Hot Topics in Networking

- IP Switching
- MPLS
- Voice over IP
- Gigabit Ethernet
- VPNs

Raj Jain
Professor of Computer and Information Sciences
The Ohio State University

Raj Jain is now at Washington University in Saint Louis,
http://www.cse.wustl.edu/~jain/

Raj Jain
Overview

- Networking Trends
- IP Switching and Label Switching
- Gigabit Ethernet
- Voice over IP
- Virtual Private Networks
Networking Trends

- Impact of Networking
- Networking Trends
- Telecommunication Trends
- Current Research Topics
IP Switching and Label Switching

- Routing vs Switching
- IP Switching (Ipsilon)
- Tag Switching (CISCO)
- Multi-protocol label switching
Gigabit Ethernet

- LAN Switching and Full duplex links
- Distance-Bandwidth Principle
- 10 Mbps to 100 Mbps
- Gigabit PHY and MAC Issues
- ATM vs Gigabit Ethernet
- 1000BASE-T for 1 Gbps over UTP5
- Link aggregation
Voice over IP

- Voice over IP: Why?
- Sample Products and Services
- 13 Technical Issues
- 4 Other Issues
- H.323 Standard
- Session Initiation Protocol (SIP)
Virtual Private Networks

- Types of VPNs
- When and why VPN?
- VPN Design Issues
- Security Issues
- VPN Examples: PPTP, L2TP, IPSec
- Authentication Servers: RADIUS and DIAMETER
- VPNs using Multiprotocol Label Switching
Schedule (Tentative)

Day 1:

- 1:00-2:15 Course Introduction/Trends
- 2:15-2:30 Coffee Break
- 2:30-3:45 IP Switching
- 3:45-4:00 Coffee Break
- 4:00-5:15 Gigabit Ethernet

Day 2:

- 8:00-9:45 Voice over IP
- 9:45-10:00 Coffee Break
- 10:00-12:00 Virtual Private Networks
References

- You can get to all on-line references via:
  http://www.cis.ohio-state.edu/~jain/refs/hot.refs.htm
Pre-Test

Check if you know the difference between:
- Tag Switching and Label Switching
- Min packet sizes on 10Base-T and 1000Base-T
- Carrier Extension and Packet Bursting
- H.323 and Session Initiation Protocol
- Gatekeeper and Gateway
- Firewall and proxy server
- Digital signature and Digital Certificate
- Private Key and Public Key encryption

Number of items checked ______
If you checked more than 4 items, you may not gain much from this course.

If you checked only a few or none, don’t worry. This course will cover all this and much more.
Disclaimer

- The technologies are currently evolving. ⇒ Many statements are subject to change.
- Features not in a technology may be implemented later in that technology.
- Problems claimed to be in a technology may later not be a problem.
Networking Trends and Their Impact

Raj Jain
The Ohio State University
Columbus, OH 43210
Jain@CIS.Ohio-State.Edu
http://www.cis.ohio-state.edu/~jain/
All I want you to tell me is what will be the networking technology in the year 2000.
Overview

- Impact of Networking
- Networking Trends
- Telecommunication Trends
- Current Research Topics
Trends

- Communication is more critical than computing
  - Greeting cards contain more computing power than all computers before 1950.
  - Genesis's game has more processing than 1976 Cray supercomputer.
- Networking speed is the key to productivity
Social Impact of Networking

- No need to get out for
  - Office
  - Shopping
  - Entertainment
  - Education

- Virtual Schools
- Virtual Cash
- Virtual Workplace
  (55 Million US workers will work remotely by 2000)
Cave Persons of 2050
Garden Path to I-Way

- Plain Old Telephone System (POTS) = 64 kbps = 3 ft garden path
- ISDN = 128 kbps = 6 ft sidewalk
- T1 Links to Businesses = 1.544 Mbps = 72 ft = 4 Lane roadway
- Cable Modem Service to Homes: = 10 Mbps = 470 ft = 26 Lane Driveway
- OC3 = 155 Mbps = 1 Mile wide superhighway
- OC48 = 2.4 Gbps = 16 Mile wide superhighway
- OC768 = 38.4 Gbps = 256 Mile wide superhighway
High Technology ≠ More vacation
Impact on R&D

- Too much growth in one year → Can't plan too much into long term
- Long term = 1½ year or 10½ years at most
- Products have life span of 1 year, 1 month, ...
- Short product development cycles. Chrysler reduced new car design time from 6 years to 2.
- Distance between research and products has narrowed → Collaboration between researchers and developers → Academics need to participate in industry consortia
New Challenges

- Networking is moving from specialists to masses ⇒ Usability (plug & play), security
- Exponential growth in number of users + Exponential growth in bandwidth per user ⇒ Traffic management
- Standards based networking for reduced cost
  ⇒ Important to participate in standardization forums
  ATM Forum, Frame Relay Forum, …
  Internet Engineering Task Force (IETF),
  Institute of Electrical and Electronic Engineers (IEEE)
  International Telecommunications Union (ITU), …
Networking Trends

- Copper is still in.
  6-27 Mbps on phone wire.
  Fiber is being postponed.
- Shared LANs to Switched LANs
- Routing to Switching. Distinction is disappearing
- LANs and PBX's to Integrated LANs
- Bandwidth requirements are doubling every 4 months
Telecommunication Trends

- Voice traffic is growing linearly
  Data traffic is growing exponentially
- Carriers are converting to ATM
- Integrated voice, video, data (internet services)
- High-speed frame relay
- xDSL ⇒ Competitive local exchange carriers (CLEC)
- Cable Modems
- Voice over IP
Research Topics

- Terabit networking: Wavelength division multiplexing, all-optical switching
- High-speed access from home
  ⇒ Robust and high-bandwidth encoding techniques
- High-speed Wireless = More than 10 bit/Hz
  28.8 kbps on 30 kHz cellular ⇒ 1 bit/Hz
- Traffic management, quality of service, multicasting:
  • Ethernet LANs, IP networks, ATM Networks
- Mobility
- Large network management Issues.
Research Topics (Cont)

- Information Glut ⇒ Intelligent agents for searching, digesting, summarizing information
- Scalable Voice/Video compression: 2400 bps to 1.5 Mbps video, 8 kbps voice
- Electronic commerce ⇒ Security, privacy, cybercash
- Active Networks ⇒ A "program" in place of addresses
ATM vs Data Networks

- Traffic Management: Loss based in IP. ATM has 1996 traffic management technology. Required for high-speed and variable demands.

- Quality of Service (QoS): Private Network to network interface (PNNI) is QoS-based routing

- Signaling: Internet Protocol (IP) is connectionless. You cannot reserve bandwidth in advance. ATM is connection-oriented. You declare your needs before using the network.

- Switching: In IP, each packet is addressed and processed individually.

- Cells: Fixed size or small size is not important
Old House vs New House

- **New needs:**
  - Solution 1: Fix the old house (cheaper initially)
  - Solution 2: Buy a new house (pays off over a long run)
Networking is the key to productivity
It is impacting all aspects of life ⇒ Networking Age
Profusion of Information
Collaboration between researchers and developers
Usability, security, traffic management
Key References

- See [http://www.cis.ohio-state.edu/~jain/refs/ref_trnd.htm](http://www.cis.ohio-state.edu/~jain/refs/ref_trnd.htm)
- T. Lewis, "The Next 10,000 years," IEEE Computer, April/May 1996
IP Switching
and Label Switching

Raj Jain
Professor of Computer and Information Sciences
The Ohio State University

http://www.cis.ohio-state.edu/~jain/
Switching vs routing
IP Switching (Ipsilon)
Tag Switching (CISCO)
Multi-protocol label switching
IP Forwarding: Fundamentals

- IP routers forward the packets towards the destination subnet
- On the same subnet, routers are not required.
- IP Addresses: 164.56.23.34
  Ethernet Addresses: AA-23-56-34-C4-56
  ATM: 47.0000 1614 999 2345.00.00.AA....
Routing vs Switching

- Routing: Based on address lookup
  ⇒ Search Operation
  ⇒ Complexity $\approx O(\log_2 n)$

- Switching: Based on circuit numbers
  ⇒ Indexing operation
  ⇒ Complexity $O(1)$
  ⇒ Fast and Scalable for large networks and large address spaces

- These distinctions apply on all datalinks: ATM, Ethernet, SONET
Routing vs Switching (Cont)

On ATM networks:

- IP routers use IP addresses
  ⇒ Reassemble IP datagrams from cells
- IP Switches use ATM Virtual circuit numbers
  ⇒ Switch cells
  ⇒ Do not need to reassemble IP datagrams
  ⇒ Fast
IP Switching

- Developed by Ipsilon
- Routing software in every ATM switch in the network
- Initially, packets are reassembled by the routing software and forwarded to the next hop
- Long term flows are transferred to separate VCs. Mapping of VCI in the switch ⇒ No reassembly
If a flow is deemed to be "flow oriented", the node asks the upstream node to set up a separate VC.

Downstream nodes may also ask for a new VC.
After both sides of a flow have separate VCs, the router tells the switch to register the mapping for cut-through.
Flow-oriented traffic: FTP, Telnet, HTTP, Multimedia

Short-lived Traffic: DNS query, SMTP, NTP, SNMP, request-response

Ipsilon claimed that 80% of packets and 90% of bytes are flow-oriented.

Ipsilon claimed their Generic Switch Management Protocol (GSMP) to be 2000 lines, and Ipsilon Flow Management Protocol (IFMP) to be only 10,000 lines of code.

Runs as added software on an ATM switch

Implemented by several vendors
Ipsilon's IP Switching: Issues

- VCI field is used as ID.
  - VPI/VCI change at switch
    ⇒ Must run on every ATM switch
    ⇒ non-IP switches not allowed between IP switches
    ⇒ Subnets limited to one switch

- Cannot support VLANs

- Scalability: Number of VC ≥ Number of flows.
  ⇒ VC Explosion. 1000 setups/sec.

- Quality of service determined implicitly by the flow class or by RSVP

- ATM Only
Tag Switching

- Proposed by CISCO
- Similar to VLAN tags
- Tags can be explicit or implicit L2 header

Ingress router/host puts a tag. Exit router strips it off.

Diagram:
- Untagged Packet
- Tagged packet
- L2 Header
- Tag

Raj Jain
Tag Switching (Cont)

- Switches switch packets based on labels. Do not need to look inside ⇒ Fast.
- One memory reference compared to 4-16 in router
- Tags have local significance
  ⇒ Different tag at each hop (similar to VC #)
Tag Switching (Cont)

- One VC per routing table entry
Alphabet Soup

- CSR Cell Switched Router
- ISR Integrated Switch and Router
- LSR Label Switching Router
- TSR Tag Switching Router
- Multi layer switches, Swoters
- DirectIP
- FastIP
- PowerIP
MPLS

- Multiprotocol Label Switching
- IETF working group to develop switched IP forwarding
- Initially focused on IPv4 and IPv6. Technology extendible to other L3 protocols.
- Not specific to ATM. ATM or LAN.
- Not specific to a routing protocol (OSPF, RIP, ...)
- Optimization only. Labels do not affect the path. Only speed. Networks continue to work w/o labels
Label Assignment

- Binding between a label and a route
- Traffic, topology, or reservation driven
- Traffic: Initiated by upstream/downstream/both
- Topology: One per route, one per MPLS egress node.
- Labels may be preassigned
  ⇒ first packet can be switched immediately
- Reservations: Labels assigned when RSVP "RESV" messages sent/received.
- Unused labels are "garbage collected"
- Labels may be shared, e.g., in some multicasts
Label Format

- Labels = Explicit or implicit L2 header
- TTL = Time to live
- Exp = Experimental
- SI = Stack indicator

<table>
<thead>
<tr>
<th>L2 Header</th>
<th>Label</th>
<th>Exp</th>
<th>SI</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>20b</td>
<td>3b</td>
<td>1b</td>
<td>8b</td>
<td></td>
</tr>
</tbody>
</table>
Label Stacks

- Labels are pushed/popped as they enter/leave MPLS domain
- Routers in the interior will use Interior Gateway Protocol (IGP) labels. Border gateway protocol (BGP) labels outside.

| L2 Header | Label 1 | Label 2 | ⋮ | Label n |
Summary

- IP Switching: Traffic-based, per-hop VCs, downstream originated
- Tag switching: Topology based, one VC per route
- MPLS combines various features of IP switching, Tag switching, and other proposals
Key References

- See [http://www.cis.ohio-state.edu/~jain/refs/ipoa_ref.htm](http://www.cis.ohio-state.edu/~jain/refs/ipoa_ref.htm) and [http://www.cis.ohio-state.edu/~jain/refs/ipsw_ref.htm](http://www.cis.ohio-state.edu/~jain/refs/ipsw_ref.htm)

- Multiprotocol Label Switching (mpls) working group at IETF. Email: mpls-request@cisco.com
Gigabit Ethernet

Raj Jain
Professor of Computer and Information Sciences
The Ohio State University
Columbus, OH 43210
http://www.cis.ohio-state.edu/~jain/
Overview

- LAN Interconnection Devices and Full duplex links
- Distance-Bandwidth Principle
- 10 Mbps to 100 Mbps
- Gigabit PHY and MAC Issues
- ATM vs Gigabit Ethernet
- 1000BASE-T for 1 Gbps over UTP5
- Link aggregation
Hub vs Bridge vs Switch

Hub

Bridge

Switch
Interconnection Devices

LAN = Broadcast domain

LANSegment = Collision Domain

Router

Gateway

Application

Transport

Network

Datalink

Physical

Application

Transport

Network

Datalink

Physical

Raj Jain
Interconnection Devices

- **Repeater**: PHY device that restores data and collision signals
- **Hub**: Multiport repeater + fault detection and recovery
- **Bridge**: Datalink layer device connecting two or more collision domains. MAC multicasts are propagated throughout “LAN.”
- **Switch**: Multiport bridge with parallel paths

These are functions. Packaging varies.
**Full-Duplex LANs**

- Uses point-to-point links between **TWO** nodes
- Full-duplex bi-directional transmission
  - Transmit any time
- Not yet standardized in IEEE 802
- Many switch/bridge/NICs with full duplex
- No collisions $\Rightarrow$ 50+ Km on fiber.
- Commonly used between servers and switches or between switches

Raj Jain
The Magic Word $\alpha$
Distance-B/W Principle

Efficiency = Max throughput/Media bandwidth

Efficiency is a non-increasing function of $\alpha$

$\alpha = \text{Propagation delay} / \text{Transmission time}$

$= (\text{Distance} / \text{Speed of light}) / (\text{Transmission size} / \text{Bits/sec})$

$= \text{Distance} \times \text{Bits/sec} / (\text{Speed of light})(\text{Transmission size})$

Bit rate-distance-transmission size tradeoff.

100 Mb/s ⇒ Change distance or frame size
# Ethernet vs Fast Ethernet

<table>
<thead>
<tr>
<th></th>
<th>Ethernet</th>
<th>Fast Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>10 Mbps</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>MAC</td>
<td>CSMA/CD</td>
<td>CSMA/CD</td>
</tr>
<tr>
<td>Network diameter</td>
<td>2.5 km</td>
<td>205 m</td>
</tr>
<tr>
<td>Topology</td>
<td>Bus, star</td>
<td>Star</td>
</tr>
<tr>
<td>Cable</td>
<td>Coax, UTP, Fiber</td>
<td>UTP, Fiber</td>
</tr>
<tr>
<td>Standard</td>
<td>802.3</td>
<td>802.3u</td>
</tr>
<tr>
<td>Cost</td>
<td>X</td>
<td>2X</td>
</tr>
</tbody>
</table>

![Diagram](Raj Jain)
Fast Ethernet Standards

- **100BASE-T4**: 100 Mb/s over 4 pairs of CAT-3, 4, 5
- **100BASE-TX**: 100 Mb/s over 2 pairs of CAT-5, STP
- **100BASE-FX**: 100 Mbps CSMA/CD over 2 fibers
- **100BASE-X**: 100BASE-TX or 100BASE-FX
- **100BASE-T**: 100BASE-T4, 100BASE-TX, or 100BASE-FX

Based on FDDI Phy
100 BASE-X

- $X =$ Cross between IEEE 802.3 and ANSI X3T9.5

100BASE-X

- IEEE 802.2 Logical Link Control
- IEEE 802.3 CSMA/CD
- IEEE 802.3 PHY Coding
- IEEE 802.3 Medium Attachment Unit
- ANSI X3T9.5 MAC
- ANSI X3T9.5 PHY
- ANSI X3T9.5 PMD
Full-Duplex Ethernet

- Uses point-to-point links between TWO nodes
- Full-duplex bi-directional transmission
- Transmit any time
- Many vendors are shipping switch/bridge/NICs with full duplex
- No collisions $\Rightarrow$ 50+ Km on fiber.
- Between servers and switches or between switches
Gigabit Ethernet

- Being standardized by 802.3z
- Project approved by IEEE in June 1996
- 802.3 meets every three months $\Rightarrow$ Too slow
  $\Rightarrow$ Gigabit Ethernet Alliance (GEA) formed. It meets every two weeks.
- Decisions made at GEA are formalized at 802.3 High-Speed Study Group (HSSG)
- Based on Fiber Channel PHY
- Shared (half-duplex) and full-duplex version
- Gigabit 802.12 and 802.3 to have the same PHY

Raj Jain
How Much is a Gbps?

- 622,000,000 bps = OC-12
- 800,000,000 bps (100 MBps Fiber Channel)
- 1,000,000,000 bps
- 1,073,741,800 bps = $2^{30}$ bps ($2^{10} = 1024 = 1k$)
- 1,244,000,000 bps = OC-24
- 800 Mbps $\Rightarrow$ Fiber Channel PHY
  $\Rightarrow$ Shorter time to market
- Decision: 1,000,000,000 bps $\Rightarrow$ 1.25 GBaud PHY
- Not multiple speed $\Rightarrow$ Sub-gigabit Ethernet rejected
- 1000Base-X
Physical Media

- Unshielded Twisted Pair (UTP-5): 4-pairs
- Shielded Twisted Pair (STP)
- Multimode Fiber: 50 µm and 62.5 µm
  - Use CD lasers
- Single-Mode Fiber
- Bit Error Rate better than $10^{-12}$
How Far Should It Go?

- Full-Duplex:
  - Fiber Channel: 300 m on 62.5 μm at 800 Mbps ⇒ 230 m at 1000 Mbps
  - Decision: 500 m at 1000 Mbps ⇒ Minor changes to FC PHY

- Shared:
  - CSMA/CD without any changes ⇒ 20 m at 1 Gb/s (Too small)
  - Decision: 200 m shared ⇒ Minor changes to 802.3 MAC

Raj Jain
PHY Issues

- Fiber Channel PHY:
  100 MBps = 800 Mbps
  \[ \Rightarrow \text{1.063 GBaud using 8b10b} \]

- Changes to get 500 m on 62.5-\(\mu\)m multimode fiber
  - Modest decrease in rise and fall times of the transceivers
- Symbol Codes for Specific Signals: Jam, End-of-packet, beginning of packet
- PHY-based flow Control: No.
  Use the XON/XOFF flow control of 802.3x
850 nm vs 1300 nm lasers

- 850 nm used in 10Base-F
  - Cannot go full distance with 62.5-μm fiber
  - 500 m with 50-μm fiber
  - 250 m with 62.5-μm fiber

- 1300 nm used in FDDI but more expensive
  - Higher eye safety limits
  - Better Reliability
  - Start with 550 m on 62.5-μm fiber
  - Could be improved to 2 km on 62.5-μm fiber
    ⇒ Needed for campus backbone
Media Access Control Issues

- Carrier Extension
- Frame Bursting
- Buffered Distributor
Carrier Extension

- Frame
- RRRRRRRRRRR
  - Carrier Extension
  - 512 Bytes

- 10 Mbps at 2.5 km ⇒ Slot time = 64 bytes
- 1 Gbps at 200 m ⇒ Slot time = 512 bytes
- Continue transmitting control symbols.
  - Collision window includes the control symbols
- Control symbols are discarded at the destination
- Net throughput for small frames is only marginally better than 100 Mbps
Frame Bursting

- Don’t give up the channel after every frame
- After the slot time, continue transmitting additional frames (with minimum inter-frame gap)
- Interframe gaps are filled with extension bits
- No new frame transmissions after 8192 bytes
- Three times more throughput for small frames
Buffered Distributor

- All incoming frames are buffered in FIFOs
- CSMA/CD arbitration inside the box to transfer frames from an incoming FIFO to all outgoing FIFOs
- Previous slides were half-duplex. With buffered distributor all links are full-duplex with frame-based flow control
- Link length limited by physical considerations only
Schedule

- November 1996: Proposal cutoff
- July 1997: Working Group Ballot
- March 1998: Approval
1000Base-X

- 1000Base-LX: 1300-nm laser transceivers
  - 2 to 550 m on 62.5-μm or 50-μm multimode, 2 to 3000 m on 10-μm single-mode
- 1000Base-SX: 850-nm laser transceivers
  - 2 to 300 m on 62.5-μm, 2 to 550 m on 50-μm. Both multimode.
- 1000Base-CX: Short-haul copper jumpers
  - 25 m 2-pair shielded twinax cable in a single room or rack.
  - Uses 8b/10b coding ⇒ 1.25 Gbps line rate
1000Base-T

- 100 m on 4-pair Cat-5 UTP
  ⇒ Network diameter of 200 m
- 250 Mbps/pair full duplex DSP based PHY
  ⇒ Requires new 5-level (PAM-5) signaling
    with 4-D 8-state Trellis code FEC
- Automatically detects and corrects pair-swapping,
  incorrect polarity, differential delay variations across
  pairs
- Autonegotiation ⇒ Compatibility with 100Base-T
- 802.3ab task force began March’97, ballot July’98,
  Final standard by March’99.
Link Aggregation

- Server needs only one IP and MAC address.
- Incremental bandwidth
- More reliability. More flexibility in bandwidth usage
- Issues: Configuration error detection
- 802.3ad task force PAR approved July 1998.

Raj Jain
### Design Parameter Summary

<table>
<thead>
<tr>
<th>Parameter</th>
<th>10 Mbps</th>
<th>100 Mbps</th>
<th>1 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot time</td>
<td>512 bt</td>
<td>512 bt</td>
<td>4096 bt</td>
</tr>
<tr>
<td>Inter Frame Gap</td>
<td>9.6 $\mu$s</td>
<td>0.96 $\mu$s</td>
<td>0.096 $\mu$s</td>
</tr>
<tr>
<td>Jam Size</td>
<td>32 bits</td>
<td>32 bits</td>
<td>32 bits</td>
</tr>
<tr>
<td>Max Frame Size</td>
<td>1518 B</td>
<td>1518 B</td>
<td>1518 B</td>
</tr>
<tr>
<td>Min Frame Size</td>
<td>64 B</td>
<td>64 B</td>
<td>64 B</td>
</tr>
<tr>
<td>Burst Limit</td>
<td>N/A</td>
<td>N/A</td>
<td>8192 B</td>
</tr>
</tbody>
</table>

-bt = bit time

Raj Jain
# ATM vs Gb Ethernet

<table>
<thead>
<tr>
<th>Issue</th>
<th>ATM</th>
<th>Gigabit Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>SM Fiber, MM Fiber, UTP5</td>
<td>Mostly fiber</td>
</tr>
<tr>
<td>Max Distance</td>
<td>Many miles using SONET</td>
<td>260-550 m</td>
</tr>
<tr>
<td>Data Applications</td>
<td>Need LANE, IPOA</td>
<td>No changes needed</td>
</tr>
<tr>
<td>Interoperability</td>
<td>Good</td>
<td>Limited</td>
</tr>
<tr>
<td>Ease of Mgmt</td>
<td>LANE</td>
<td>802.1Q VLANs</td>
</tr>
<tr>
<td>QoS</td>
<td>PNNI</td>
<td>802.1p (Priority)</td>
</tr>
<tr>
<td>Signaling</td>
<td>UNI</td>
<td>None/RSVP (?)</td>
</tr>
<tr>
<td>Traffic Mgmt</td>
<td>Sophisticated</td>
<td>802.3x Xon/Xoff</td>
</tr>
</tbody>
</table>

Raj Jain
Summary

- Gigabit Ethernet runs at 1000 Mbps
- Both shared and full-duplex links
- Fully compatible with current Ethernet
- 1000BASE-T allows 1000 Mbps over 100m of UTP5
- Link aggregation will allow multiple links in parallel
References

- For a detailed list of references, see [http://www.cis.ohio-state.edu/~jain.refs/gbe.refs.htm](http://www.cis.ohio-state.edu/~jain.refs/gbe.refs.htm)


- Gigabit Ethernet Consortium [http://www.gigabit-ethernet.org](http://www.gigabit-ethernet.org)
Voice over IP

Raj Jain
The Ohio State University
Columbus, OH 43210
Jain@CIS.Ohio-State.Edu

http://www.cis.ohio-state.edu/~jain/

Raj Jain
Overview

- Voice over IP: Why?
- Sample Products and Services
- 13 Technical Issues
- 4 Other Issues
- H.323 Standard
- Session Initiation Protocol (SIP)
Market

- International VOIP calls could cost 1/5th of normal rates ⇒ Big share of $18B US to foreign calls. $15B within Europe.
- 500,000 IP telephony users at the end of 1995.
- 15% of all voice calls on IP/Internet by 2000 ⇒ 10M users and $500M in VOIP product sales in 1999 [IDC]
Scenario 1: PC to PC

- Need a PC with sound card
- IP Telephony software: Cuseeme, Internet Phone, ...
- Video optional
Scenario 2: PC to Phone

- Need a gateway that connects IP network to phone network (Router to PBX)
Scenario 3: Phone to Phone

- Need more gateways that connect IP network to phone networks
- The IP network could be dedicated intra-net or the Internet.
- The phone networks could be intra-company PBXs or the carrier switches
Advantages

- Private voice networks require \( n(n-1) \) access links. Private data networks require only \( n \) access links.
- Voice has per-minute distance sensitive charge. Data has flat time-insensitive distance-insensitive charge.
- Easy alternate routing \( \Rightarrow \) More reliability.
- No 64kbps bandwidth limitation \( \Rightarrow \) Easy to provide high-fidelity voice.
Applications

- Any voice communication where PC is already used:
  - Document conferencing
  - Helpdesk access
  - On-line order placement
- International callbacks
  (many operators use voice over frame relay)
- Intranet telephony
- Internet fax
Sample Products

- VocalTec Internet Phone: PC to PC.
- Microsoft NetMeeting: PC to PC. Free.
- Internet PhoneJACK: ISA card to connect a standard phone to PC. Works with NetMeeting, InternetPhone etc. Provides compression.
- Internet LineJACK: Single-line gateway.
- Micom V/IP Family:
  - Analog and digital voice interface cards
  - PC and/or gateway
Features:

- Compression
- Phone number to IP address translation.
- Supports RSVP.
- Limits number of calls.
Products (Cont)

- VocalTec Internet Telephony Gateway:
  - Similar to Micom V/IP
  - Interactive voice response system for problem reporting
  - Allows WWW plug in
  - Can monitor other gateways and use alternate routes including PSTN
  - Sold to Telecom Finland. New Zealand Telecom.

- Lucent's Internet Telephony Server: Gateway
  - Lucent PathStar Access Server
Products (Cont)

- CISCO 2600 Routers: Voice interface cards (VICs)
  Reduces one hop.
- Baynetworks, 3COM, and other router vendors have announced product plans
Sample Services

- IDT Corporation offers Net2Phone, Carrier2Phone, Phone2Phone services.
- Global Exchange Carrier offers international calls using VocalTec InternetPhone s/w and gateways.
- Qwest offers 7.5¢/min VOIP Q.talk service in 16 cities.
- ITXC provides infrastructure and management to 'Internet Telephone Service Providers (ITSPs)'
- America On-line offers 9¢/min service.
- AT&T announced 7.5¢/min VOIP trials in 9 US cities.

Raj Jain
Other trials: USA Global link, Delta 3, WorldCom, MCI, U.S. West, Bell Atlantic, Sprint, AT&T/Japan, KDD/Japan, Dacom/Korea, Deutsche Telekom in Germany, France Telecom, Telecom Finland, and New Zealand Telecom.

Level 3 is building a nation wide IP network for telephony.

Bell Canada has formed 'Emergis' division.

Bellcore has formed 'Soliant Internet Systems' unit

Bell Labs has formed 'Elemedia' division
Technical Issues

1. Large Delay
   - Normal Phone: 10 ms/kmile $\Rightarrow$ 30 ms coast-to-coast
   - G.729: 10 ms to serialize the frame + 5 ms look ahead + 10 ms computation $= 25$ ms one-way algorithmic delay
   - G.723.1 $= 100$ ms one-way algorithmic delay
   - Jitter buffer $= 40-60$ ms
   - Poor implementations $\Rightarrow$ 400 ms in the PC
   - In a survey, 77% users found delay unacceptable.
Technical Issues (Cont)

   Shorter packets? IP precedence (TOS) field.

3. Frame length: $9 \text{ kB} \text{ at } 64 \text{ kbps} = 1.125 \text{ s}$  
   Smaller MTU $\Rightarrow$ Fragment large packets

4. Lost Packets: Replace lost packets by silence,  
   extrapolate previous waveform

5. Echo cancellation: 2-wire to 4-wire.  
   Some FR and IP systems include echo suppressors.
Technical Issues (Cont)

6. Silence suppression
7. Address translation: Phone # to IP. Directory servers.
8. Telephony signaling: Different PBXs may use different signaling methods.
9. Bandwidth Reservations: Need RSVP.
10. Multiplexing: Subchannel multiplexing
    \[\Rightarrow\] Multiple voice calls in one packet.
11. Security: Firewalls may not allow incoming IP traffic
12. Insecurity of internet
13. Voice compression: Load reduction
Other Issues

1. Per-minute distance-sensitive charge vs flat time-insensitive distance-insensitive charge
2. Video requires a bulk of bits but costs little. Voice is expensive. On IP, bits are bits.
3. National regulations and government monopolies
   ⇒ Many countries forbid voice over IP
   In Hungary, Portugal, etc., it is illegal to access a web site with VOIP s/w. In USA, Association of Telecommunications Carriers (ACTA) petitioned FCC to levy universal access charges in ISPs
4. Modem traffic can’t get more than 2400 bps.
Compression Standards

- G.711: 64 kbps Pulse Code Modulation (PCM)
- G.721:
  - 32 kbps Adaptive Differential PCM (ADPCM).
  - Difference between actual and predicted sample.
  - Used on international circuits
- G.728: 16 kbps Code Excited Linear Prediction (CELP).
Compression (Cont)

- G.729A:
  - Supported by AT&T, Lucent, NTT.
  - Used in simultaneous voice and data (SVD) modems.
  - Used in Voice over Frame Relay (VFRADs).
  - 4 kbps with proprietary silence suppression.
Compression (Cont)

- G.723.1: Dual rates (5.3 and 6.3 kbps).
  - Packet loss tolerant.
  - Silence suppression option.
  - Recommended by International Multimedia Teleconferencing Consortium (IMTC)'s VOIP forum as default for H.323.
  - Supported by Microsoft, Intel.
- Mean opinion score (MOS) of 3.8.
  4.0 = Toll quality.
Telephony/Conferencing Systems

- Video I/O Equipment
- Audio I/O Equipment
- Data Application
- System Control
- Video Codec
- Audio Codec
- Data Protocol
- Control Protocol
- Multiplexing/Demultiplexing
- Network Interface
- Network
## Conferencing Standards

<table>
<thead>
<tr>
<th>Network</th>
<th>ISDN</th>
<th>ATM</th>
<th>PSTN</th>
<th>LAN</th>
<th>POTs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conf. Std.</td>
<td>H.320</td>
<td>H.321</td>
<td>H.322</td>
<td>H.323 V1/V2</td>
<td>H.324</td>
</tr>
<tr>
<td>Audio</td>
<td>G.711,</td>
<td>G.711,</td>
<td>G.711,</td>
<td>G.711,</td>
<td>G.723.1,</td>
</tr>
<tr>
<td></td>
<td>G.728</td>
<td>G.728</td>
<td>G.728</td>
<td>G.728</td>
<td></td>
</tr>
<tr>
<td>Audio Rates</td>
<td>64, 48-64</td>
<td>64, 48-64, 16</td>
<td>64, 48-64, 16</td>
<td>64, 48-64, 16, 8, 5.3/6.3</td>
<td>8, 5.3/6.3</td>
</tr>
<tr>
<td>kbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video</td>
<td>H.261</td>
<td>H.261,</td>
<td>H.261,</td>
<td>H.261</td>
<td>H.261</td>
</tr>
<tr>
<td>Codec</td>
<td>H.263</td>
<td>H.263</td>
<td>H.263</td>
<td>H.263</td>
<td>H.263</td>
</tr>
<tr>
<td>Data Sharing</td>
<td>T.120</td>
<td>T.120</td>
<td>T.120</td>
<td>T.120</td>
<td>T.120</td>
</tr>
<tr>
<td>Control</td>
<td>H.230,</td>
<td>H.242</td>
<td>H.242,</td>
<td>H.245</td>
<td>H.245</td>
</tr>
<tr>
<td></td>
<td>H.242</td>
<td></td>
<td>H.230</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiplexing</td>
<td>H.221</td>
<td>H.221</td>
<td>H.221</td>
<td>H.225.0</td>
<td>H.223</td>
</tr>
<tr>
<td>Signaling</td>
<td>Q.931</td>
<td>Q.931</td>
<td>Q.931</td>
<td>Q.931</td>
<td>-</td>
</tr>
</tbody>
</table>

Raj Jain
**H.323 Protocols**

- Multimedia over LANs
- Provides component descriptions, signaling procedures, call control, system control, audio/video codecs, data protocols

<table>
<thead>
<tr>
<th>Video</th>
<th>Audio</th>
<th>Control and Management</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.261</td>
<td>G.711, G.722, G.723.1, G.728, G.729</td>
<td>H.225.0 RAS</td>
<td>T.124</td>
</tr>
<tr>
<td>H.263</td>
<td></td>
<td>H.225.0 Signaling</td>
<td></td>
</tr>
<tr>
<td>RTP</td>
<td></td>
<td>H.245 Control</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td></td>
<td>X.224 Class 0</td>
<td>T.125</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>T.123</td>
</tr>
<tr>
<td>Network (IP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Datalink (IEEE 802.3)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Raj Jain
H.323 Components

Terminals

Gatekeeper

MCU

Gateway

Firewall

Router

To Internet

ISDN

PSTN

ATM

H.323 Proxy

Raj Jain
H.323 Terminals

- Video I/O Equipment
  - H.261
  - H.263
- Audio I/O Equipment
  - G.711
  - G.723
  - G.729
  - G.729
  - T.120
- Data Application
  - H.245 Control
  - Q.931 Call Setup
  - RAS Gatekeeper Interface
- System Control
- User Interface
- LAN Interface
H.323 Terminals

- Client end points. PCs.
- H.245 to negotiate channel usage and capabilities.
- Q.931 for call signaling and call setup.
- Registration/Admission/Status (RAS) protocol to communicate with gatekeepers.
- RTP/RTCP for sequencing audio and video packets.
H.323 Gateways

- Provide translation between H.323 and other terminal types (PSTN, ISDN, H.324)
- Not required for communication with H.323 terminals on the same LAN.
H.323 Gatekeepers

- Provide call control services to registered end points.
- One gatekeeper can serve multiple LANs
- Address translation (LAN-IP)
- Admission Control: Authorization
- Bandwidth management
  (Limit number of calls on the LAN)
- Zone Management: Serve all registered users within its zone of control
- Forward unanswered calls
- May optionally handle Q.931 call control
H.323 MCUs

- Multipoint Control Units
- Support multipoint conferences
- Multipoint controller (MC) determines common capabilities.
- Multipoint processor (MP) mixes, switches, processes media streams.
- MP is optional. Terminals multicast if no MP.
Session Initiation Protocol (SIP)

- Application level signaling protocol
- Allows creating, modifying, terminating sessions with one or more participants
- Carries session descriptions (media types) for user capabilities negotiation
- Supports user location, call setup, call transfers
- Supports mobility by proxying and redirection
- Allows multipoint control unit (MCU) or fully meshed interconnections
- Gateways can use SIP to setup calls between them
SIP (Cont)

- SIP works in conjunction with other IP protocols for multimedia:
  - RSVP for reserving network resources
  - RTP/RTCP/RTSP for transporting real-time data
  - Session Announcement Protocol (SAP) for advertising multimedia session
  - Session description protocol (SDP) for describing multimedia session
- Can also be used to determine whether party can be reached via H.323, find H.245 gateway/user address
SIP (Cont)

- SIP is text based (similar to HTTP)
  - SIP messages can be easily generated by humans, CGI, Perl, or Java programs.

- SIP Uniform Resource Locators (URLs):
  - Similar to email URLs
  - sip:jain@cis.ohio-state.edu
  - sip:+1-614-292-3989:123@osu.edu?subject=lecture

- SIP messages are sent to SIP server at the specified IP address

- SIP can use UDP or TCP
Locating using SIP

- Allows locating a callee at different locations
- Callee registers different locations with SIP Server
- Servers can also use finger, rwhois, ldap to find a callee
- SIP Messages: Ack, Bye, Invite, Register, Redirection, ...

```
X
```
```
Location
Server
```
```
Jain@cis
```
```
Jain@acm
```
```
Invite Jain@cis
```
```
Moved to Jain@acm
```
```
Invite Jain@acm
```
```
Ack Jain@acm
```
```
Raj Jain
```
Gateway = Signaling Fns + Media Transfer Fns

Call Agents: Signaling functions ⇒ Intelligent
⇒ More complex ⇒ Fewer
⇒ Control multiple media gateways ⇒ Need MGCP

MGCP = Simple Gateway Control Protocol (SGCP) + Internet Protocol Device Control (IPDC)
Media Gateways: Examples

- Trunking Gateway: Connects a PSTN trunk to VOIP
  Terminates multiple digital circuits

- Residential Gateway: Connects a RJ11 to VOIP
  Will be used in cable set-top boxes, xDSL, ...

- Business Gateway: Connects a PBX to VOIP

- Network Access Servers: Answer data + VOIP calls
MGCP Terminology

- Connections between End-Points
- Call = Set of Connections
- End Points: Analog line, Digital Channel (DS0), Announcement server (does not listens), Interactive Voice Response (announces and listens), Wiretap (listens only), Conference Bridge (mixes), Packet Relay (proxy server)
- Call agents are identified by name not address ⇒ Can be easily moved to different machine
MGCP Terminology (Cont)

- Events: hang-up (hu), flash hook (hf), …
- 3 Types of Events: on/off (stay until changed), time-out (change or time out), brief (very short)
- Events are grouped into packages for various types of end points, e.g., Trunk package (T), Line Package (L), …
- Notation: Package/event@connection
  E.g., L/hu@0A3F58
MGCP Commands

- Endpoint Configuration (EPCF): Specify coding
- Notification Request (RQNT): Watch for event
- Notify (NTFY): Used by gateway to inform Call agent
- Create Connection (CRCX)
- Modify Connection (MDCX)
- Delete Connection (DLCX)
- Audit Endpoint (AUEP): Give me status
- Audit Connection (AUCX)
- Restart in Progress (RSIP): Used by gateway to indicate initialization/shutdown of endpoints/gateway
Session Description Protocol

- SDP V2 [RFC2327]
- Used to describe media type and port # for connections and mbone sessions
- Includes: Version (v), Session name (s), Information (i), Owner (o), Connection information (c), media type, port, and coding (m), session attributes (a), ...
- Example:
  s = Netlab Seminars
  c = 224.5.17.11 127 2873397496 2873404696
  m = audio 3456 0
  m = video 2232 0
Session Announcement Protocol

- SAP [draft-ietf-mmusic-sap-v2-01.txt, 6/99]
- To announce multicast sessions
- Sends SDP session descriptions to a well-known multicast address and port
- Use same scope as session being announced
  Anyone who gets the announcement can get the session.
- Announcers listen to other announcements and adjust frequency to limit bandwidth usage.
- Announcements are stopped after the session end time
Summary

- Voice over IP products and services are being rolled out
- Ideal for computer-based communications
- IP needs QoS for acceptable quality
- A number of working group at IETF are working on it
- H.323 provides interoperability
References

- See
  [http://www.cis.ohio-state.edu/~jain/refs/ref.voip.htm](http://www.cis.ohio-state.edu/~jain/refs/ref.voip.htm)
  for a detailed list of references.
Virtual Private Networks

Raj Jain
The Ohio State University
Columbus, OH 43210
Jain@CIS.Ohio-State.Edu

http://www.cis.ohio-state.edu/~jain/
Overview

- Types of VPNs
- When and why VPN?
- VPN Design Issues
- Security Issues
- VPN Examples: PPTP, L2TP, IPSec
- Authentication Servers: RADIUS and DIAMETER
- VPNs using Multiprotocol Label Switching
What is a VPN?

- Private Network: Uses leased lines

- Virtual Private Network: Uses public Internet
A Private network is like having a private road to all employees and branch offices.

Better to share the public roads.
VPN are like having a private talk in a crowded room. You need to code your messages.

Can I have a private talk with you?
Types of VPNs

- WAN VPN: Branch offices
- Access VPN: Roaming Users
- Extranet VPNs: Suppliers and Customers
Why VPN?

- Reduced telecommunication costs
- Less administration ⇒ 60% savings (Forester Res.)
- Less expense for client and more income for ISPs
- Long distance calls replaced by local calls
- Increasing mobility ⇒ More remote access
- Increasing collaborations
  ⇒ Need networking links with partners
When to VPN?

- **Modest Bandwidth**
  - Many Locations
  - QoS not Critical

- **Long Distance**
  - Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical
  ⇒ VPN less justifiable

- **More Locations, Longer Distances, Less Bandwidth/site, QoS less critical**
  ⇒ VPN more justifiable

Raj Jain
VPN Design Issues

1. Security
2. Address Translation
3. Performance: Throughput, Load balancing (round-robin DNS), fragmentation
4. Bandwidth Management: RSVP
5. Availability: Good performance at all times
6. Scalability: Number of locations/Users
7. Interoperability: Among vendors, ISPs, customers (for extranets) ⇒ Standards Compatibility, With firewall
Design Issues (Cont)

8. Compression: Reduces bandwidth requirements
9. Manageability: SNMP, Browser based, Java based, centralized/distributed
10. Accounting, Auditing, and Alarming
11. Protocol Support: IP, non-IP (IPX)
12. Platform and O/S support: Windows, UNIX, MacOS, HP/Sun/Intel
13. Installation: Changes to desktop or backbone only
14. Legal: Exportability, Foreign Govt Restrictions, Key Management Infrastructure (KMI) initiative
   ⇒ Need key recovery
Security 101

- Integrity: Received = sent?

- Availability: Legal users should be able to use. Ping continuously $\Rightarrow$ No useful work gets done.

- Confidentiality and Privacy: No snooping or wiretapping

- Authentication: You are who you say you are. A student at Dartmouth posing as a professor canceled the exam.

- Authorization = Access Control Only authorized users get to the data
Secret Key Encryption

- Encrypted_Message = Encrypt(Key, Message)
- Message = Decrypt(Key, Encrypted_Message)
- Example: Encrypt = division
- 433 = 48 R 1 (using divisor of 9)
Public Key Encryption

- Invented in 1975 by Diffie and Hellman
- $\text{Encrypted\_Message} = \text{Encrypt}(\text{Key1, Message})$
- $\text{Message} = \text{Decrypt}(\text{Key2, Encrypted\_Message})$
Public Key Encryption

- RSA: Encrypted_Message = $m^3 \mod 187$
- Message = Encrypted_Message$^{107} \mod 187$
- Key1 = <3,187>, Key2 = <107,187>
- Message = 5
- Encrypted Message = $5^3 = 125$
- Message = $125^{107} \mod 187$
  = $125^{(64+32+8+2+1)} \mod 187$
  = $\{(125^{64} \mod 187)(125^{32} \mod 187)...(125^2 \mod 187)(125)\} \mod 187 = 5$
- $125^4 \mod 187 = (125^2 \mod 187)^2 \mod 187$
Public Key (Cont)

- One key is private and the other is public
- \[ \text{Message} = \text{Decrypt} \left( \text{Public\_Key,}\right. \]
  \[ \quad \text{Encrypt} \left( \text{Private\_Key, Message} \right) \]
- \[ \text{Message} = \text{Decrypt} \left( \text{Private\_Key,}\right. \]
  \[ \quad \text{Encrypt} \left( \text{Public\_Key, Message} \right) \]
Digital Signature

- Message Digest = Hash(Message)
- Signature = Encrypt(Private_Key, Hash)
- Hash(Message) = Decrypt(Public_Key, Signature)  ⇒ Authentic

\[
\begin{align*}
\text{Private Key} & \quad \text{Hash} \\
\text{Text} & \rightarrow \text{Digest} & & \rightarrow \text{Signature} \\
\text{Public Key} & \\
\text{Signature} & \downarrow \\
& \rightarrow \text{Digest} & & \rightarrow \text{Hash} & & \rightarrow \text{Text}
\end{align*}
\]
Certificate

- Like driver license or passport
- Digitally signed by Certificate authority (CA) - a trusted organization
- Public keys are distributed with certificates
- CA uses its public key to sign the certificate
  ⇒ Hierarchy of trusted authorities
Confidentiality

- User 1 to User 2:
  - Encrypted_Message = Encrypt(Public_Key2, Encrypt(Private_Key1, Message))
  - Message = Decrypt(Public_Key1, Decrypt(Private_Key2, Encrypted_Message))

⇒ Authentic and Private
Firewall: Bastion Host

- Bastions overlook critical areas of defense, usually having stronger walls.
- Inside users log on the Bastion Host and use outside services.
- Later they pull the results inside.
- One point of entry. Easier to manage security.
Proxy Servers

- Specialized server programs on bastion host
- Take user's request and forward them to real servers
- Take server's responses and forward them to users
- Enforce site security policy
  \[\Rightarrow\] May refuse certain requests.
- Also known as application-level gateways
- With special "Proxy client" programs, proxy servers are almost transparent

Raj Jain
VPN Security Issues

- Authentication methods supported
- Encryption methods supported
- Key Management
- Data stream filtering for viruses, JAVA, active X
- Supported certificate authorities (X.509, Entrust, VeriSign)
- Encryption Layer: Datalink, network, session, application. Higher Layer ⇒ More granular
- Granularity of Security: Departmental level, Application level, Role-based
Private Addresses

- 32-bit Address ⇒ 4 Billion addresses max
- Subnetting ⇒ Limit is much lower
- Shortage of IP address ⇒ Private addresses
- Frequent ISP changes ⇒ Private address
- Private ⇒ Not usable on public Internet
- RFC 1918 lists such addresses for private use
- Prefix = 10/8, 172.16/12, 192.168/16
- Example: 10.207.37.234
Address Translation

- **NAT** = Network Address Translation
  Like Dynamic Host Configuration Protocol (DHCP)
- **IP Gateway**: Like Firewall
- **Tunneling**: Encapsulation

Raj Jain
Tunnel

- Tunnel = Encapsulation
- Used whenever some feature is not supported in some part of the network, e.g., multicasting, mobile IP
VPN Tunneling Protocols

- GRE: Generic Routing Encapsulation (RFC 1701/2)
- PPTP: Point-to-point Tunneling Protocol
- L2F: Layer 2 forwarding
- L2TP: Layer 2 Tunneling protocol
- ATMP: Ascend Tunnel Management Protocol
- DLSW: Data Link Switching (SNA over IP)
- IPSec: Secure IP
- Mobile IP: For Mobile users
GRE

<table>
<thead>
<tr>
<th>Delivery Header</th>
<th>GRE Header</th>
<th>Payload</th>
</tr>
</thead>
</table>

- Generic Routing Encapsulation (RFC 1701/1702)
- Generic $\Rightarrow$ X over Y for any X or Y
- Optional Checksum, Loose/strict Source Routing, Key
- Key is used to authenticate the source
- Over IPv4, GRE packets use a protocol type of 47
- Allows router visibility into application-level header
- Restricted to a single provider network $\Rightarrow$ end-to-end
PPTP = Point-to-point Tunneling Protocol

Developed jointly by Microsoft, Ascend, USR, 3Com and ECI Telematics

PPTP server for NT4 and clients for NT/95/98

MAC, WFW, Win 3.1 clients from Network Telesystems (nts.com)
PPTP with ISP Support

- PPTP can be implemented at Client or at NAS
- With ISP Support: Also known as Compulsory Tunnel
- W/O ISP Support: Voluntary Tunnels
PPTP Packets

- Private Network
- PPTP Server
- Internet
- Network Access Server
- Client

Public IP Addressing
- IP/IX/NetBEUI
- Data

Internal IP Addressing
- IP/IX/NetBEUI
- Data

Encrypted

IP
- GRE
- PPP
- IP/IX/NetBEUI
- Data

PPP
- IP
- GRE
- PPP
- IP/IX/NetBEUI
- Data
L2TP

- Layer 2 Tunneling Protocol
- L2F = Layer 2 Forwarding (From CISCO)
- L2TP = L2F + PPTP
  - Combines the best features of L2F and PPTP
- Will be implemented in NT5
- Easy upgrade from L2F or PPTP
- Allows PPP frames to be sent over non-IP (Frame relay, ATM) networks also (PPTP works on IP only)
- Allows multiple (different QoS) tunnels between the same end-points. Better header compression. Supports flow control
IPSec

- Secure IP: A series of proposals from IETF
- Separate Authentication and privacy
- Authentication Header (AH) ensures data integrity and authenticity
- Encapsulating Security Protocol (ESP) ensures privacy and integrity

<table>
<thead>
<tr>
<th>IP Header</th>
<th>AH</th>
<th>ESP</th>
<th>Original IP Header*</th>
<th>Original Data</th>
</tr>
</thead>
</table>

Authenticated — Encrypted

* Optional
**IPSec (Cont)**

- Two Modes: Tunnel mode, Transport mode
- Tunnel Mode $\implies$ Original IP header encrypted
- Transport mode $\implies$ Original IP header removed. Only transport data encrypted.
- Supports a variety of encryption algorithms
- Better suited for WAN VPNs (vs Access VPNs)
- Little interest from Microsoft (vs L2TP)
- Most IPSec implementations support machine (vs user) certificates $\implies$ Any user can use the tunnel
- Needs more time for standardization than L2TP

Raj Jain
SOCKS

- Session layer proxy
- Can be configured to proxy any number of TCP or UDP ports
- Provides authentication, integrity, privacy
- Can provide address translation
- Developed by David Koblas in 1990. Backed by NEC
- Made public and adopted by IETF Authenticated Firewall Traversal (AFT) working group
- Current version v5 in RFC 1928
- Proxy ⇒ Slower performance
- Desktop-to-Server ⇒ Not suitable for extranets
Application Level Security

- Secure HTTP
- Secure MIME
- Secure Electronic Transaction (SET)
- Private Communications Technology (PCT)
RADIUS

- Remote Authentication Dial-In User Service
- Central point for **Authorization, Accounting, and Auditing** data ⇒ **AAA server**
- Network Access servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances
DIAMETER

- Enhanced RADIUS
- Light weight
- Can use both UDP and TCP
- Servers can send unsolicited messages to Clients
  \[\Rightarrow\] Increases the set of applications
- Support for vendor specific Attribute-Value-Pairs (AVPs) and commands
- Authentication and privacy for policy messages
Quality of Service (QoS)

- Resource Reservation Protocol (RSVP) allows clients to reserve bandwidth
- Need routers with proper scheduling: IP Precedence, priority queueing, Weighted Fair Queueing (WFQ)
- All routers may not support RSVP
- Even more difficult if multiple ISPs
VPN Support with MPLS

- Multiprotocol Label Switching
- Allows packets to be switched using labels (tags)
  \[\implies\] Creates connections across a network
- Labels contain Class of Service
VPN allows secure communication on the Internet

Three types: WAN, Access, Extranet

Key issues: address translation, security, performance

Layer 2 (PPTP, L2TP), Layer 3 (IPSec), Layer 5 (SOCKS), Layer 7 (Application level) VPNs

RADIUS allows centralized authentication server

QoS is still an issue $\Rightarrow$ MPLS
References

- For a detailed list of references, see
  
  http://www.cis.ohio-state.edu/~jain/refs/refs_vpn.htm

Raj Jain
Final Review: Hot Facts

1. Networking is critical and growing exponentially.
2. Networking is the key to productivity
3. IP switching allows some IP packets to go through an ATM network without reassembly at intermediate routers.
4. MPLS uses circuit numbers in the header to switch IP packets
5. MPLS works on ATM and non-ATM networks.

Raj Jain
6. Gigabit Ethernet will compete with ATM for campus backbone and desktop

7. Gigabit Ethernet will support both shared and full-duplex links

8. Most gigabit Ethernet links will be full-duplex

9. H.323 is the conferencing standard designed for LANs and best effort networks.

10. Gatekeepers provide bandwidth management while Gateway provide protocol translation.

11. VPNs allow private networks over public Internet
Thank You!

Raj Jain