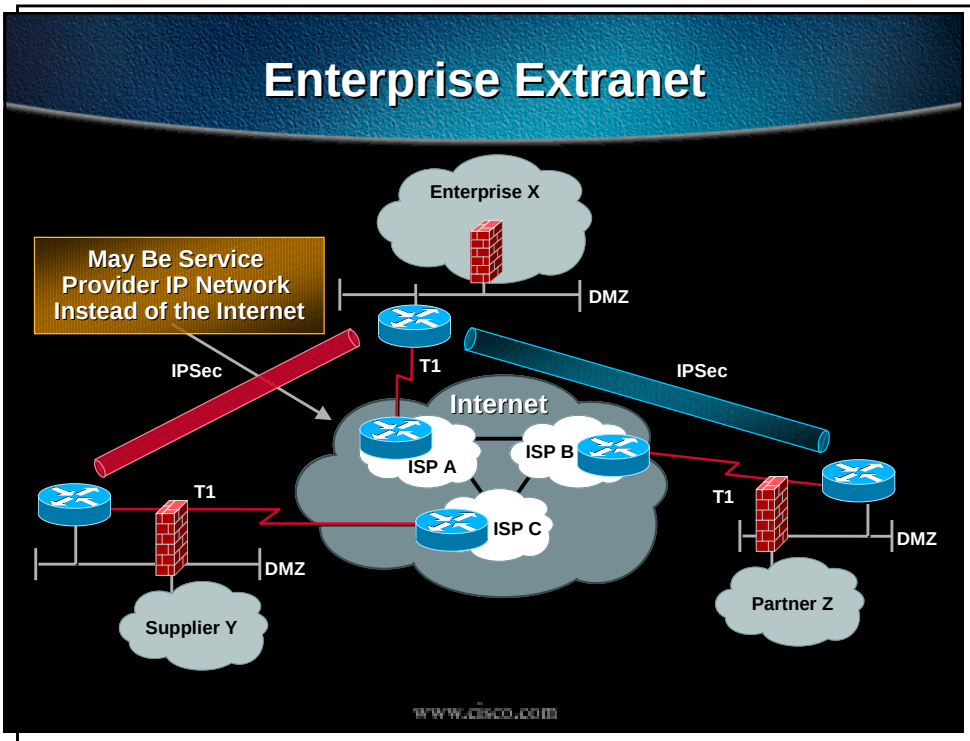
IPSec Router LEFT Configuration

- A simple IPSec config that uses pre-shared keys instead of a CA
- Multiple policies may be defined
- Tie the crypto map to the outbound interface
- In this example, only PING (or other ICMP traffic) will be encrypted

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 3600
crypto isakmp key cisco address 20.1.1.1
!
crypto ipsec transform-set Foo ah-md5-hmac esp-des
crypto ipsec transform-set Foo2 ah-sha-hmac esp-des
crypto ipsec transform-set Foo3 ah-md5-hmac esp-3des
!
 crypto map CryptPing 10 ipsec-isakmp
 set peer 20.1.1.1
 set security-association lifetime seconds 300
 set transform-set Foo Foo2 Foo3
 match address 101
!
interface Serial0
 ip address 20.1.1.2 255.255.255.0
 crypto map CryptPing
!
access-list 101 permit icmp host 20.1.1.2 host 20.1.1.1
```

www.cisco.com

Enterprise Extranet



Enterprise Intranet and Extranet VPN Summary

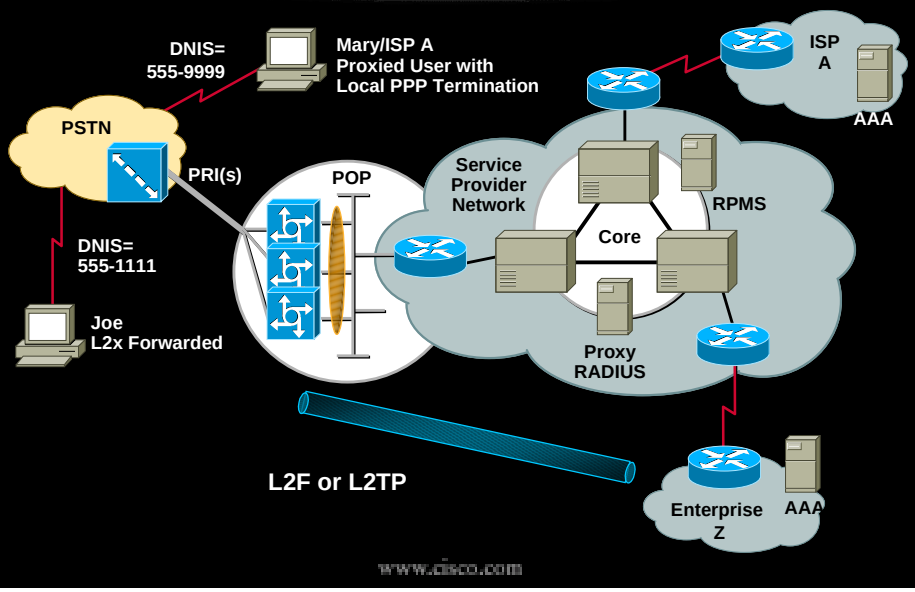
Pro	• Service Provider Independent • Reduced Cost for Enterprises • Quick and Easy Provisioning
Con	• No QoS Guarantee • Performance Dictated by Weakest Link in the Internet

Agenda

- Scope of the Session
- VPN Overview
- Enterprise Dial/Access VPNs
- Enterprise Intranet/Extranet VPNs
- Service Provider VPNs
- Next Generation VPN Solutions

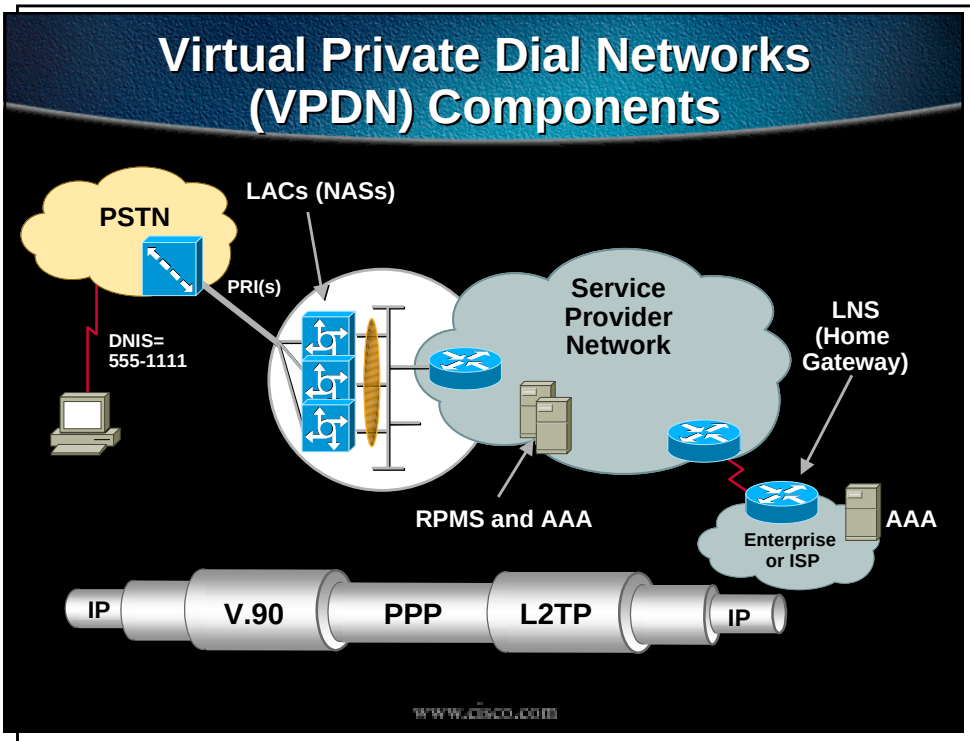
www.cisco.com

Service Provider Enterprise Outsourcing and Wholesale Dial



www.cisco.com

Virtual Private Dial Networks (VPDN) Components



L2TP Basic Cisco IOS Commands

```
LAC:
vpdn-group 1
 request dialin [l2f|l2tp] ip x.x.x.x [domain|dnis] <y>
 local name <foo>
 l2tp tunnel password <password>

LNS:
vpdn-group 1
 accept dialin [l2f|l2tp|any] virtual-template 1 remote <y>
 local name <foo>
 l2tp tunnel password <password>
```

www.cisco.com

L2TP LAC Configuration through AAA

- Enables centralized configuration of NAS/LACs
- Simplifies and standardizes NAS/LAC configuration
- RADIUS, TACACS+
- Resource Pool Management (RPM) adds the ability to configure this locally in the Cisco IOS

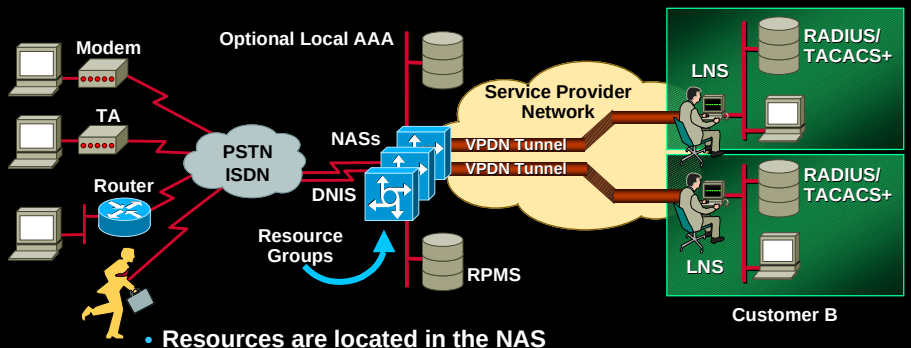
RADIUS Tunnel Attribute Sample Configuration

```
foo.com     Password = "cisco  User-Service = Outbound-User
      Tunnel-type = L2TP,
      Tunnel-Medium-Type = IP,
      Tunnel-Server-Endpoint = "10.1.1.1, 10.1.1.2, 10.1.1.3",
      Tunnel-Id = "nas-pool",
      Tunnel-Password = "welcome"
```

Cisco-specific AV-Pairs Are Also Supported in Earlier Versions of the Cisco IOS, for Example:

```
5551212   Password= "cisco" User-Service = Outbound-user,
          cisco-avp="vpdn:ip-addresses=10.1.1.1,10.1.1.2/20.1.1.1",
          cisco-avp="vpdn:tunnel-id=nas-pool",
          cisco-avp="vpdn:tunnel-type=l2tp",
          cisco-avp="vpdn:l2tp-tunnel-password=welcome”
```

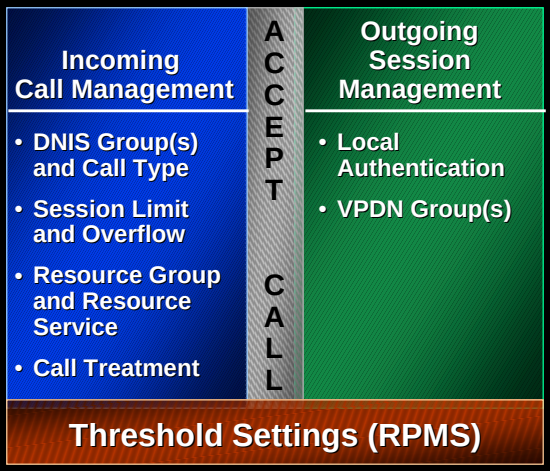
Resource Pool Management (RPM) Network Layout



- Resources are located in the NAS
- Information captured at call setup
  - DNIS, Call Type, CLID
- Public network interfaces supported
  - PRI, CT1, CT3, CE1, SS7
- Resource pool management may be located:
  - In the NAS (if single NAS) or in a Resource Pool Manager Server

www.cisco.com

RPM Customer Profile Components



www.cisco.com

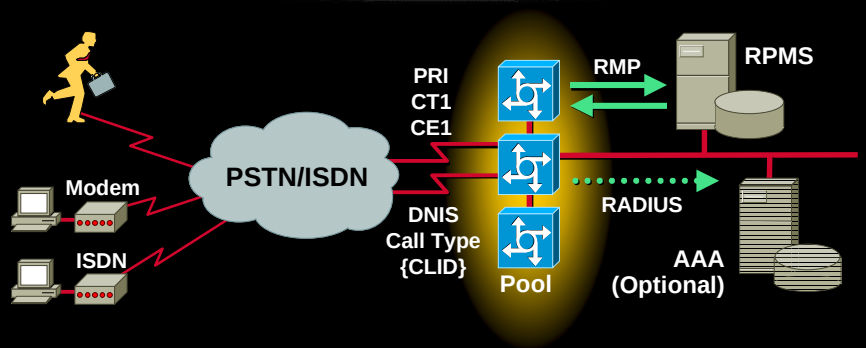
Resource Pool Management Cisco IOS Command Sample

```
resource-pool enable
vpdn enable
!
resource-pool group resource ISDN1
 range limit 46
!
vpdn-group VG1
 request dialin l2tp ip 10.1.1.1 dnis DG1
 local name NAS1
 dnis DG1
 loadsharing ip 10.1.1.1 limit 12
 loadsharing ip 10.1.1.2 limit 12
 backup ip 10.1.1.3
```

```
resource-pool profile customer FOO1
 limit base-size 16
 limit overflow-size 8
 resource ISDN1 digital
 dnis group DG1
 vpdn group VG1
!
dialer dnis group DG1
 number 5551212
 number 5553434
```

www.cisco.com

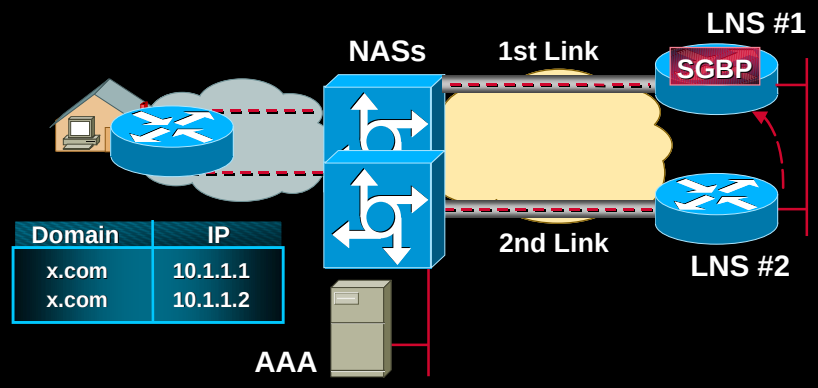
RPMS Control



- Customer profiles stored in the RPMS
- RPMS may control a single NAS, or multiple NASes in a single or multiple PoP definitions
- Utilizes Resource Manager Protocol (RMP)

www.cisco.com

Stackable L2TP LNSs and Multilink PPP



- SGBP determines bundle owner
- Multihop code forwards link

www.cisco.com

Stacking Home Gateways/ LNS's Configuration

```
hostname LNS1
!
username LNSstack password 7 00071A150754
!
multilink virtual-template 1
!
sgbp group LNSstack
sgbp member LNS2 10.1.1.2
sgbp member LNS3 10.1.1.3
sgbp member LNS4 10.1.1.4
!
vpdn multihop
```

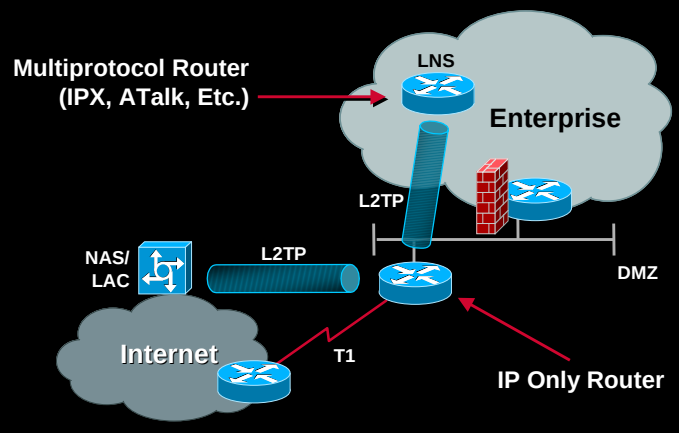
www.cisco.com

QoS Considerations

- The IP ToS byte may be copied from the IP header down to the L2TP header for class-based queuing
- Individual tunnels/VCs can have standard QoS techniques applied such as CAR and traffic shaping

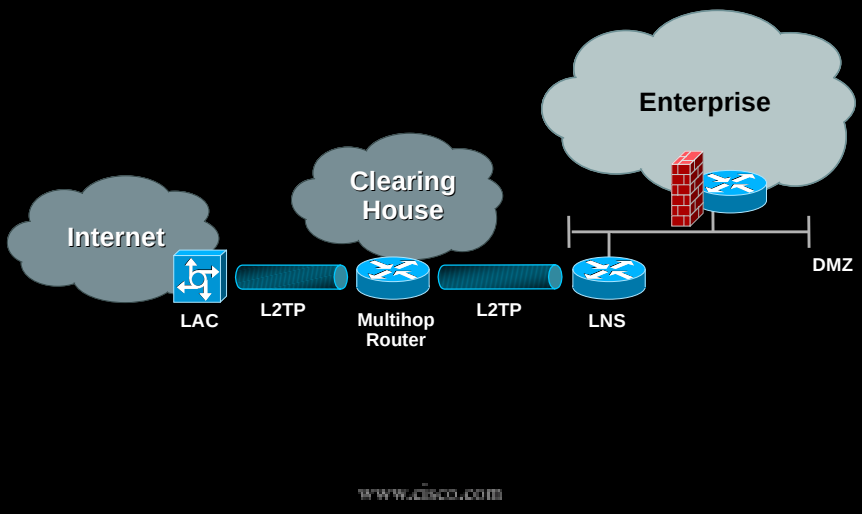
www.cisco.com

L2TP Multihop for Multiprotocol



www.cisco.com

L2TP Multihop for Clearing House Model



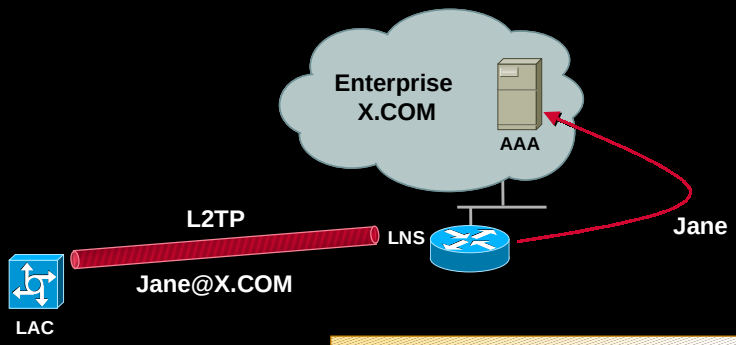
www.cisco.com

L2F/L2TP Multihop Configuration

```
vpdn enable
vpdn multihop
!
vpdn-group 1
  accept dialin l2tp virtual-template 1 remote cs1
  local name cs2
!
vpdn-group 2
 request dialin l2tp ip 10.1.1.1 domain x.com
  local name cs2
```

www.cisco.com

Domain Name Stripping Configuration



Cisco IOS config:

```
ip host x.com 10.1.1.1
...
radius-server host 10.1.1.1
radius-server directed-request restricted
```


Service Provider VPN Summary

Pro	• Service Guarantees Such as Modem Reservation and QoS • Service Provider IP Network Reliability and Privacy • No Client Software to Manage
Con	• Must Contract with Service Provider(s) • Coverage Area May Not Be as Great

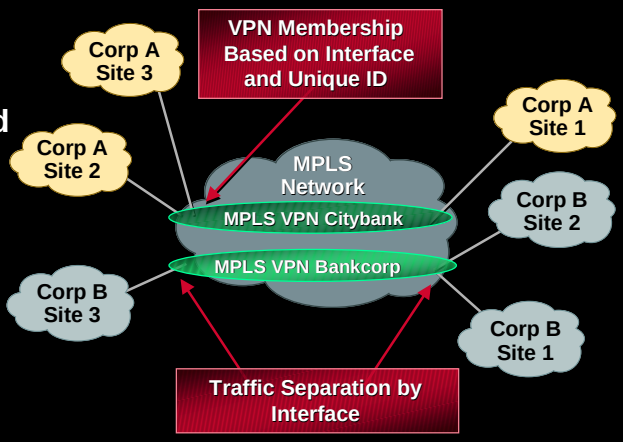
Agenda

- Scope of the Session
- VPN Overview
- Enterprise Dial/Access VPNs
- Enterprise Intranet/Extranet VPNs
- Service Provider VPNs
- Next Generation VPN Solutions

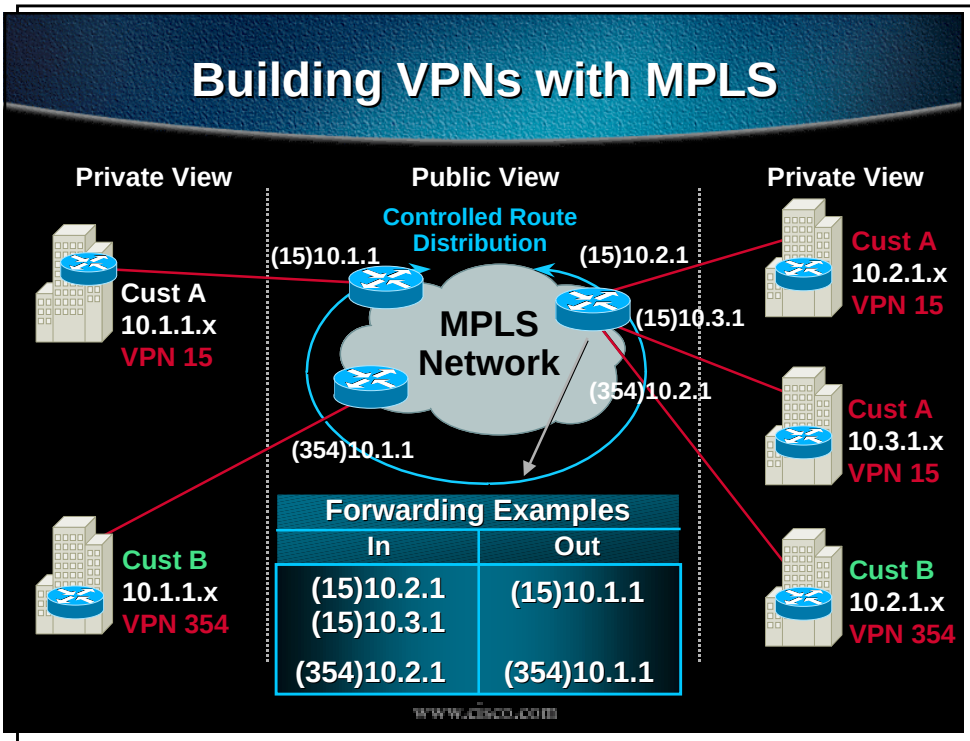
www.cisco.com

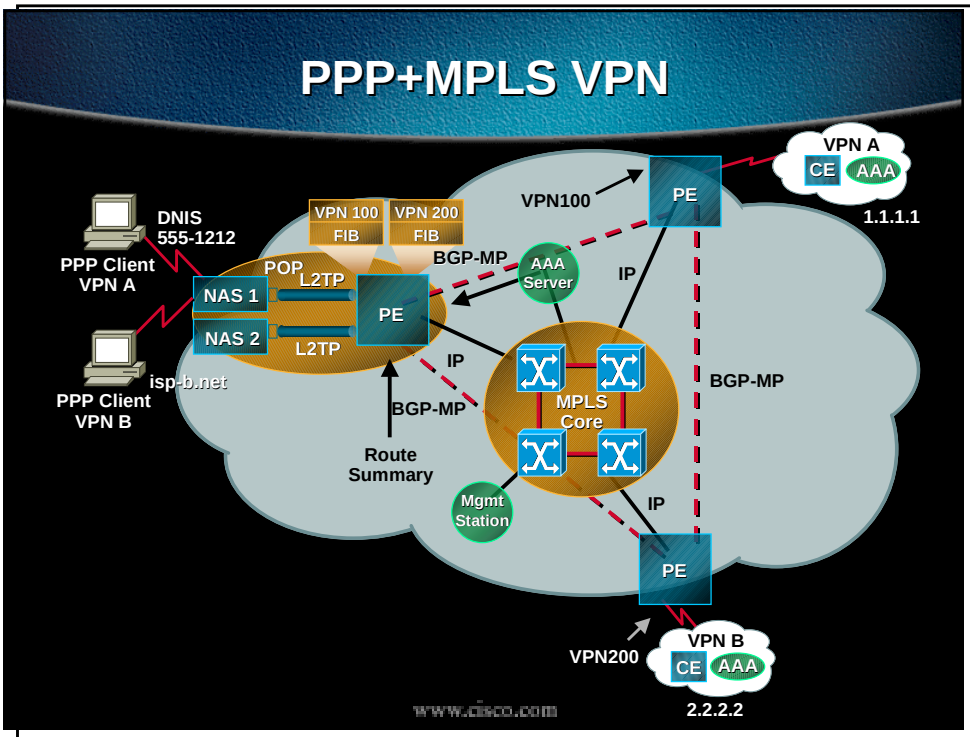
Cisco MPLS VPN Architecture

- Scalable VPNs
- Standards-based
- IP QoS and traffic engineering
- WAN B/W optimization
- No VC provisioning required



www.cisco.com





PPP/MPLS VPN Configuration—Define VPDN and VRFs

```
vpdn enable
vpdn-group 1
 accept dialin l2tp virtual-template 1 remote nas-cisco
 local name pe1
vpdn-group 2
 accept dialin l2tp virtual-template 2 remote nas-stanford
 local name pe1
!
ip vrf CISCO
 rd 100:1
 route-target both 100:1
!
ip vrf STANFORD
 rd 100:2
 route-target both 100:2
```

www.cisco.com

PPP/MPLS VPN Configuration—Define Virtual Templates

```
interface virtual-template 1
 ip vrf forwarding CISCO
 ip address 10.100.0.1 255.255.255.0
 no ip directed-broadcast
 ppp authentication chap
 peer default ip address pool CISCO
!
interface virtual-template 2
 ip vrf forwarding STANFORD
 ip address 10.200.0.1 255.255.255.0
 no ip directed-broadcast
 ppp authentication chap
 peer default ip address pool STANFORD
```

www.cisco.com

PPP/MPLS VPN—Define Pools and Configure Routing

```
ip local pool CISCO 10.100.0.2 10.100.0.254
ip local pool STANFORD 10.200.0.2 10.200.0.254
!
router bgp 1
 address-family ipv4 vrf CISCO
  network 10.100.0.0 mask 255.255.255.0
  aggregate 10.100.0.0 255.255.255.0 summary
  redistribute connected
  exit-address-family
 address-family ipv4 vrf STANFORD
  network 10.200.0.0 mask 255.255.255.0
  aggregate 10.200.0.0 255.255.255.0 summary
  redistribute connected
  exit-address-family
```

www.cisco.com

PPP/MPLS VPN—Configure Interfaces

```
Interface FastEthernet 1.1
! this is a VLAN interface, but it doesn't have to be
 ip vrf forwarding CISCO
 ip address 10.100.10.1 255.255.255.0

Interface FastEthernet 1.2
 ip vrf forwarding STANFORD
 ip address 10.200.10.1 255.255.255.0

! Optional static routes

ip vrf CISCO route 0.0.0.0 0.0.0.0 FastEthernet 1.1
ip vrf STANFORD route 0.0.0.0 0.0.0.0 FastEthernet 1.2
```

www.cisco.com

PPP/MPLS VPN—Other Configuration Considerations

- Use Proxy RADIUS in first release
- Much work is being done in this area

Next Generation MPLS VPN Solutions Summary

Pro	• Offers Optimal Use of the Backbone • Offers New Managed Service Opportunities, Bundled VPN Services (Dedicated and Access) • Offers Traffic Engineering • No Client Software to Manage
Con	• Requires an Upgrade of the Backbone Network

Resources

- VPN Services (Enterprise): http://www.cisco.com/warp/public/779/largeent/learn/technologies/VPNs.html
- VPN Services (Service Provider): http://www.cisco.com/warp/public/779/servpro/solutions/vpn/about.htm
- VPN Solutions for Service Providers: http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/index.shtml
- MPLS VPNs: http://www.cisco.com/warp/public/784/packet/apr99/6.html