Introduction to
Virtual Private Networks

Session 305

Cisco Systems

Agenda

- **Scope of this Session**

- **Intro and History of VPNs**

- **VPN Technology Building Blocks**

- **Basic VPN Architectures**

- **Next Generation VPN Solutions**

www.cisco.com

Scope of this Session

- **Provide a basic understanding of the component technologies relevant to VPNs**

- **Show how these technologies fit together to provide today's VPN solutions**

- **Speculate on some of the VPN advances that may come along in the near future**

- **For further info attend Phil Harris' Level 2 Deploying VPN Solutions (Session 313)**

www.cisco.com

What Is a VPN Service ?

A "VPN service" is a service which offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. Because the infrastructure is "shared", connectivity can be provided at lower cost than existing dedicated private networks
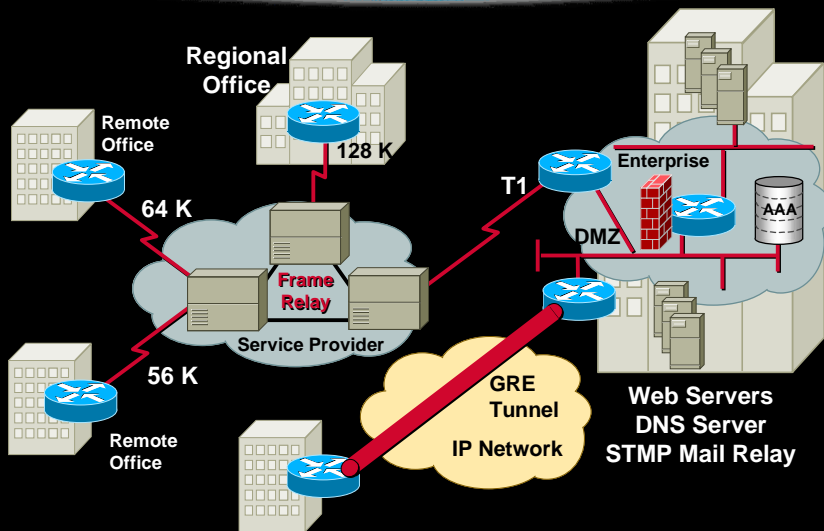
www.cisco.com
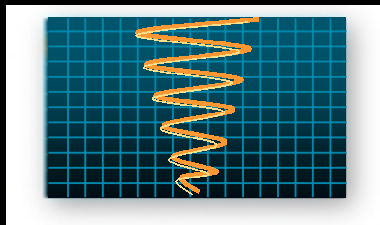
A VPN Analogy!

www.cisco.com

Traditional VPNs

What's Driving VPN Offerings

Reduced Networking Costs
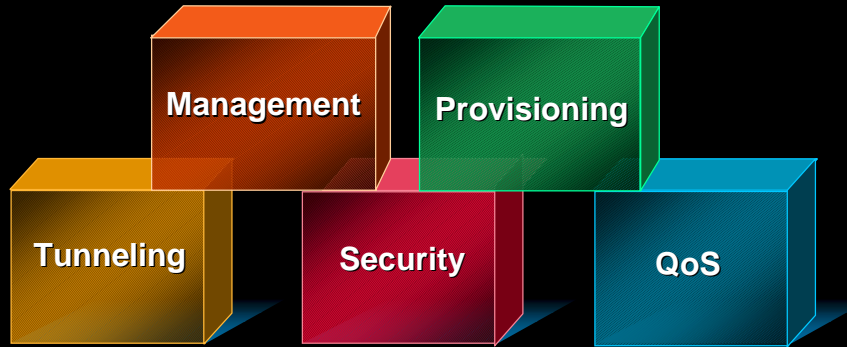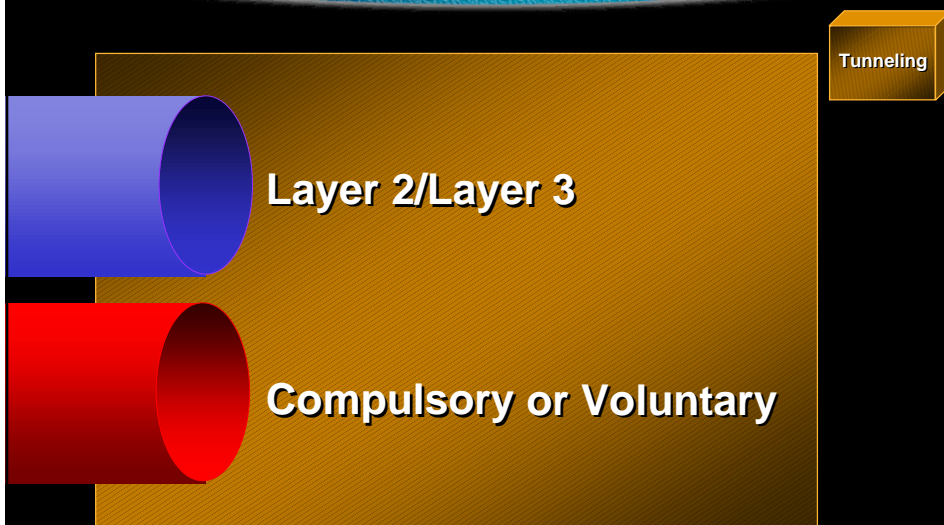
Increased Network Flexibility

VPN Building Blocks

Management

Provisioning

Tunneling

Security

QoS

www.cisco.com

Tunneling Types

Tunneling

Layer 2/Layer 3

Compulsory or Voluntary

www.cisco.com

Layer 2 vs. Layer 3

Tunneling

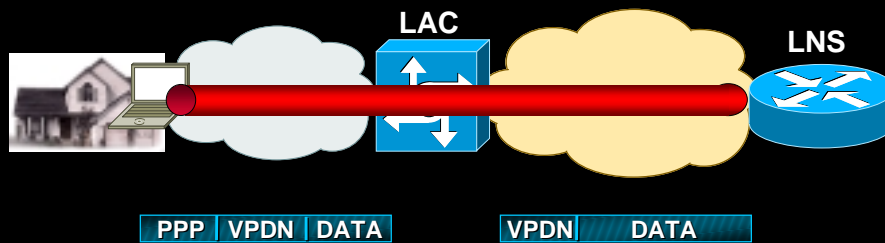| Tunneling Comparison	
Layer 3	IP Centric Less Integrated Solutions Solutions Still in Definition Stage
Layer 2	Center on PPP Multiprotocol Integrated With Existing Access Technologies

www.cisco.com

Generic Route Encapsulation (GRE)

IP Network

GRE Tunnel

IP	GRE	Network Packet
Transport Protocol	**Carrier Protocol**	**Passenger Protocol**
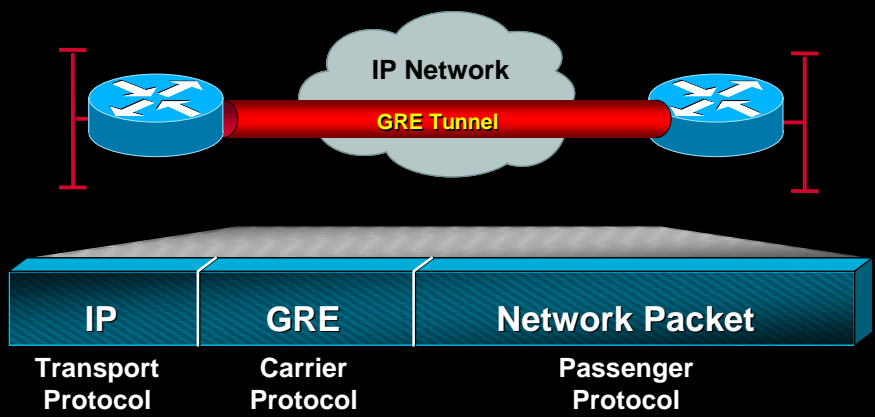
www.cisco.com

Compulsory Tunnel Model

LAC		LNS

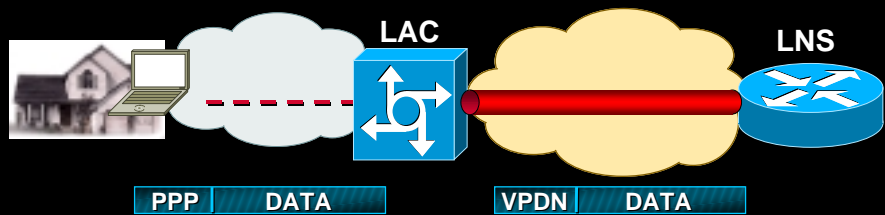| PPP	VPDN	DATA		VPDN	DATA

- **Client software wraps data in tunneling protocol then in transport protocol**
- **Transparent to LAC**

www.cisco.com

Voluntary Tunnel Model

LAC		LNS

PPP	DATA		VPDN	DATA

- **Generic PPP encapsulated data from any standard client**

www.cisco.com

PPP Tunneling

Tunneling

L2TP

PPTP

PPPoE

www.cisco.com

L2TP

Tunneling

LAC

LNS

- **L2TP is an IETF draft moving towards standards status**
- **Mostly used in voluntary mode**
- **Some third party clients available**
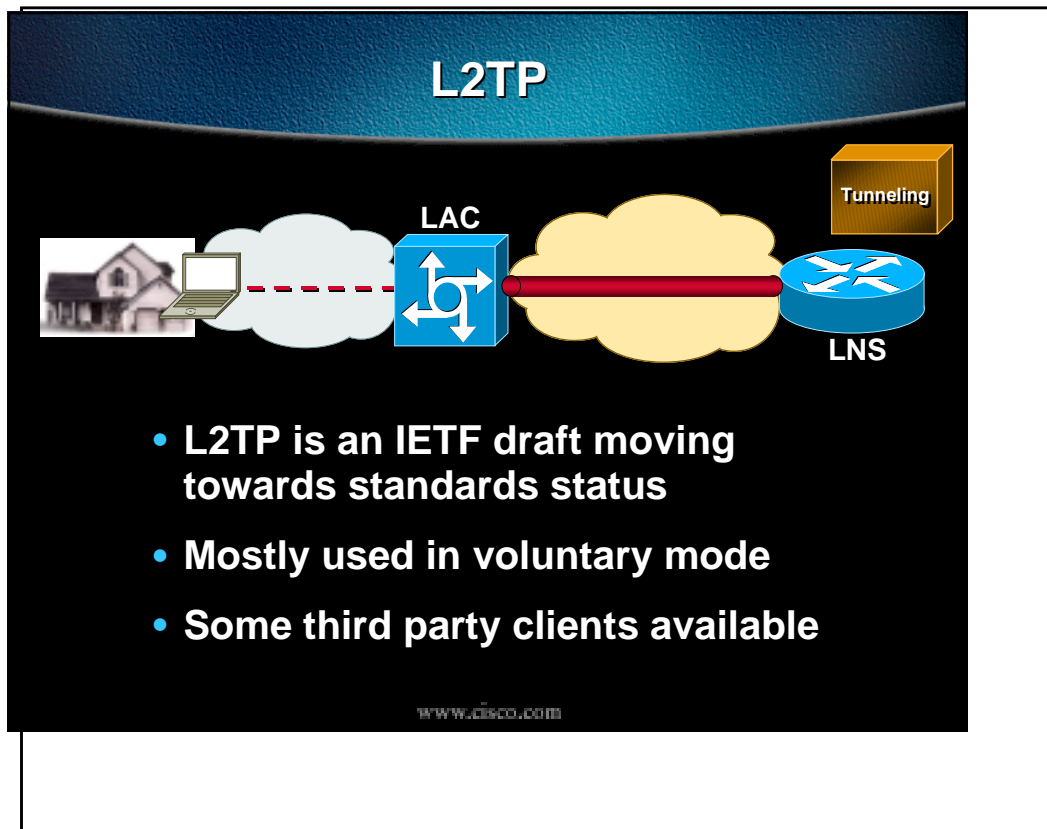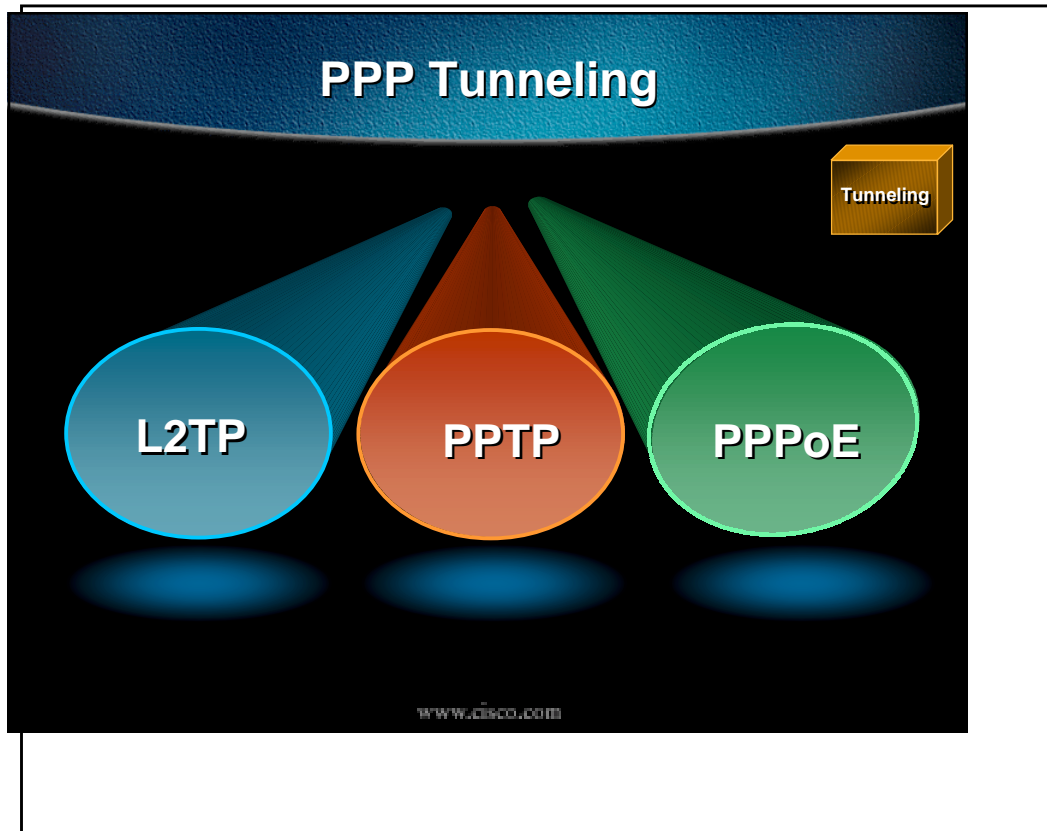
www.cisco.com

Microsoft Point-to-Point Tunneling Protocol

LAC

Tunneling

LNS
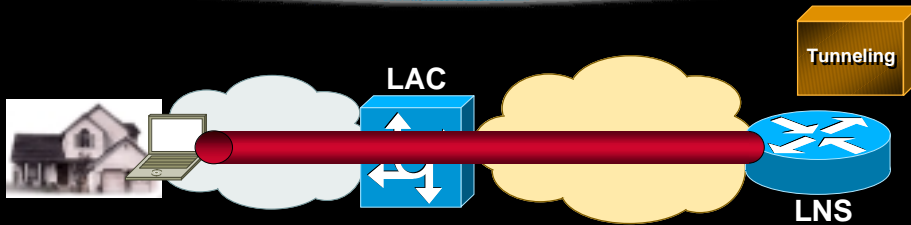
- **An informational RFC**

- **Primarily used in compulsory mode**

- **Widely available clients**

  Win95, Win98, NT, Third parties

www.cisco.com

PPP over Ethernet

Hosts Run PPPoE Client SW

Runs RFC 1483 Bridge Mode

Tunneling

ATM PVC

LAC

Corporate

DSLAM

Host 1

CPE

VI

PPP Tunneling Routing, etc.

VI

Host 2

DSL

ISP

PPP over Ethernet

Key Benefits

- **Preservation of Dial Model—PPP session-based communication**
- **Leverages existing Ethernet based infrastructure**
- **Allows multiple PPP sessions to be initiated within home LAN**
- **Enables destination selection**
- **DSL Modem Independent (must run RFC 1483 Bridging)**

- **Informational RFC**

- **Primarily used in xDSL environments**

www.cisco.com

VPN Security

- **IPSec**
- **MPPE**

www.cisco.com

IPSec Transport Mode

IP Network

IPSec Transport Mode

Router LEFT   **Router RIGHT**

IP HDR	Data

IP HDR	IPSec HDR	Data

← **May Be Encrypted** →

www.cisco.com

IPSec Tunnel Mode

Security

SP 1

IPSec Tunnel Mode

SP 2

Router LEFT

Router RIGHT

IP HDR	Data

New IP HDR	IPSec HDR	IP HDR	Data

← **May Be Encrypted** →

www.cisco.com

IPSec VPN Client Operation

Security

Remote User
w/IPSec Client

Public Network

Home Gateway
Router

Home
Network

Secure Tunnel Established

Certificate
Authority/
AAA

**Dial Access to Corporate Network
Exchange X.509 or One-Time Password**

**IKE
Negotiation**

Authentication Approved

Encrypted Data flows

www.cisco.com

Microsoft Point-to-Point Encryption

Security

PPTP Tunnel

LNS
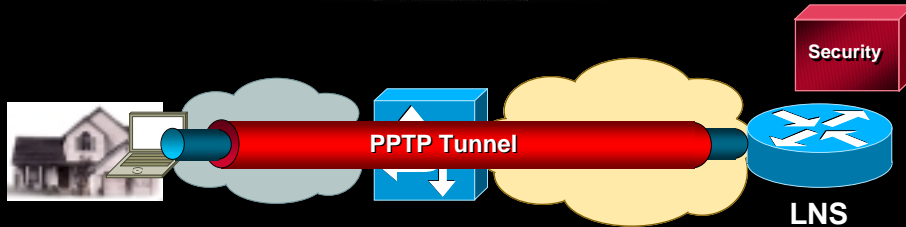
- **RC4 encryption of PPP packets**

- **Used almost exclusively with PPTP**
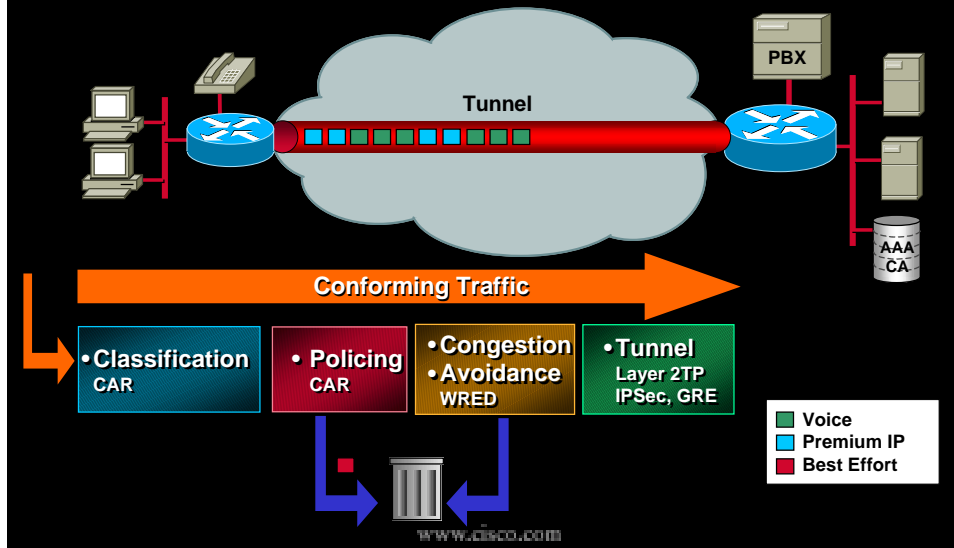
- **Informational RFC 2118**

www.cisco.com

VPNs and Quality of Service

- **Optimize use of the WAN link**

- **Guarantee bandwidth for mission critical applications**

- **Take advantage of differentiated services offered by the ISP**

www.cisco.com

VPNs and Quality of Service

Tunnel

PBX

AAA CA

Conforming Traffic

- Classification
  CAR
- Policing
  CAR
- Congestion
- Avoidance
  WRED
- Tunnel
  Layer 2TP
  IPSec, GRE

Voice
Premium IP
Best Effort

www.cisco.com

Management and Provisioning

- **Generic configuration**
- **AAA**
- **Policy management**
- **Certificate authorities**

www.cisco.com

Architectures

So, How Does It All Go Together?
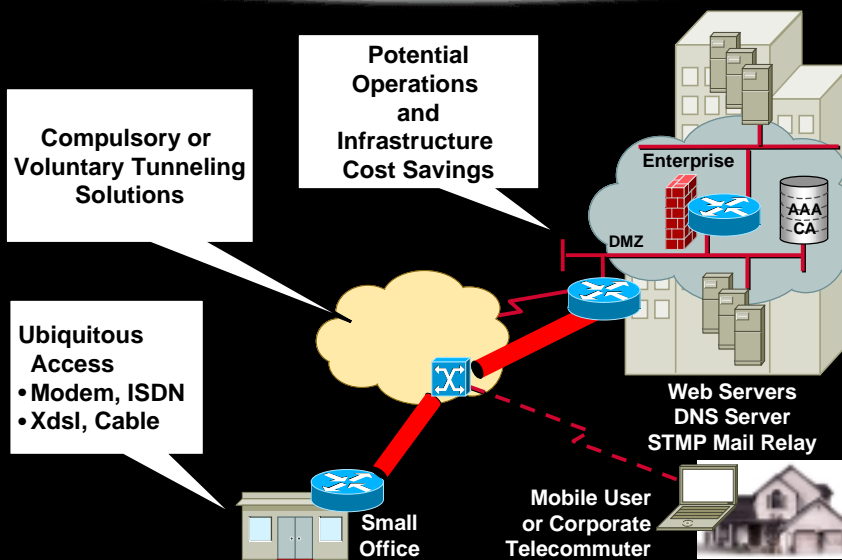
www.cisco.com

VPN Architectures

Intranet VPN

Extranet VPN

Cisco IOS®
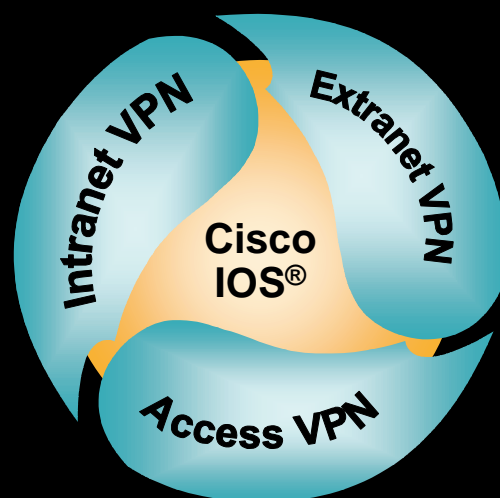
Access VPN

www.cisco.com

VPN Architectures and Applications

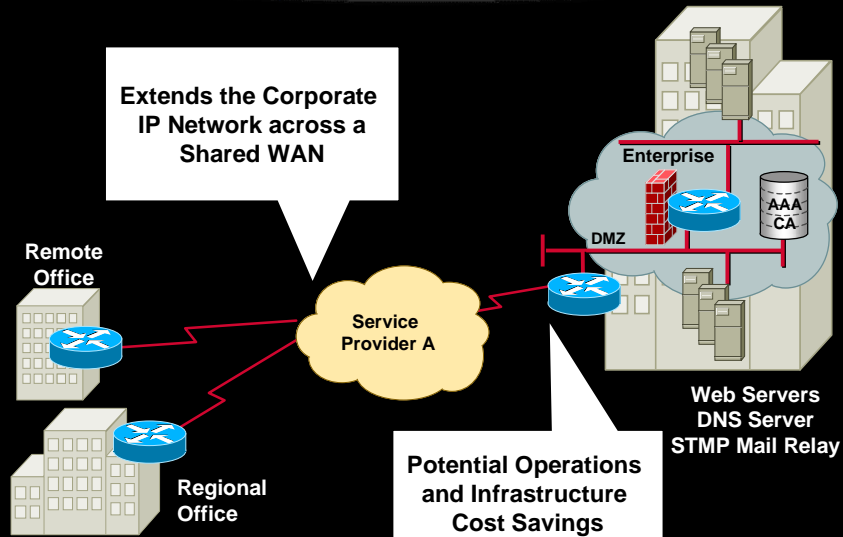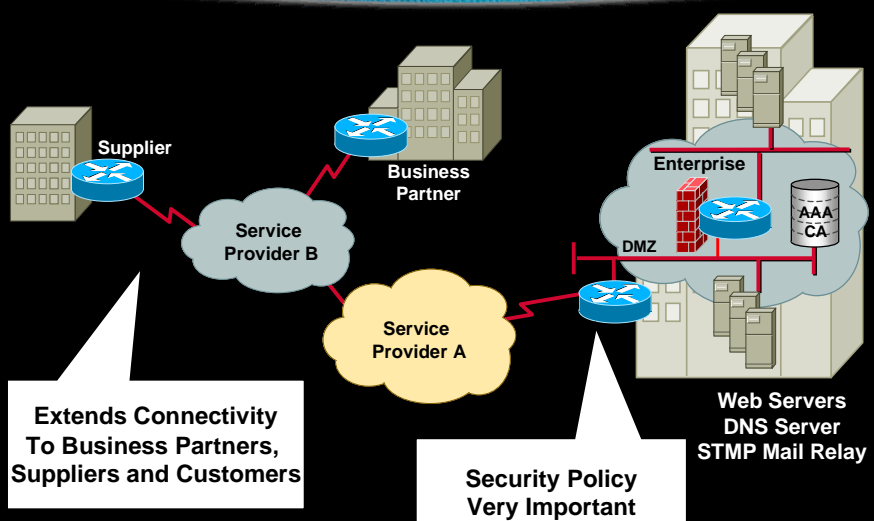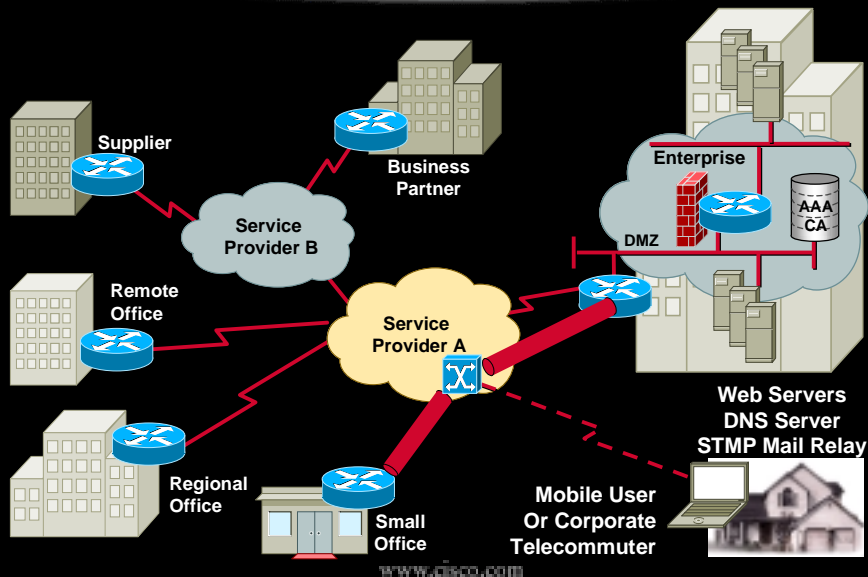| Type	Application	Alternative To	Benefits
Access VPN	Remote Connectivity	Dedicated Dial ISDN	Ubiquitous Access Lower Cost
Intranet VPN	Internal Corporate Connectivity	Leased Lines	Extend Connectivity Lower Cost
Extranet VPN	Business-to Business External Connectivity	Fax, Mail, EDI	Facilitates E-Commerce

www.cisco.com

Access VPNs

Compulsory or Voluntary Tunneling Solutions

Potential Operations and Infrastructure Cost Savings

Enterprise

AAA CA

DMZ

Ubiquitous Access
• Modem, ISDN
• Xdsl, Cable

Web Servers
DNS Server
STMP Mail Relay

Small Office

Mobile User or Corporate Telecommuter

www.cisco.com

The Intranet VPN

Extends the Corporate IP Network across a Shared WAN

Remote Office

Service Provider A

Enterprise

DMZ

AAA CA

Web Servers
DNS Server
STMP Mail Relay

Regional Office

Potential Operations and Infrastructure Cost Savings

www.cisco.com

The Extranet VPN

Supplier

Business Partner

Service Provider B

Enterprise

DMZ

AAA CA

Service Provider A

Web Servers
DNS Server
STMP Mail Relay

Extends Connectivity To Business Partners, Suppliers and Customers

Security Policy Very Important

www.cisco.com

The Complete VPN

Deployment Alternatives

Service Provider Focused	Collaborative	Enterprise Focused
Service Provider Supplies Majority of VPN Solution Equipment Service Training Help Desk	**Service Provider** Supplies Hardware Qos to Bandwidth Offering	**Service Provider** Supplies Basic Network Access
Enterprise Manages Security Services	**Enterprise** Application and Configuration Management Help Desk Support	**Enterprise** Supplies VPN Equipment Manages Network

www.cisco.com
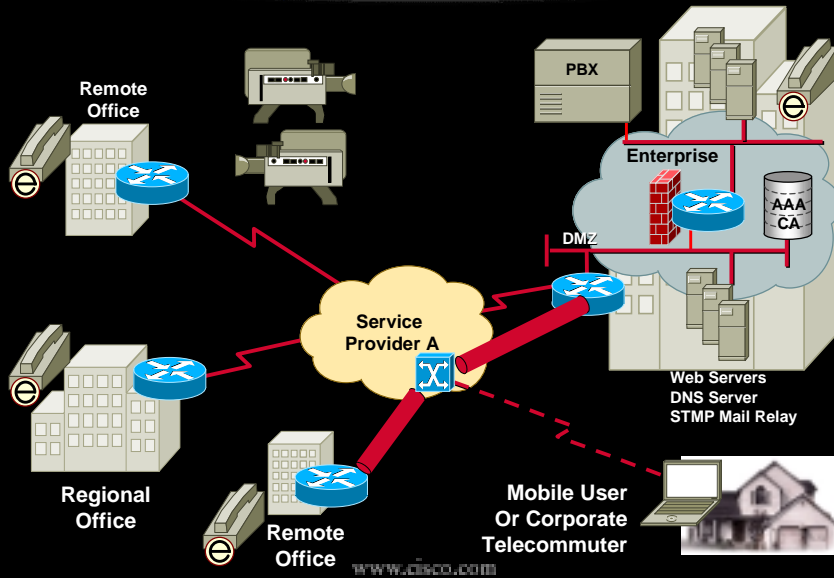
Next Generation VPNs
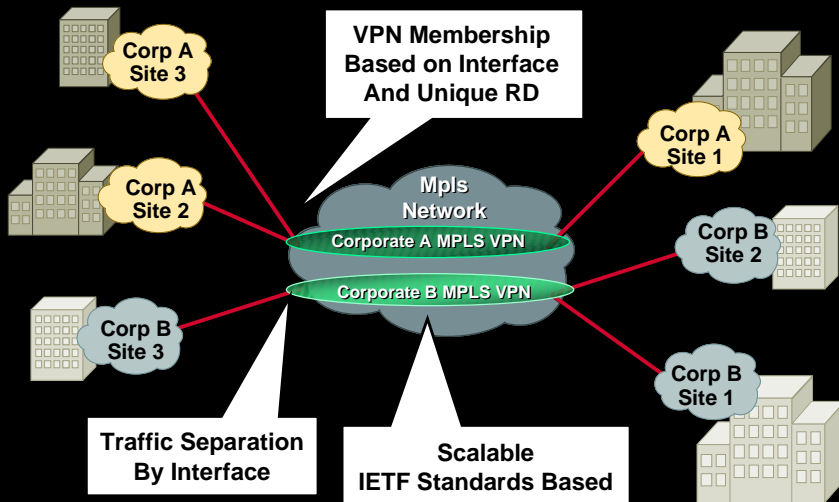
- **Multiservice VPNs**
- **MPLS VPNs**

"Next generation
networks must allow
the corporation to
thrive on change…"
The Burton Group
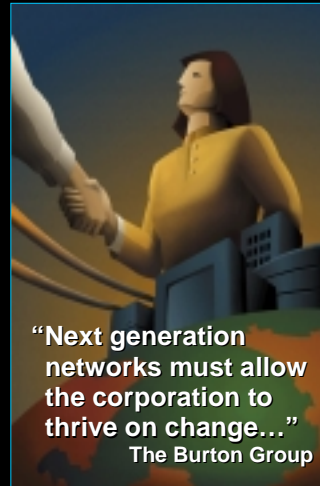
WWW.cisco.com

Multiservice VPNs

Tokyo

London

Internet

**Live
Audio/Video
Feed**

**Stored
Video**

Brazil

Australia

Multiservice VPNs

MPLS VPNs

Summary

QoS Security Mgmt.

Core

Platforms

Services

Scalability

Standards Based

Future Flexibility
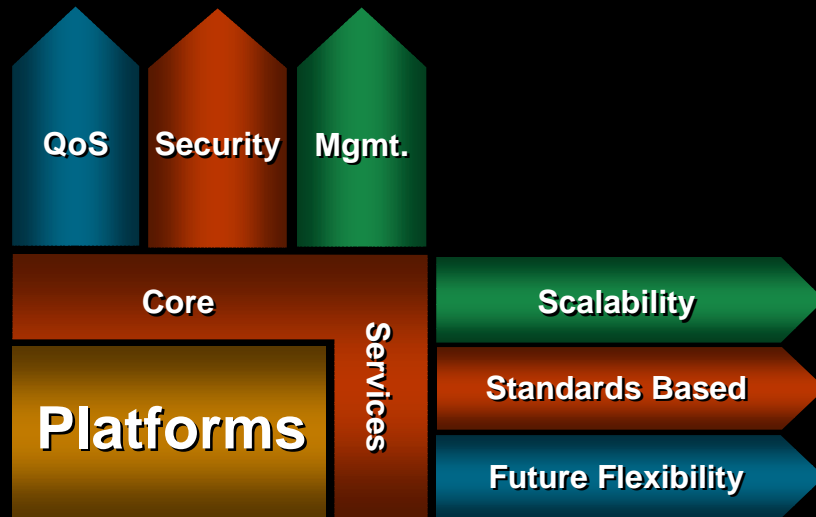
www.cisco.com

Other Useful Information

	Location
Cisco VPN Solutions	http://www.cisco.com/warp/public/779/largeent/learn/technologies/vpn/ http://www.cisco.com/warp/public/779/servpro/solutions/vpn/
L2TP	http://search.ietf.org/internet-drafts/draft-ietf-pppext-l2tp-15.txt
IPSec	http://www.cisco.com/warp/public/cc/cisco/mkt/security/encryp/tech/ipsec_wp.htm
PPTP	http://search.ietf.org/internet-drafts/draft-ietf-pppext-pptp-10.txt
MPPE	http://search.ietf.org/internet-drafts/draft-ietf-pppext-mppe-03.txt

www.cisco.com

Q&A

Thank You

Please Complete Your
Evaluation Form

Session 305