VPNs: Reality Behind the Hype

Steven Taylor
President, Distributed Networking Associates
Editor/Publisher, Webtorials.Com
Fall/Winter - 2000

Copyright & Notices

Professional Opinions - All information presented and opinions expressed by Distributed Networking are the current opinions of Distributed Networking based on professional judgment and best available information at the time of presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the Customer.

Biographical Information - The seminar will be led by Steven Taylor, President of Distributed Networking Associates and Publisher/Editor in Chief of Webtorials.Com, a premier source of on-line telecommunications seminars and market research. An independent consultant, planner, author, and teacher since 1984, Mr. Taylor is frequently quoted in the trade press and is one of the industry's most published authors on high bandwidth networking techniques. Distributed Networking Associates may be contacted at 2707 Lake Forest Drive, Greensboro, NC 27408; (336) 288-3858. E-mail: taylor@webtorials.com.

eHandouts

- VPNs: Realities Behind the Hype
  - http://www.webtorials.com/main/eduweb/ipvpn/tutorial/vpnover/
- Gold Sponsor Product/Service Briefing by AT&T
  - http://www.webtorials.com/main/sponsors/att/
- Updates
  - Registered visitors who elect to receive updates via e-mail will be notified
- Hardcopy at end of session

VPNs: Reality Behind the Hype

- Technology Background
- VPN and Access Reference Architectures
- Application Models and Business Cases
- What to Look For in a VPN

What's a Virtual Private Network (VPN)?

- Hot marketing term
- Viewed as the newest panacea to all your networking woes
  - Infinite free bandwidth with no configuration needed
  - Often implies IP
    - Even "Internet" is sometimes implied

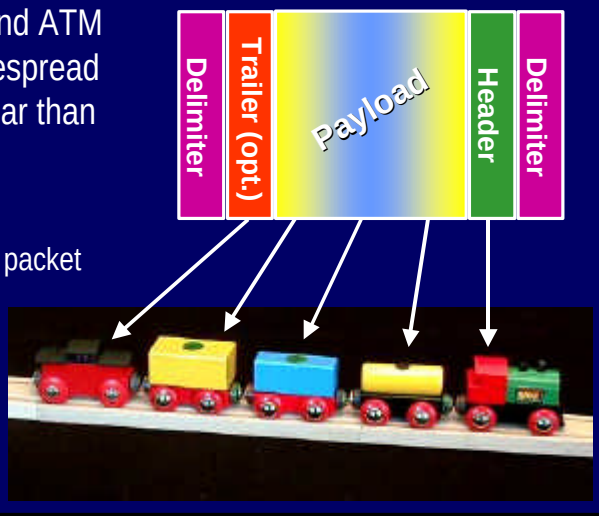
What's a Virtual Private Network (VPN)?

- Virtual network: A network that provides virtual circuits and that is established by using the facilities of a real network.*
- Has the look and feel of a "real" private network
- Enterprise maintains control of the network
  - Customer Network Management (CNM) is a key feature
- Usually will be based on packet switching

*Source: Federal Standard 1037C at http://glossary.its.bldrdoc.gov/fs-1037/

Broadband Packet Service Types

- Frame Relay, IP and ATM are becoming widespread and are more similar than different
- Key differences:
  - Fixed vs. variable packet length
  - Connection vs. connectionless

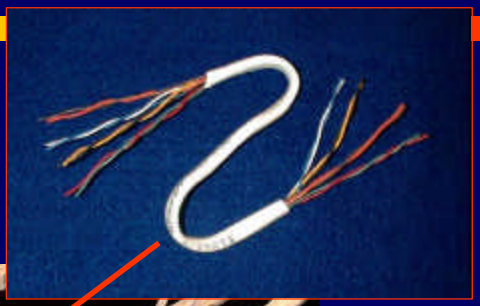


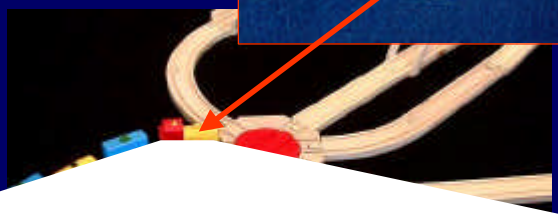
Generic Packet Format: Payload

- Variable: Frames
  - Efficient use of bandwidth
  - "Frame Relay" & IP
- Fixed length: Cells (ATM)
  - Easy to process with Predictable delay
  - ***Always*** the same size

Generic Packet Format: Header

- Connection oriented
  - Virtual Circuit number
  - Conserves address space
  - PVCs and SVCs

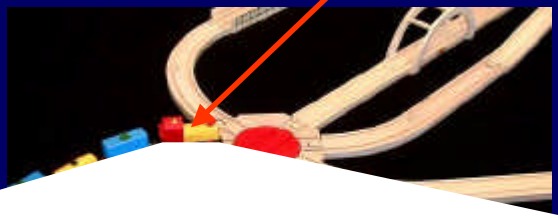




EA	DE	FECN	BECN	DLCI	EA	EA	DLCI

Generic Packet Format: Header

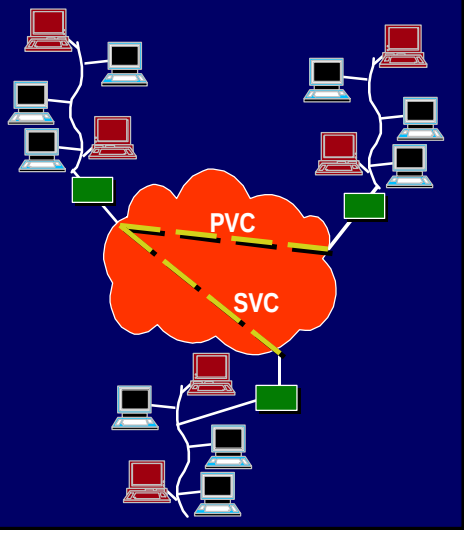
- Connectionless (IP)
  - "Universal," unique address
  - Needs large address space
    - Is this a problem?



Other header info	Source Address	Destination Address	Other header info

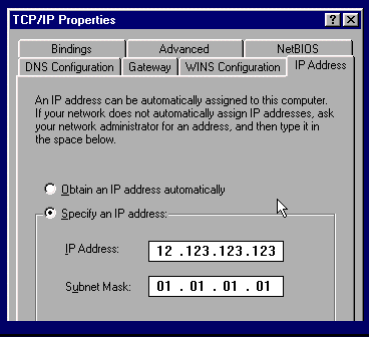
Address Spoofing: Who sets the address?

- ATM and Frame Relay
  - PVC / SVC addresses are set by network operations
  - SVC user controls connection, not address



Address Spoofing: Who sets the address?

- IP address is set by the user
  - Can be spoofed
  - Need for authentication



Broadband Packet Types

- Bottom Line: All three “work”

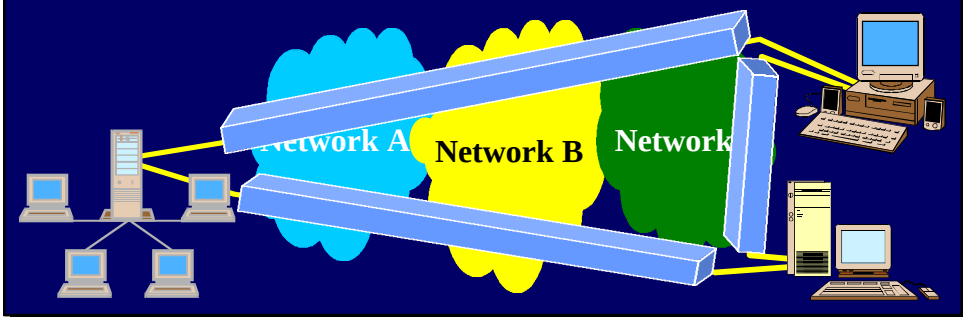
	Fixed Length	Variable Length
Connection	ATM	Frame Relay
Connectionless	(None)	IP

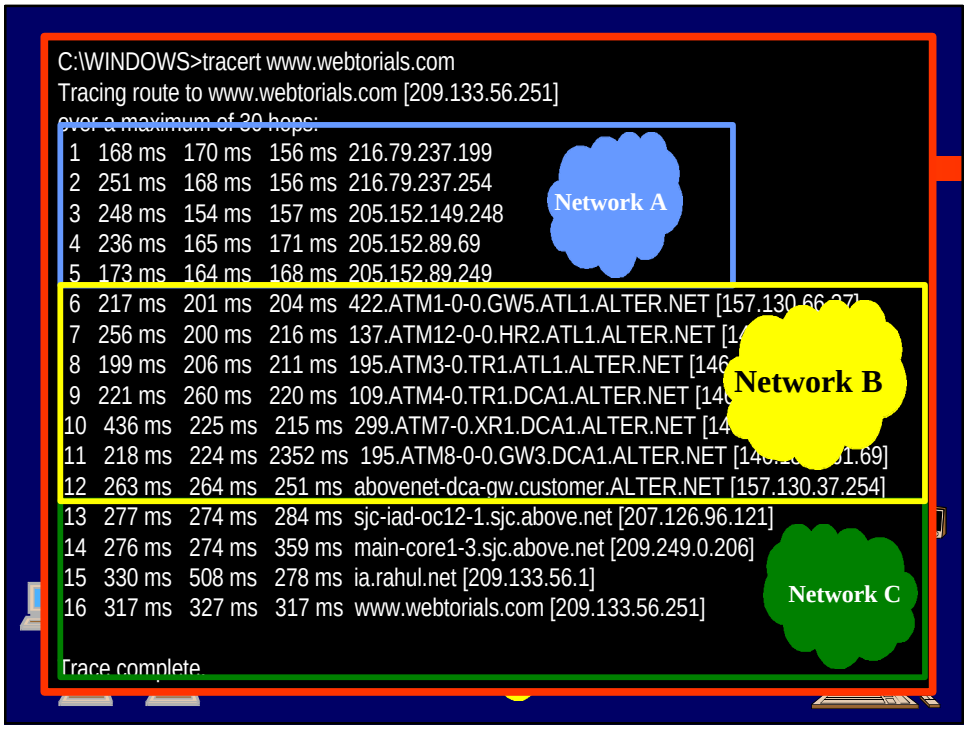
VPNs: Reality Behind the Hype

- Overview
- ➡ VPN and Access Reference Architectures

Internet Backbone VPN

- Uses the Internet for transport layer





Internet Backbone VPN

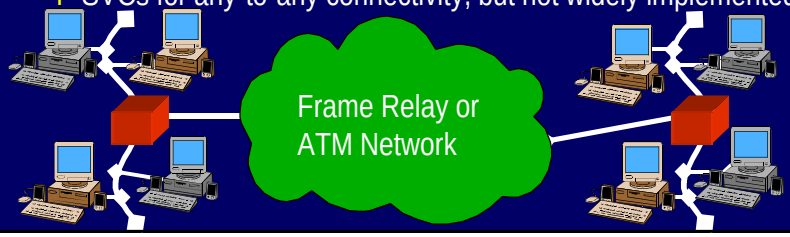
- Uses the Internet for transport layer
  - Tunneling - *For multiprotocol, private addressing, etc.*
  - Encryption - *For security across "unknown" connections*
  - Authentication - *To ensure the connection is to the "right" user*

Internet Backbone VPN Scorecard

VPN Type	Strengths	Weaknesses
Internet Backbone	Price	Lack of Control
	Ubiquity	No Guaranteed QoS
	Connectivity	Lack of Security
ATM & Frame Relay		
Enhanced IP		

ATM and Frame Relay

- Traditional Frame Relay or ATM service
  - Provides same basic functions as leased lines
    - At a fraction of the cost
  - PVCs provide continuous point-to-point connectivity
    - More than 95% of installed VCs are PVCs
    - SVCs for any-to-any connectivity, but not widely implemented

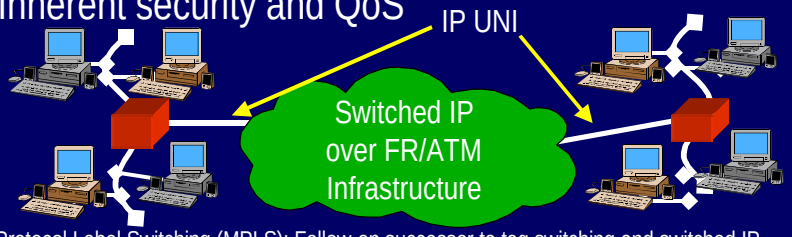


Leased Line Replacement VPN Scorecard

VPN Type	Strengths	Weaknesses
Internet Backbone	Price	Lack of Control
	Ubiquity	No Guaranteed QoS
	Connectivity	Lack of Security
ATM & Frame Relay	Price vs. Leased Line	Predefined Endpoints
	Inherent Security	Limited Dial-up
	Well-defined QoS	Not Glitzy
	Inherent Multiprotocol Support	
	Excellent Control	
Enhanced IP		

Enhanced IP VPN

- IP as the “UNI” to the network
- Switched infrastructure using a combination of MPLS*, Frame Relay, and ATM
- *NOT* over the Internet, but has gateway functions
- Inherent security and QoS

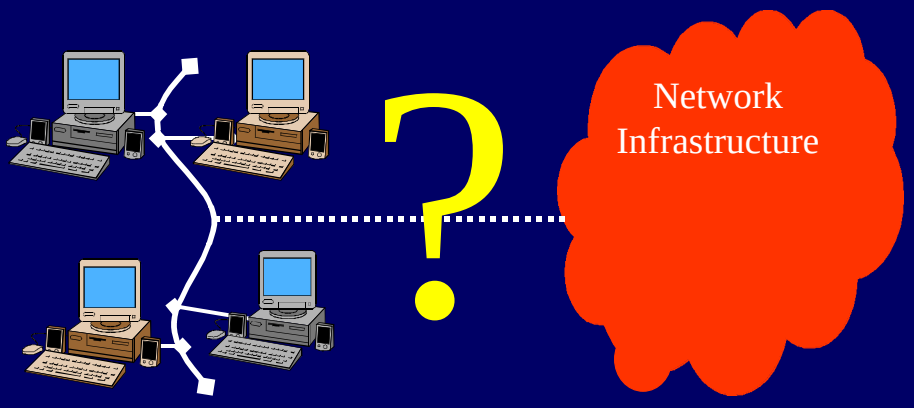


*MultiProtocol Label Switching (MPLS): Follow-on successor to tag switching and switched IP.

Leased Line Replacement VPN Scorecard

VPN Type	Strengths	Weaknesses
Internet Backbone	Price	Lack of Control
	Ubiquity	No Guaranteed QoS
	Connectivity	Lack of Security
ATM & Frame Relay	Price vs. Leased Line	Predefined Endpoints
	Inherent Security	Limited Dial-up
	Well-defined QoS	Not Glitzy
	Inherent Multiprotocol Support	
	Excellent Control	
Enhanced IP	**Great for IP**	**Some static definition required**
	Secure on backbone	**Needs Gateway for Ubiquity & Connectivity**
	QoS	**Emerging Technology/Service**
	Has IP Name	

Next Generation Access



High Performance

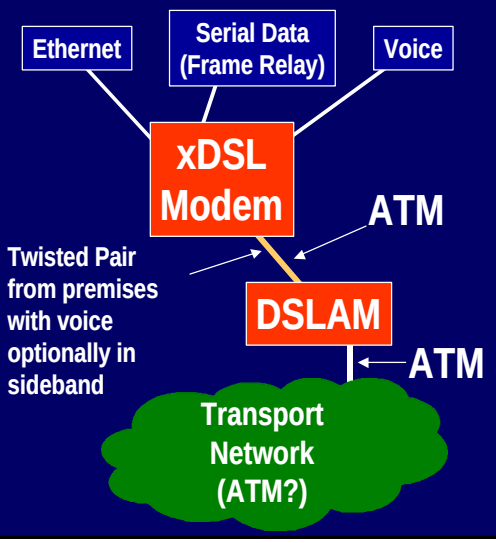
High Performance

Historical Access Options

- Leased line
  - Reliable
  - High speed
  - Usually not redundant
- Dial
  - Universally available
  - Low speed
  - Analog & ISDN

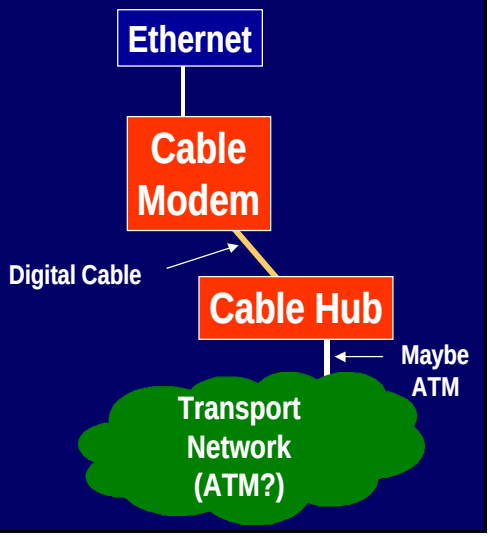
New Access Options - xDSL

- Uses existing copper
- High speed
  - SDSL/ADSL/VDSL
- Dedicated access
- Data interfaces
  - Ethernet
  - Serial (Frame Relay)
- Voice
  - Lifeline, VoDSL, VoIP/FR



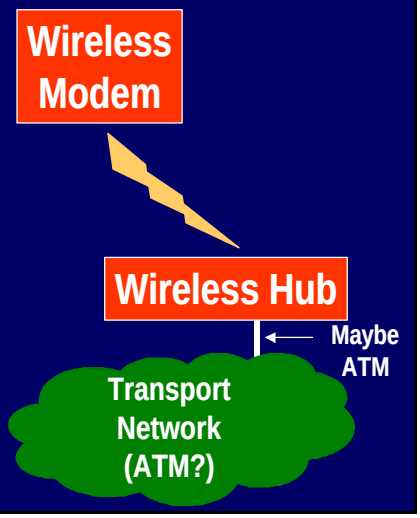
New Access Options – Cable Modem

- Uses digital cable infrastructure
- High speed
  - 2 Mbps (and higher)
- Data interfaces
  - Typically Ethernet
- Voice options vary
- Shared (but encrypted) access
- Physically diverse routing



New Access Options – Wireless

- Newest and least deployed of the three technologies
- Huge potential
  - Theoretically simple installation
  - Great for underdeveloped areas
- Exact impact yet to be determined…



Access Summary

	Traditional	xDSL	Cable
Speed	56/64 kbps, T1/E1, T3/E3. SONET	Typically 1.5 to 2 Mbps	Typically 1.5 to 2 Mbps
Price	High	Low	Low
Media	Dedicated	Dedicated	Shared
Encryption	Optional	Optional	Assumed
Reliability	High	?	?
Service Availability	Universal	Varies	Varies

Access by Service Type

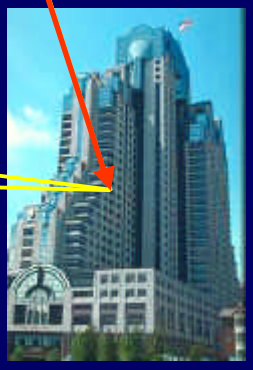
	Private Line	Internet VPN	Frame Relay and ATM	Enhanced IP
Public Internet?	No	Yes	Future?	Gateway
Dedicated	Yes	Yes	Yes	Yes
Dial	N/A	Yes	Very Limited	Yes
xDSL	Future? (CBR ATM)	Yes	Yes, but new service	Yes
Cable Modem	Future? (CBR ATM)	Yes	Yes, but new service	Yes
Wireless	Future? (CBR ATM)	Yes	Very Limited (Future)	Yes

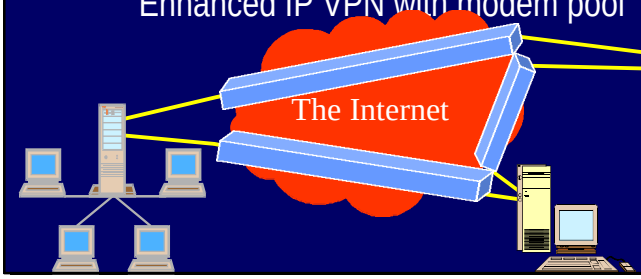
VPNs: Reality Behind the Hype

- Technology Background
- VPN and Access Reference Architectures
- ➡ Application Models and Business Cases

"Road Warriors"

- Calls from anywhere in the world
  - No fixed location; Dial service
- Great fit for Internet Backbone VPN
  - Possibly ATM, Frame Relay, or Enhanced IP VPN with modem pool



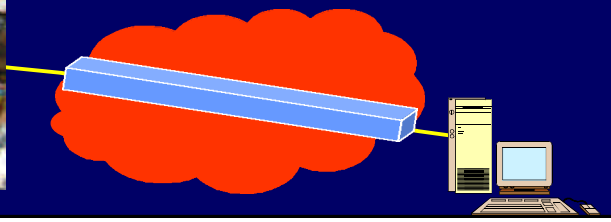


Business Case: "Road Warrior" using Internet VPN

- Up to $25 per mo. versus long distance dial-in
  - 500 minutes to break even at 5¢ per minute
    - 25 minutes per business day
- Service Provider has modem pool and dial support
  - Enterprise has "normal" internet connection
- Caveats
  - "Roaming" or long distance surcharges
    - Footprint of ISP service
  - Administration and support
    - Tunneling, encryption, and authentication
    - Support (finding "local" numbers, etc.)

Fixed Location Telecommuter

- SOHO (Small Office / Home Office)
  - Location doesn't change
  - Could fit all 3 models depending on
    - QoS
    - Multimedia
    - Local access options

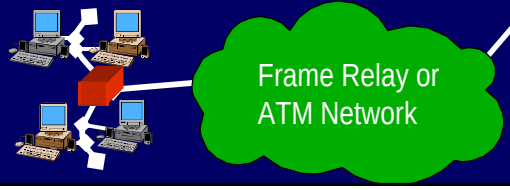


Business Case: Fixed Location Telecommuter

- If Internet VPN:
  - $14.95 for dial
  - $40 to $50 for DSL/Cable
  - May be most attractive for "long distance" telecommuter
- Service provider modem pool and dial support
- Potential for worldwide workforce
- Watch for:
  - xDSL and cable modem may be an important factor
  - Raw speed versus QoS guarantees

Corporate Intranetwork Transport

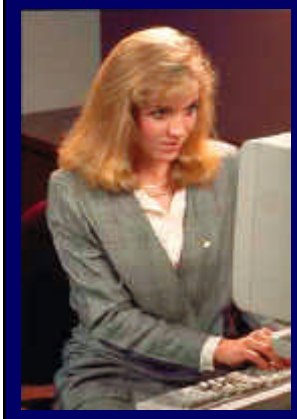
- Core corporate communications as opposed to “remote access”
- “Leased line” function and reliability
  - Capabilities outweigh price
- ATM and Frame Relay usually best
  - Enhanced IP if most traffic is IP



Business Case: Corporate Intranetwork Transport

- Most realistic comparison is with traditional leased lines
  - Usually save at least 50%
  - The larger and more complex the network, the greater the savings
- Enhanced IP may have similar savings...
- Enhanced IP should be in the same price range
  - “Free” internet bandwidth (via Internet VPNs) for the corporate infrastructure is not a reasonable expectation
- This application requires:
  - QoS - including some form of “CIR”
  - Manageability

Remote Office / Branch Office



- Small workgroup, Regional office, Functional workgroup, etc.
  - Low traffic compared with intranetwork node, but more than SOHO
  - Multiple applications
    - Probably includes voice, maybe video
    - May have multiple protocols (e.g. banking)
  - Frame Relay, ATM, or maybe Enhanced IP
    - Depends on multiprotocol and tolerance of overhead

Business Case: Remote / Branch Office using LLR VPN and EIP VPN

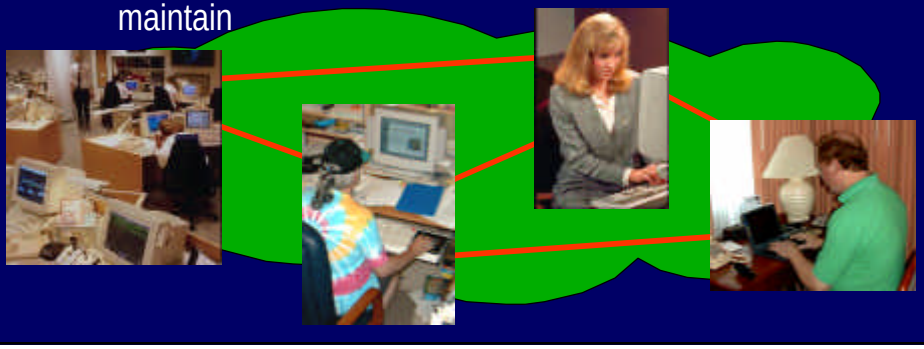
- Just like corporate intranetwork transport, significant cost savings
  - Greater connectivity than a single line for “meshed” connectivity
  - Local FR/ATM (and IP) services in same price range (or less expensive) as dedicated point-to-point
- Internet VPN is an option, but have realistic expectations for QoS and security
- Access price as a major driver

Application Models and Reference Architectures

Model	Internet VPN	Frame Relay and ATM	Enhanced IP VPN
"Road Warrior"	Great fit	Not mobile	OK, with dial capability
Fixed-location Telecommuter	Great fit, especially with DSL/Cable	Seldom economical	Good possibilities
Corporate Intranetwork Transport	QoS, Security, and throughput concerns	Great fit	Great, especially if corporate net is IP-centric
Remote/Branch office	Maybe, depends on protocols and throughput	Good, especially if multiprotocol	Good, especially if corporate net is IP-centric

Interworking among Application Models

- Networks require any-to-any connectivity
- The network infrastructure must be seamless
  - Separate infrastructures are expensive to build and maintain



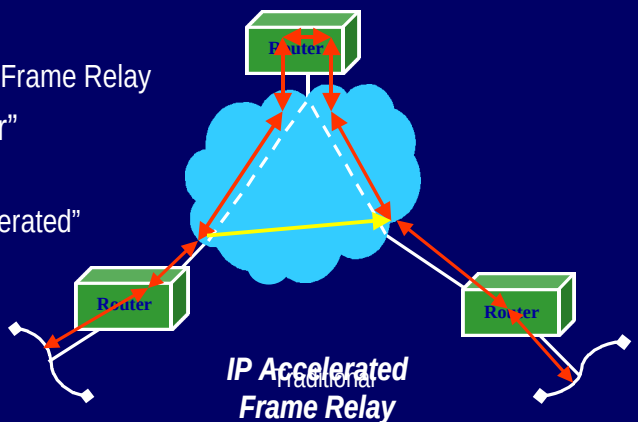
Technology Interworking

- IP to Frame Relay Interworking is especially key
  - Similar to "IP-Enabled Frame Relay"
  - Maps IP address to FR PVC at gateway

Interworking	Enhanced IP VPN	Frame Relay and ATM	Internet-Based VPN
Internet-Based VPN	IP to Internet Gateway	IP (Internet) to FR/ATM Gateway	IP Gateway
Frame Relay and ATM	IP (Internet) to FR/ATM Gateway	Current NNI for each technology	
Enhanced IP VPN	IP Gateway		

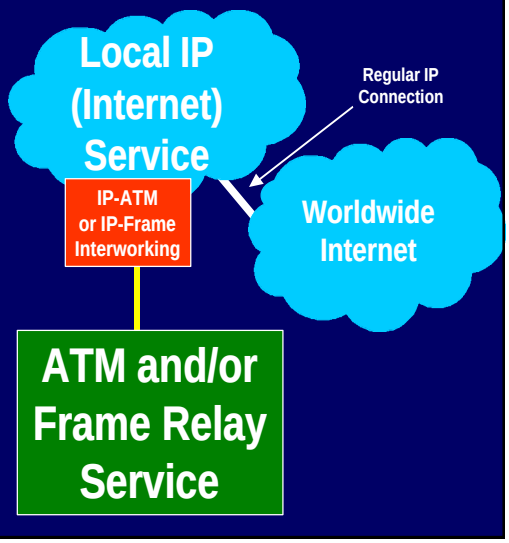
Frame Relay / ATM Interworking with IP

- Any-to-Any Virtual Topologies
  - Unlike current Frame Relay
- Eliminating "star" bottlenecks
  - E.g., IP "Accelerated" frame relay



IP Access to ATM and Frame Relay Services (New Service Option)

- Similar to Frame Relay access to Internet Service
- Local IP-based service
  - Single service provider
    - Maybe single switch
  - Limited contention
- WAN ATM/FR service
  - CoS and QoS
  - Control / reliability



Bottom Line on Business Case

- At least one of the VPN reference architectures provides significant cost advantages for each application model
- It's important to match the application with the "right" VPN service
- Choose a Service Provider with all three options and interworking capabilities

VPNs: Reality Behind the Hype

- Technology Background
- VPN and Access Reference Architectures
- Application Models and Business Cases
- ➡ What to Look For in a VPN

Security

- Tunneling, encryption, & authentication as needed
- Connection-oriented backbone provides security for Frame Relay and ATM

Physical Security: Transmission Facilities

- Is this a repairman or a hacker?
- At some point, you must assume that you can trust the service provider(s)
- Common problem for all types
  - Packets provide limited security
- Encryption is the only real solution

Physical Security: Office Facilities

- There are easier ways than tapping lines to get valuable data
- Two examples:
  - Theft of credit card numbers from e-commerce site
    - 485,000 credit card numbers stolen in 1/99 from one site
    - 300,000 credit cards from CD Universe in 3/99
  - Theft of Server
    - Visa International in 11/96

Are VPNs Secure?

- Security is a process of balancing risks and benefits
- All major transmission systems ***can*** be secure
  - Internet-based networks take more effort
- Greater connectivity introduces more potential exposure

Flexibility

- Multiple Access Options
- Multiprotocol / Multimedia
  - Non-IP Data, e.g., SNA
  - Voice
  - Video / Image
- Ability to Move within the Suite of Services
  - Support for all VPN architectures
  - Full interoperability among services

Scalability & Availability

- Access Speeds and Options
- Access Reach
- Scalable Control
- Scalable Complexity
- Various QoS and CoS options
  - Best effort versus "Gold" service
- Pricing commensurate with the service level

Manageability and Control

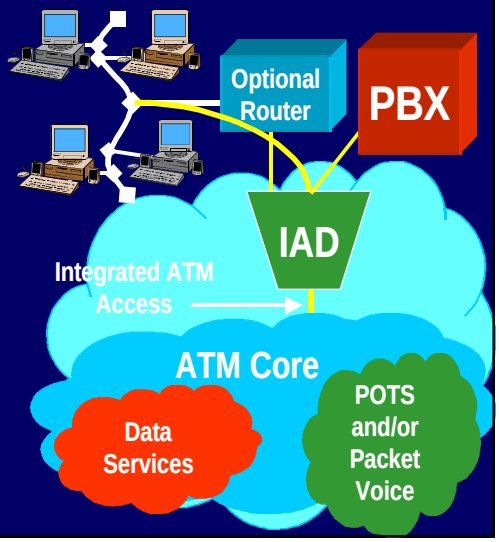
- CNM capabilities
  - Adds, moves and changes under the customer's control
  - Customer-controlled QoS
  - Support for private IP addresses
- Preserve the "look and feel" of the private network

Integrated Total Service Packages

- Need for smooth interworking among the three VPN reference architectures
  - Frame Relay to IP interworking is especially important
- CPE (CLE) equipment management as an option
  - Managed Network Service

Managed Integrated Access Service

- Integrated access for voice and data
- Generic interface for:
  - Voice: T1/E1 for PBX
  - Data: Integral router (Ethernet interface) or frame relay
- ATM for QoS
  - Current generation IADs
  - Next Generation DSL



Integrated Total Service Packages

- Need for smooth interworking among the three VPN reference architectures
  - Frame Relay to IP interworking is especially important
- CPE (CLE) equipment management as an option
  - Managed Network Service
- Gateway services to other services
  - Also for packet to traditional voice
  - Including directory services

VPNs: Reality Behind the Hype

- Technology Background
- VPN and Access Reference Architectures
- Application Models and Business Cases
- What to Look For in a VPN
- ➡ Summary

Summary

- Be sure you choose the right type of VPN
- There's a great business case for VPNs
  - Enterprise customers can save a lot of money with
  - The right *complete suite* of services at
  - The right price with
  - Proven quality and dependability based on
  - The proper set of service and equipment features

Summary

- VPNs have the potential to be a win-win situation for the Enterprise and Service Providers
- Allow both to excel at their core competencies


Thank You!
Webtorials.Com