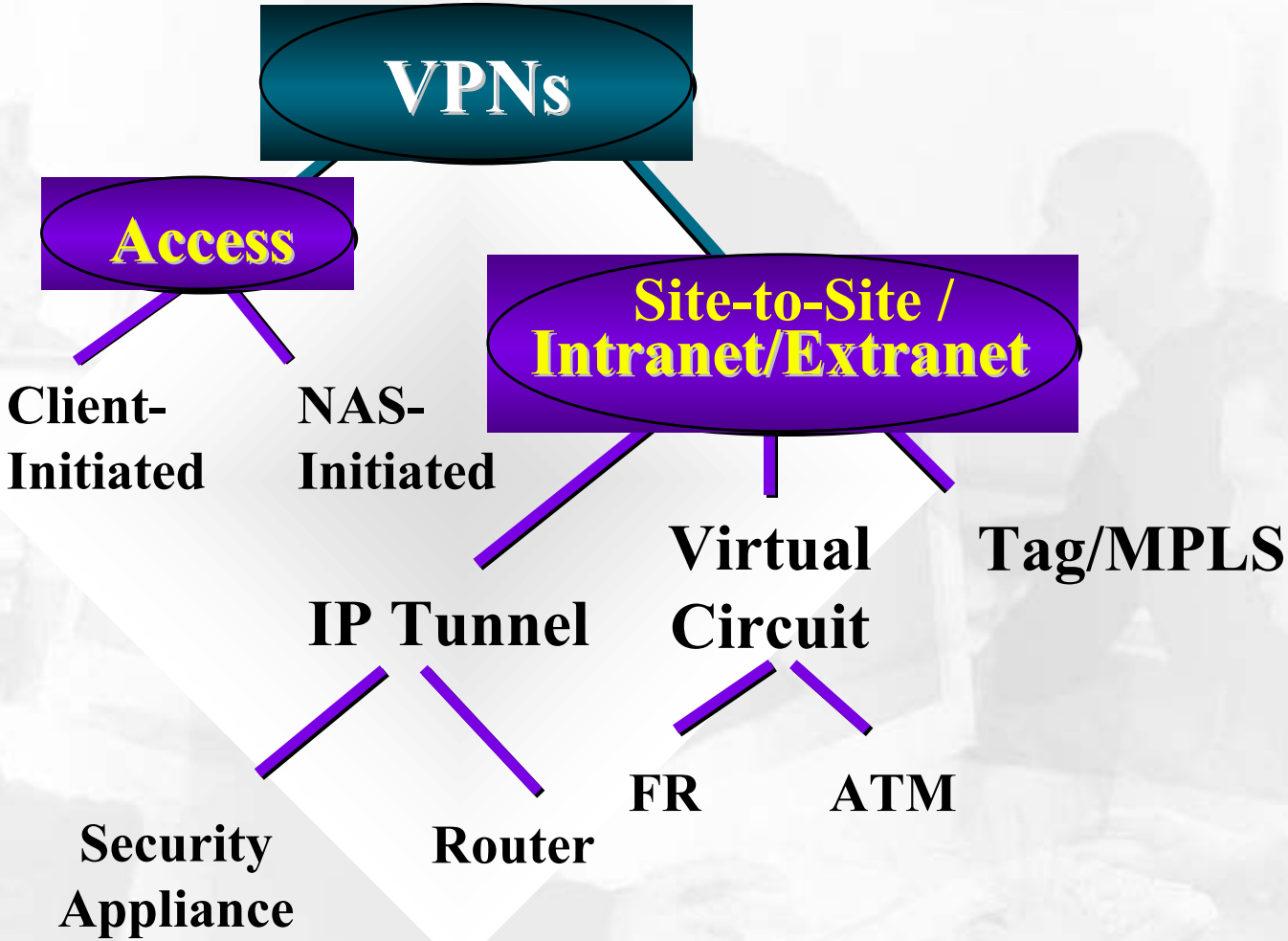
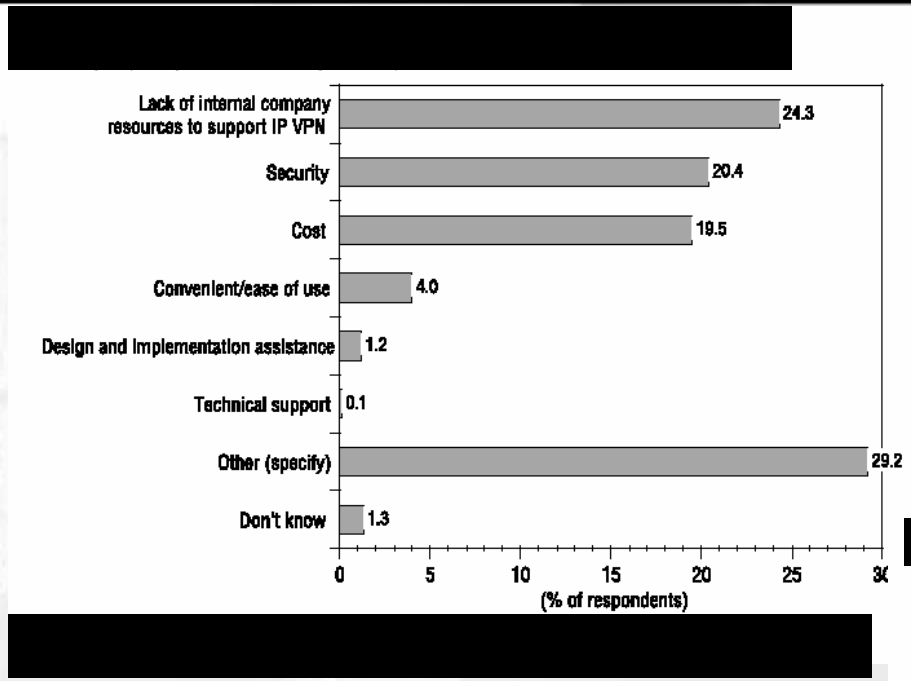
Carrier Based IP-VPN Implementations

Michael Tighe
Director Advanced Data Services
Verizon Enterprise Solutions Group
April 24th 2004

VPN Taxonomy

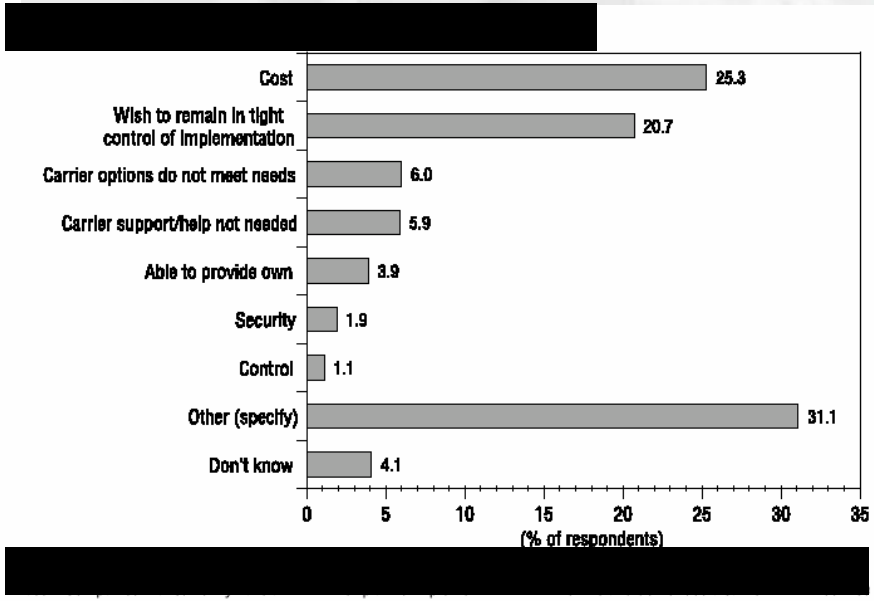


Why Do Enterprises Select a Managed VPN Service?



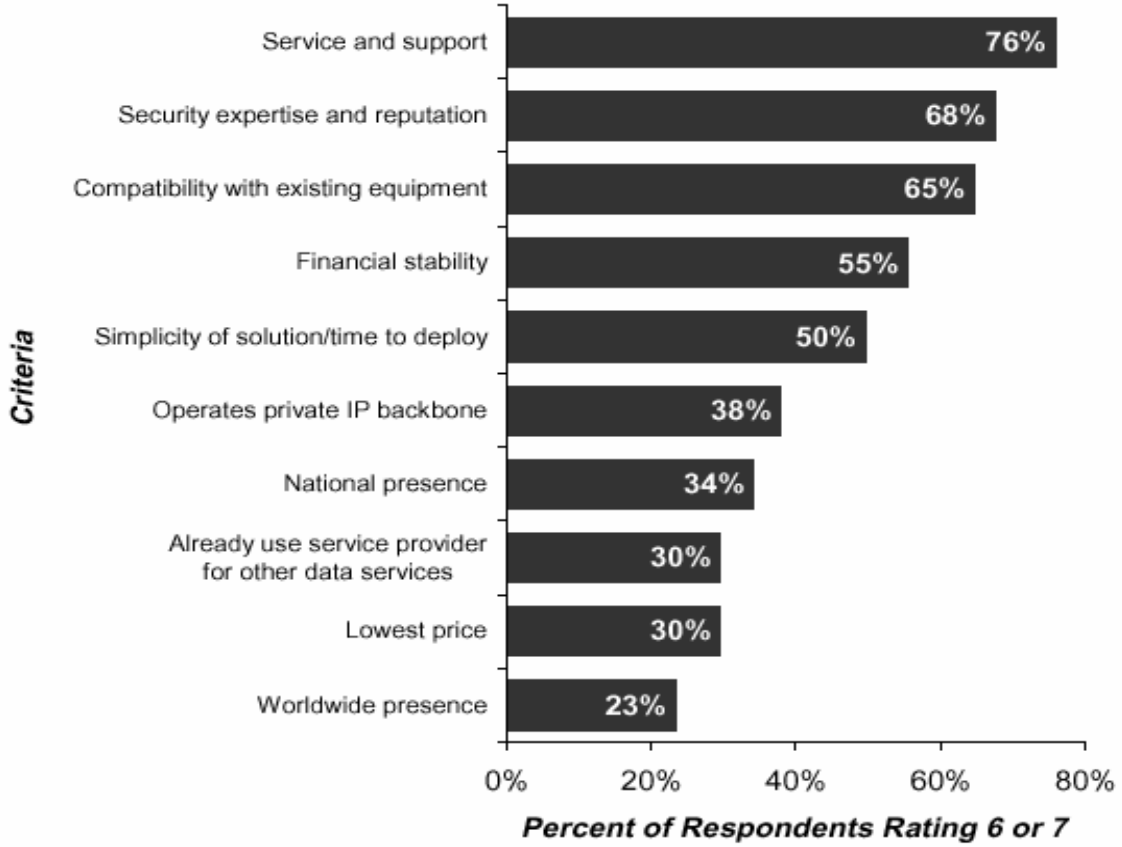
Drivers for Outsourced VPN Services

Inhibitors to Outsourced VPN Services



Source: IDC, 2001

Service Provider Selection Criteria



Source: Infonetics, 2001

Evolving Enterprise Network Requirements

- Proven Network Architecture that is highly available, secure and reliable
- Highly scalable network architecture to support ever increasing bandwidth requirements.
- Support a distributed applications environment
- Ability to support legacy and advanced IP-Based Applications such as VOIP, IP Conferencing, Streaming Video.
- Ability to securely extend Extranet Applications to Business Partners
- Provide high quality access to road warriors, teleworkers, and small branch offices.
- Converge voice, video and data networks into one coherent architecture
- Reduce the cost of deploying and managing network

Carrier Based IP-VPN Offerings

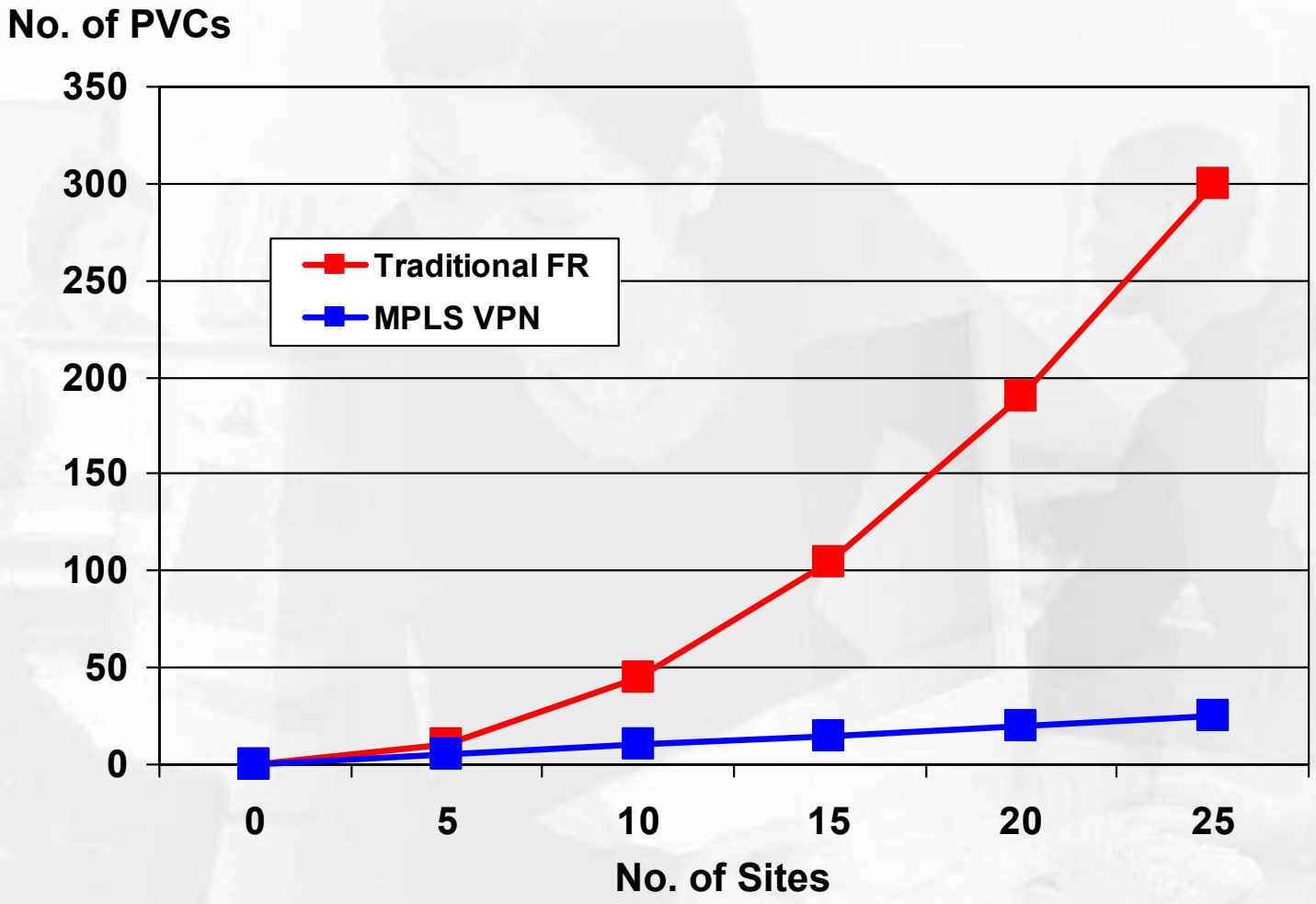
Service	Targetted Users	Architecture	Technologies
Access VPN's	Mobile Workers	Client Initiated or network access server initiated	CPE & Network Based IP-Sec, Point to Point tunneling Protocol, SSL, dial ISDN, DSL or Cable
Site to Site VPN	Branch offices requiring data connectively to a data center(s)	IP-Tunnel, Virtual Circuit	Frame Relay, ATM & CPE Based IP-SEC or SSL Offerings
Multiservice VPN's	Multisite businesses with requirements for converged data, voice and video	Framework for a converged packet based VPN service that supports voice, data and video	Network Based MPLS IP-VPN

Service Providers have developed a portfolio of VPN services targeted at different user requirements.

Limitations of Existing Carrier Fast Packet Offerings

- **As Enterprise IT Requirements have evolved Carrier based Frame Relay and ATM are increasingly not meeting customer's IT requirements:**
  - Connection Orientation of Layer Two IP-VPN's does not scale to support multiple data center environments or multicast applications.
  - No support for QOS limits ability to deploy advanced applications.
  - Not cost effective to provide teleworker or small office support
  - Poor integration with Internet limits support for Extranet Services and teleworkers with DSL and Cable Modems
  - Service availability limitations

MPLS IP-VPN
Operational Simplicity



- Full mesh connectivity based on single-priority PVCs

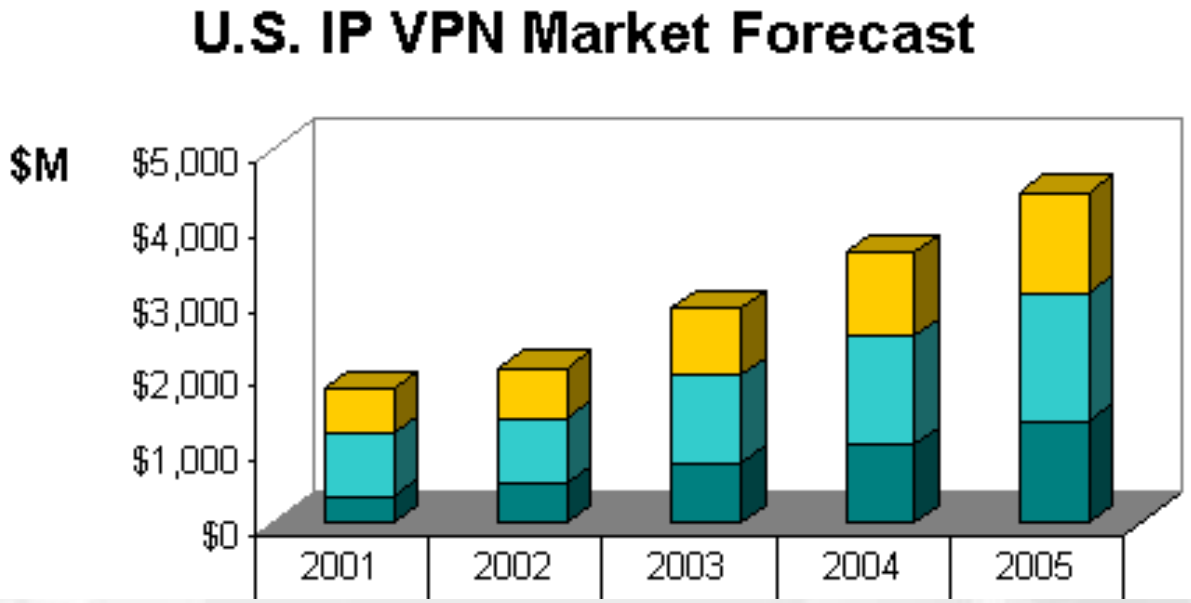
Source : AT&T

MPLS Advantages

Advantages of MPLS-enabled IP over non-MPLS IP Networks

- Greatly enhanced scalability
  - Per customer tunnel mesh is not required
- Enhanced operational cost effectiveness
  - Enhanced forwarding and path selection allows more efficient bandwidth use
- Better IP service performance
  - Traffic engineering based on service type
  - Dynamic QoS and service based loading balancing

MPLS and Network-Based IPSec VPN Managed Services Expected to Grow



	2001	2002	2003	2004	2005	2006	CAGR	Source
United States								
Carrier Site-to-Site IP VPN ($M)	$1,181	$1,393	$1,986	$2,504	$3,077	$3,706	25.7%	IDC
MPLS Network-Based	30.0%	37.0%	40.0%	41.7%	44.0%	46.0%	8.9%	Ovum
IP Sec CPE-Based	70.0%	60.6%	50.1%	39.4%	33.2%	27.2%	-17.2%	Ovum
IP Sec Network-Based	0.1%	2.4%	9.9%	18.9%	22.8%	26.8%	205.9%	Ovum
Carrier Remote Access IP VPN ($M)	$597	$681	$896	$1,106	$1,339	$1,607	21.9%	IDC

Source: IDC, Ovum, 2002

US Carriers are embracing MPLS IP-VPN technology

- AT&T's strategy for its IP services can be summed up in an acronym MPLS. "Network World 01/12/2004"
- MCI is expanding the geographic reach of it's MPLS network to 48 countries. "Network World 02/16/2004"
- SBC goes nationwide with VPN service. The carrier's PremierServ VPN uses MPLS services. "Network World 02/29/2004"
- BellSouth Energizes Network Services with MPLS Technology "MPLS World"
- Verizon Plugs in New National Broadband Network. The IP Backbone uses a technology called MPLS. "Network World April 14th,2004"

MPLS VPN's better support Enterprise customer's evolving IT Requirements

Carrier MPLS VPN Offerings

Carriet	Service
AT&T	IP Enabled Frame Relay
	IP Enabled ATM
	Enhanced IP-VPN
MCI	Private IP Services
Sprint	Sprintlink Frame Relay and VLAN
	IP Intelligent Frame Relay
SBC	SBC PremierSERV IP-VPN
Qwest	IP Enabled Frame Relay
Verizon	IP-VPN Services
BellSouth	BellSouth Regional IP Backbone (BRIB)

As a first step towards a converged network architecture carriers are IP Enabling existing frame relay and ATM offers.

Source: ESG Market Intelligence, CCMI and Verizon Regulatory

AT&T Private IP VPN
Classes of Service

Real-time	**For voice over IP and video conferencing**
High Priority	**For mission-critical data applications, such as ERP**
Medium Priority	**Can be used for company email and HR websites**
Low priority	**Can be used for Internet browsing**

AT&T's private IP VPN offer is based on its IP-Enabled Frame Relay (IPFR) service that uses Multiprotocol Label Switching technology to implement a VPN on customers' existing frame relay networks. AT&T Managed Router Service for IPFR also supports these classes of service.

Verizon IP-VPN Class of Service

- **QoS mechanisms will be utilized to provide end users with four distinct classes of service on their Verizon IP-VPN solution. Layer 2 and layer 3 QoS systems may be used to deliver end-to-end IP services. The following four IP-VPN classes of service will be supported on an end-to-end basis:**
  - Priority Voice Traffic
    - Voice traffic requiring < 150 ms of end-to-end delay and a maximum of 30 ms of jitter
    - Considered to be steady stream traffic, e.g., high-quality real-time packet video
  - Real-Time Traffic
    - Considered to be “urgent” real-time bursty traffic, e.g., compressed video, real time imaging and IBM SNA traffic
    - IP video traffic to be discarded during network congestion only after Best Effort and Priority Data are are discarded
  - Priority Data Traffic
    - IP data traffic to be discarded during network congestion only after all Best Effort traffic has been discarded
    - Considered “normal” bursty traffic with moderate tolerance for delay with low packet loss.
  - Best Effort Traffic
    - Any type of IP traffic (voice, data, or video) deemed by end-users to be eligible for packet discard during periods of network congestion.
    - There are no performance guarantees associated with best effort traffic.

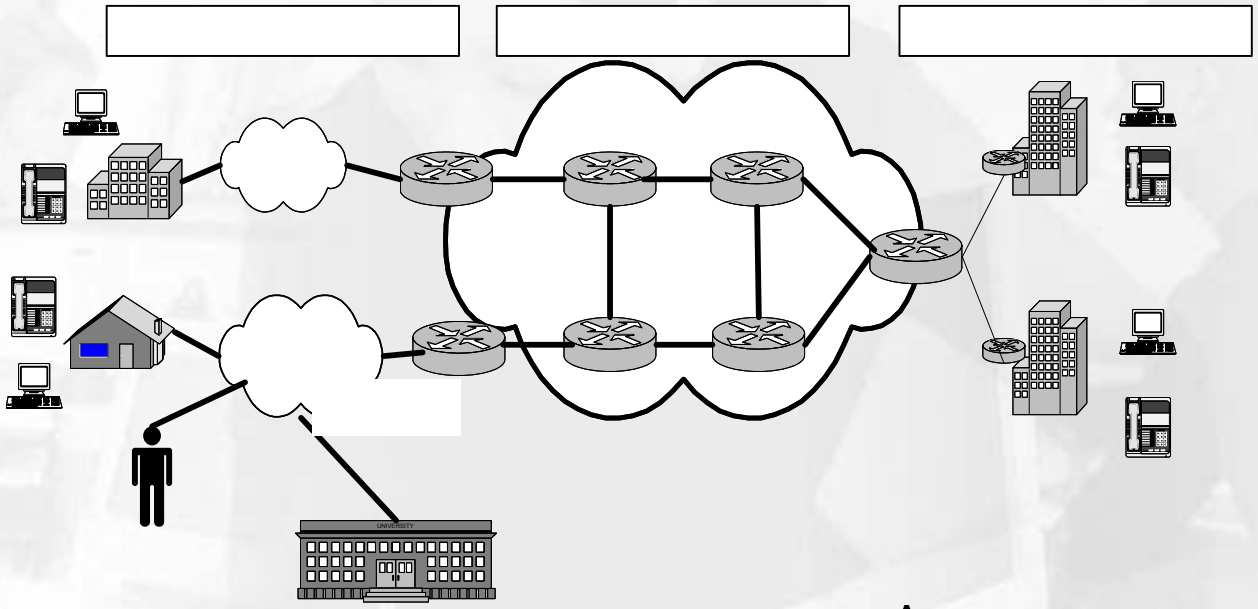
SAVVIS Class-of-Service VPN SLA

verizon

	Round-Trip Latency	Packet Loss
Level 1	50 milliseconds	0.1%
Level 2	60 milliseconds	0.25%
Level 3	70 milliseconds	0.5%
Level 4	75 milliseconds	1.0%

Source: SAVVIS, Yankee Group

Integrated IP-VPN Networks



To meet enterprise network requirements requires that carriers Integrate access, site-site, Fast Packet and MPLS VPN technologies Into one coherent architecture

VPN Managed Service Roadmap