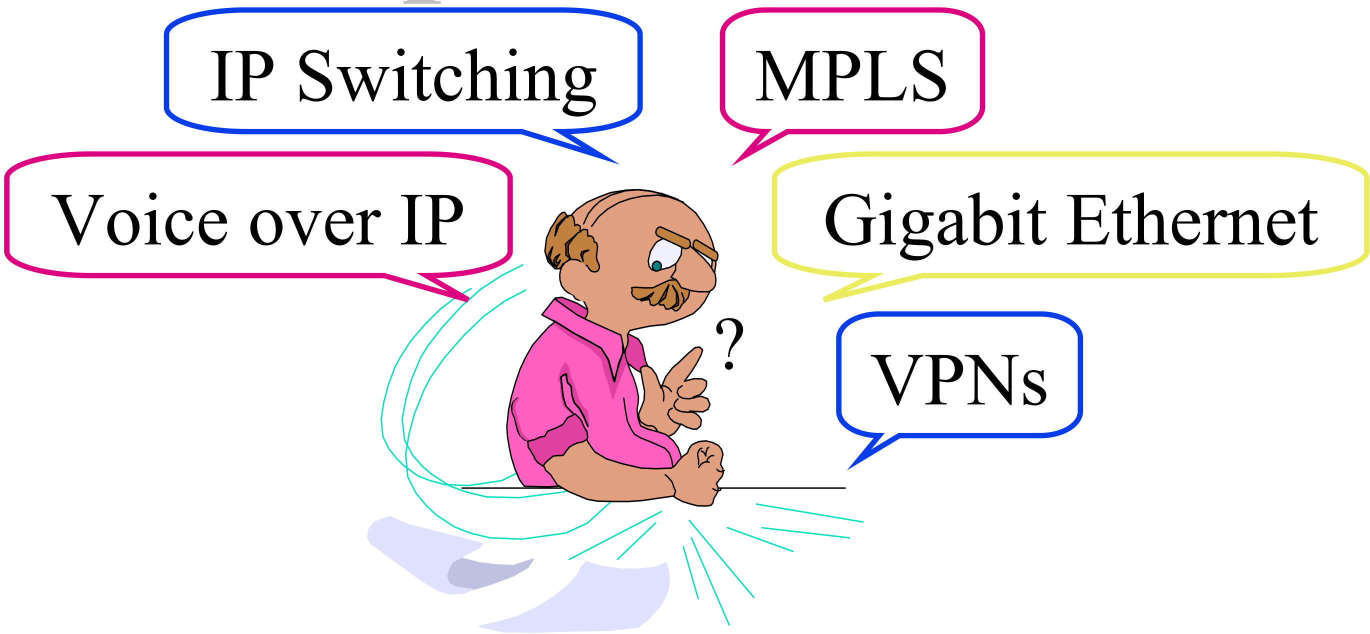
Hot Topics in Networking



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

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

- 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.
  $\Rightarrow$ 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/

Future

White House Astrologer

Joan Quigly

All I want you to tell me is what will be the networking technology in the year 2000.

Raj Jain

- 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)

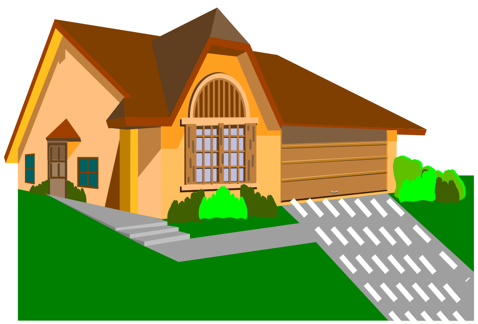
Raj Jain

Cave Persons of 2050

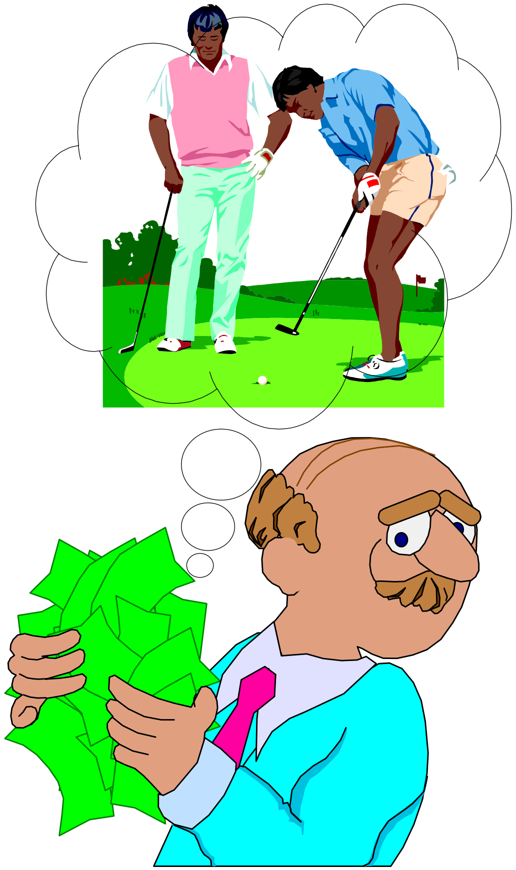
Raj Jain

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 = 1_2 year or 10_2 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
  $\Rightarrow$ Robust and high-bandwidth encoding techniques
- High-speed Wireless = More than 10 bit/Hz
  28.8 kbps on 30 kHz cellular $\Rightarrow$ 1 bit/Hz
- Traffic management, quality of service, multicasting:
  - Ethernet LANs, IP networks, ATM Networks
- Mobility
- Large network management Issues.

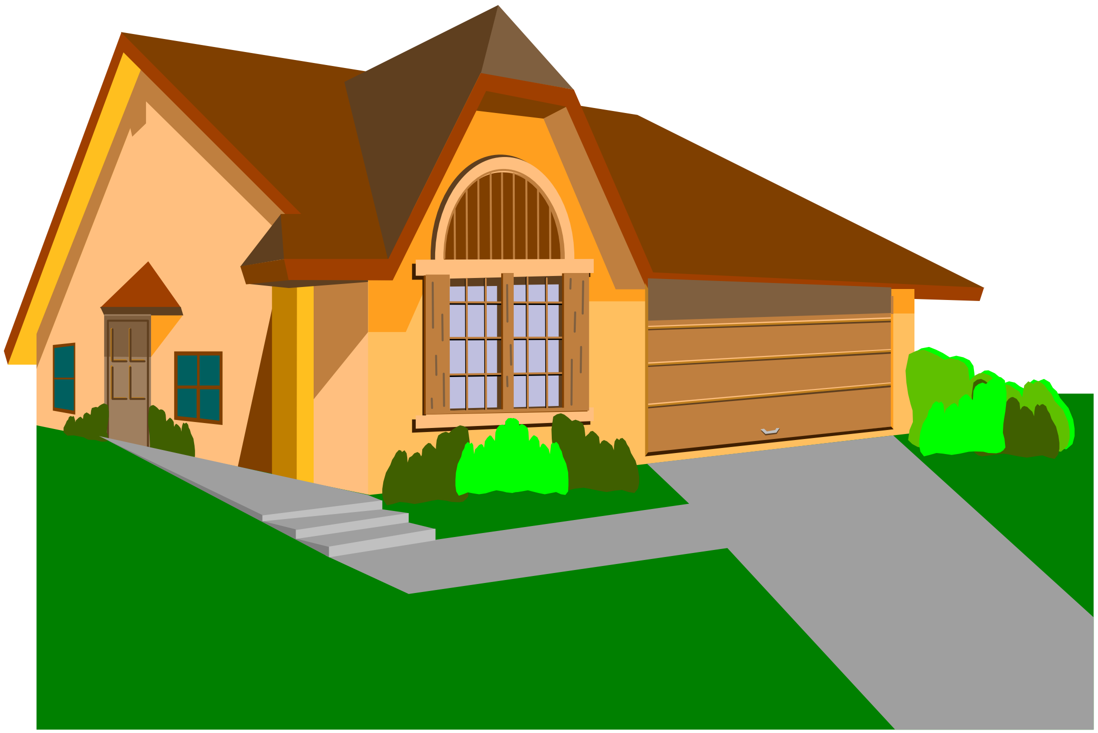
Research Topics (Cont)

- 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

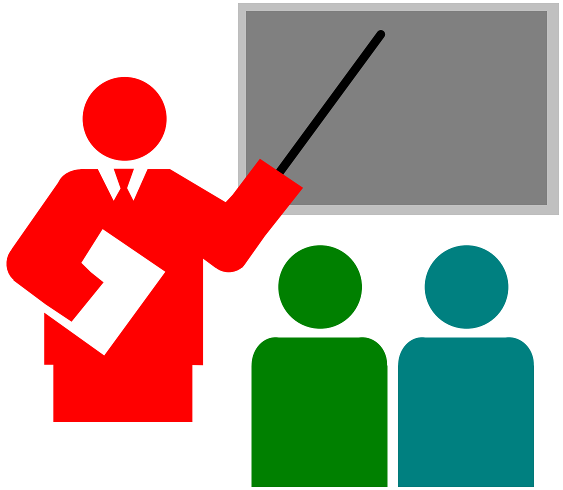
Old House vs New House



- New needs:
  Solution 1: Fix the old house (cheaper initially)
  Solution 2: Buy a new house (pays off over a long run)

Raj Jain

Summary



- 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

Raj Jain

Key References

- See http://www.cis.ohio-state.edu/~jain/refs/ref_trnd.htm
- "The Next 50 years," Special issue of Communications of the ACM, Feb 1997.
- D. Tapscott, "The Digital Economy: Promise and Peril in the Age of Networked Intelligence," McGraw-Hill, 1995.
- T. Lewis, "The Next $10{,}000_2$ years," IEEE Computer, April/May 1996

IP Switching and Label Switching

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

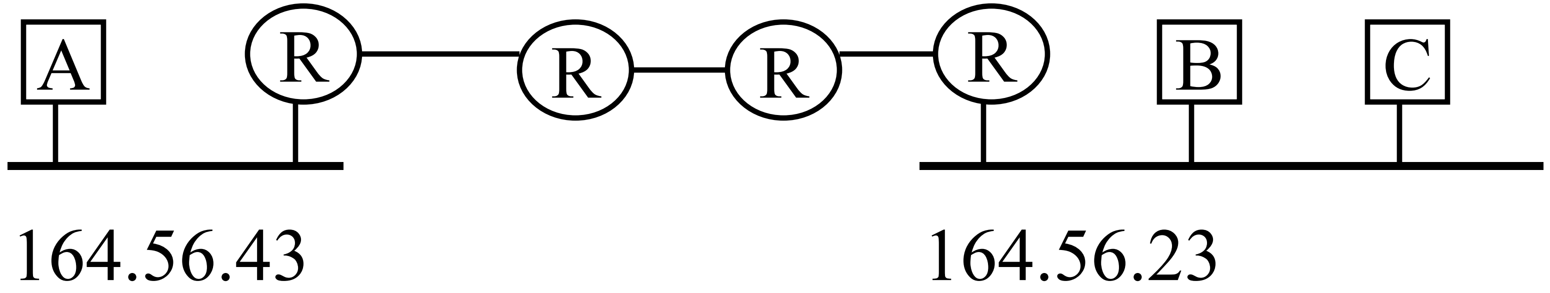
http://www.cis.ohio-state.edu/~jain/

- Switching vs routing
- IP Switching (Ipsilon)
- Tag Switching (CISCO)
- Multi-protocol label switching

Raj Jain

IP Forwarding:Fundamentals

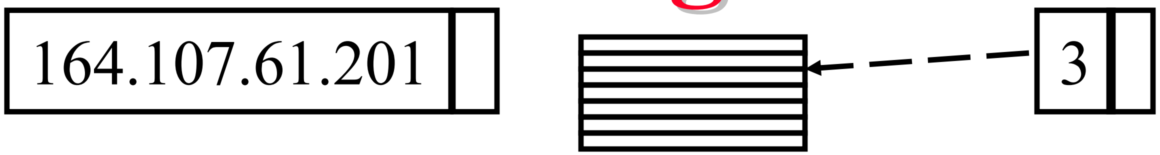
To: 164.56.23.34	From: 164.56.43.96	



- 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 <u>1 614 999 2345</u>.00.00.AA....

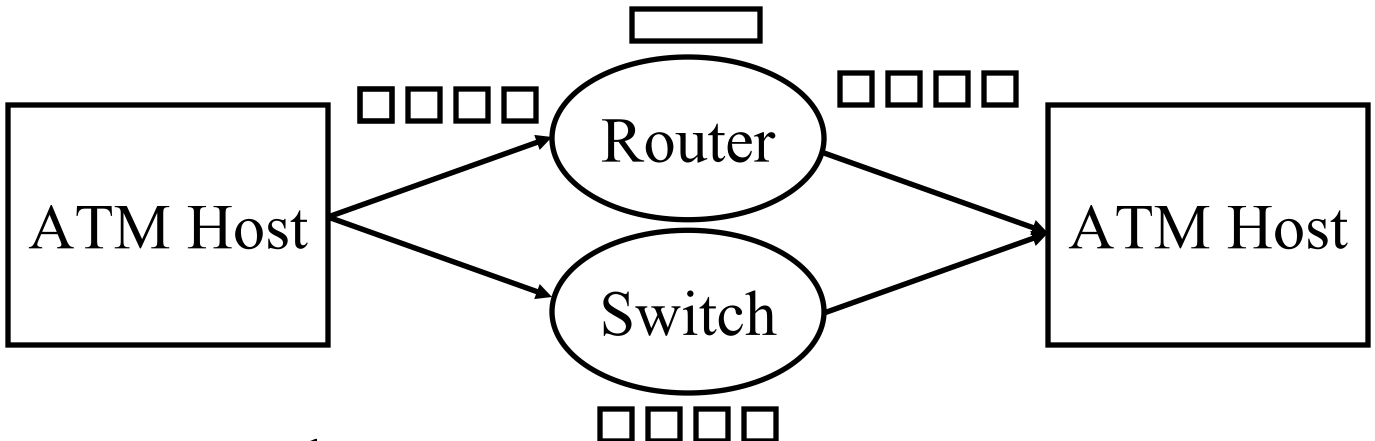
Raj Jain

Routing vs Switching



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

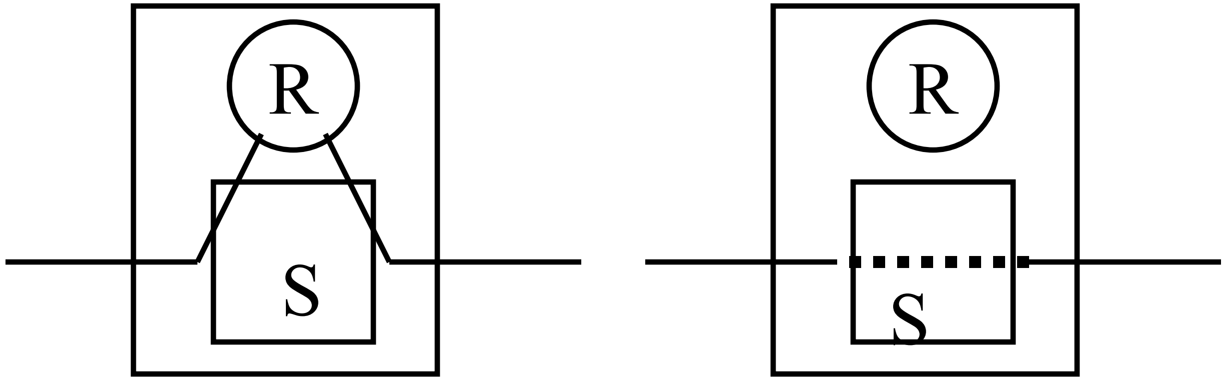


On ATM networks:

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

IP Switching

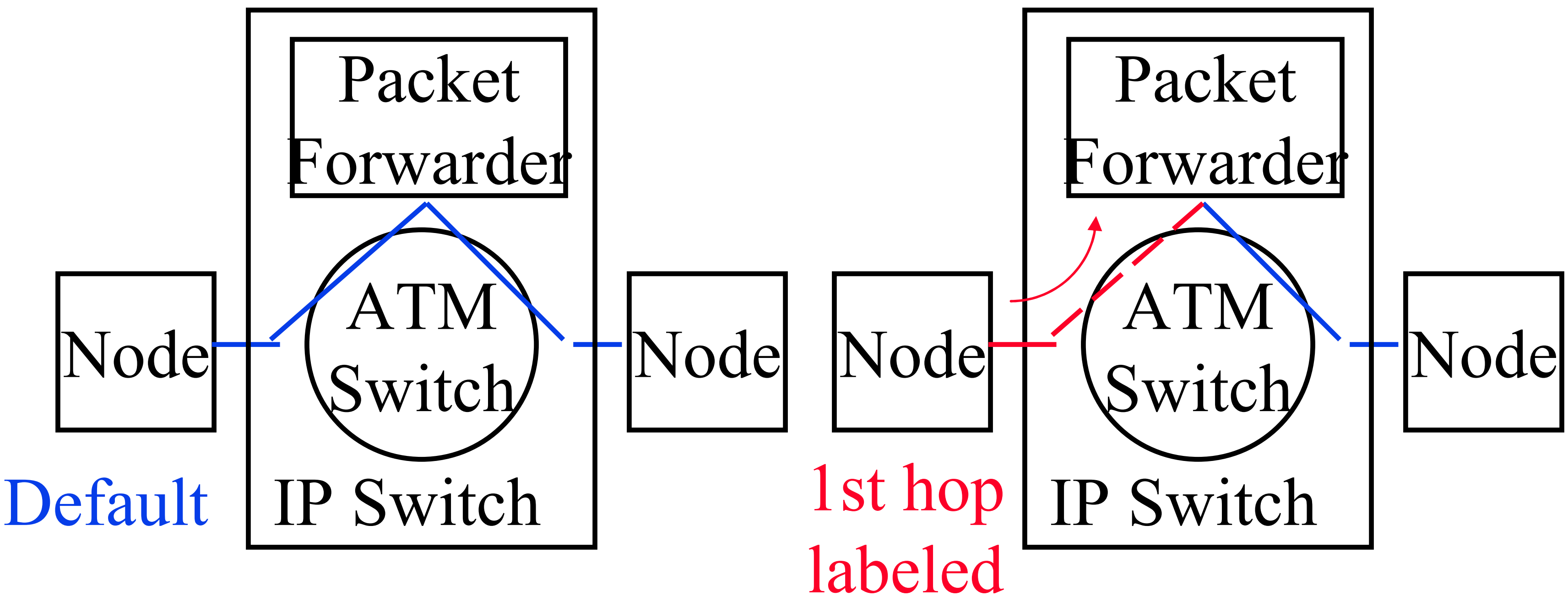
- Developed by Ipsilon
- Routing software in every ATM switch in the network
- Initially, packets are reassembled by the routing software and forwarded to the next hop
- Long term flows are transferred to separate VCs. Mapping of VCIs in the switch ⇒ No reassembly



Raj Jain

IP Switching: Steps 1-2

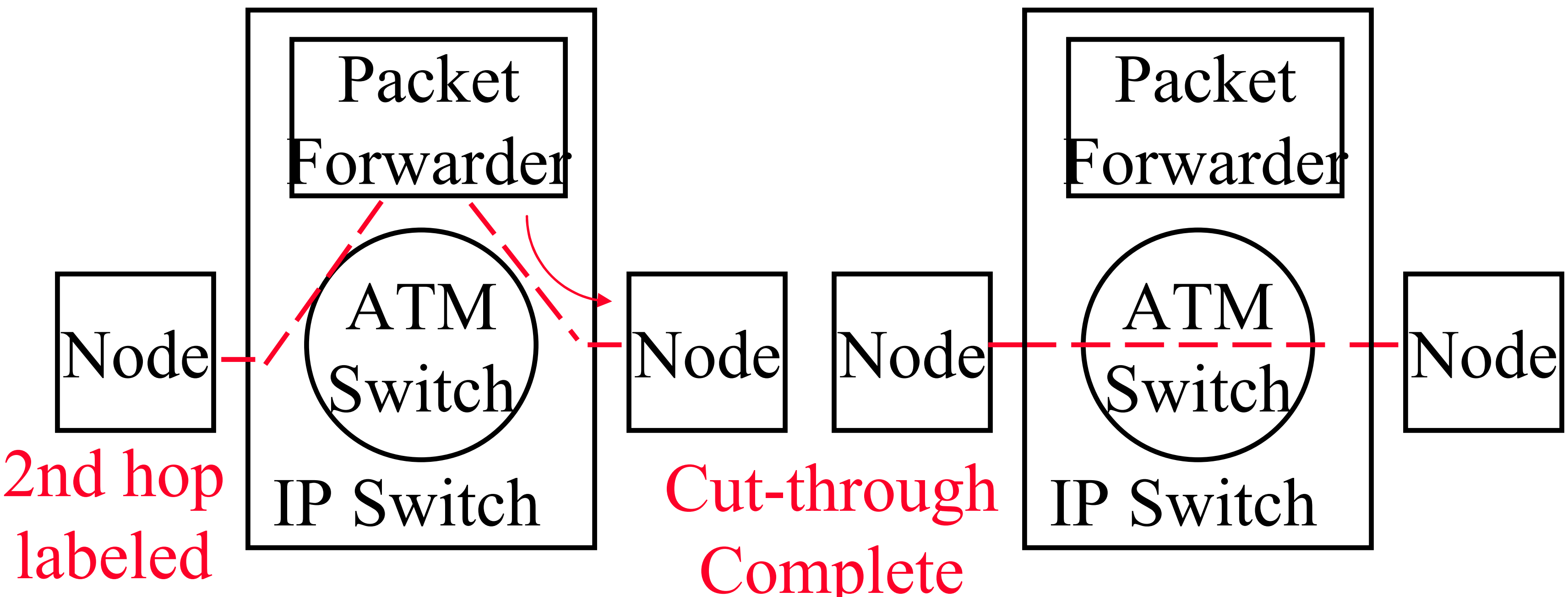
- If a flow is deemed to be "flow oriented", the node asks the upstream node to set up a separate VC.
- Downstream nodes may also ask for a new VC.



Raj Jain

IP Switching: Steps 3, 4

- After both sides of a flow have separate VCs, the router tells the switch to register the mapping for cut-through



Raj Jain

IP Switching (Cont)

- 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

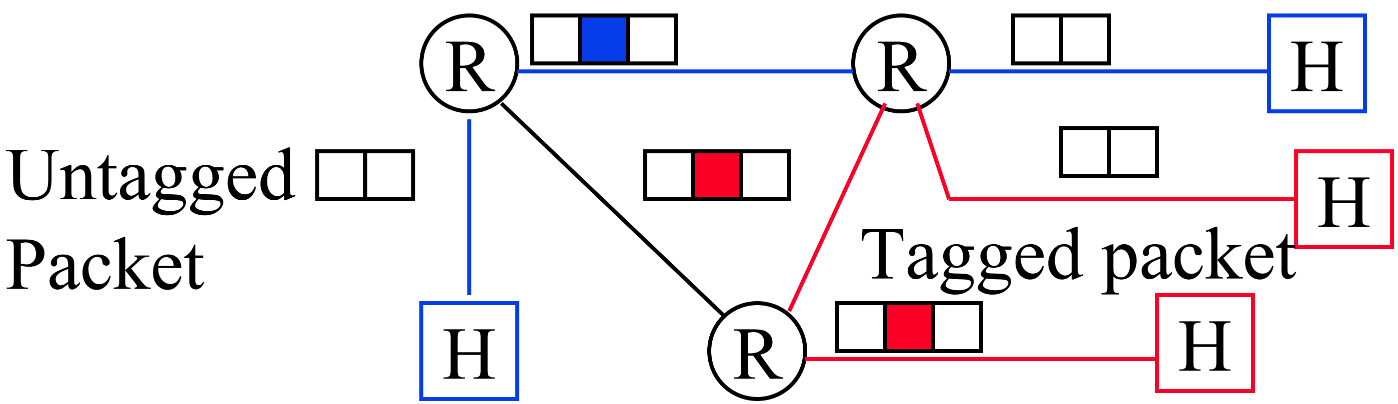
- VCI field is used as ID.
  VPI/VCI change at switch
  $\Rightarrow$ Must run on **every** ATM switch
  $\Rightarrow$ non-IP switches not allowed between IP switches
  $\Rightarrow$ Subnets limited to one switch
- Cannot support VLANs
- Scalability: Number of VC $\geq$ Number of flows.
  $\Rightarrow$ **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

L2 Header	**Tag**	

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



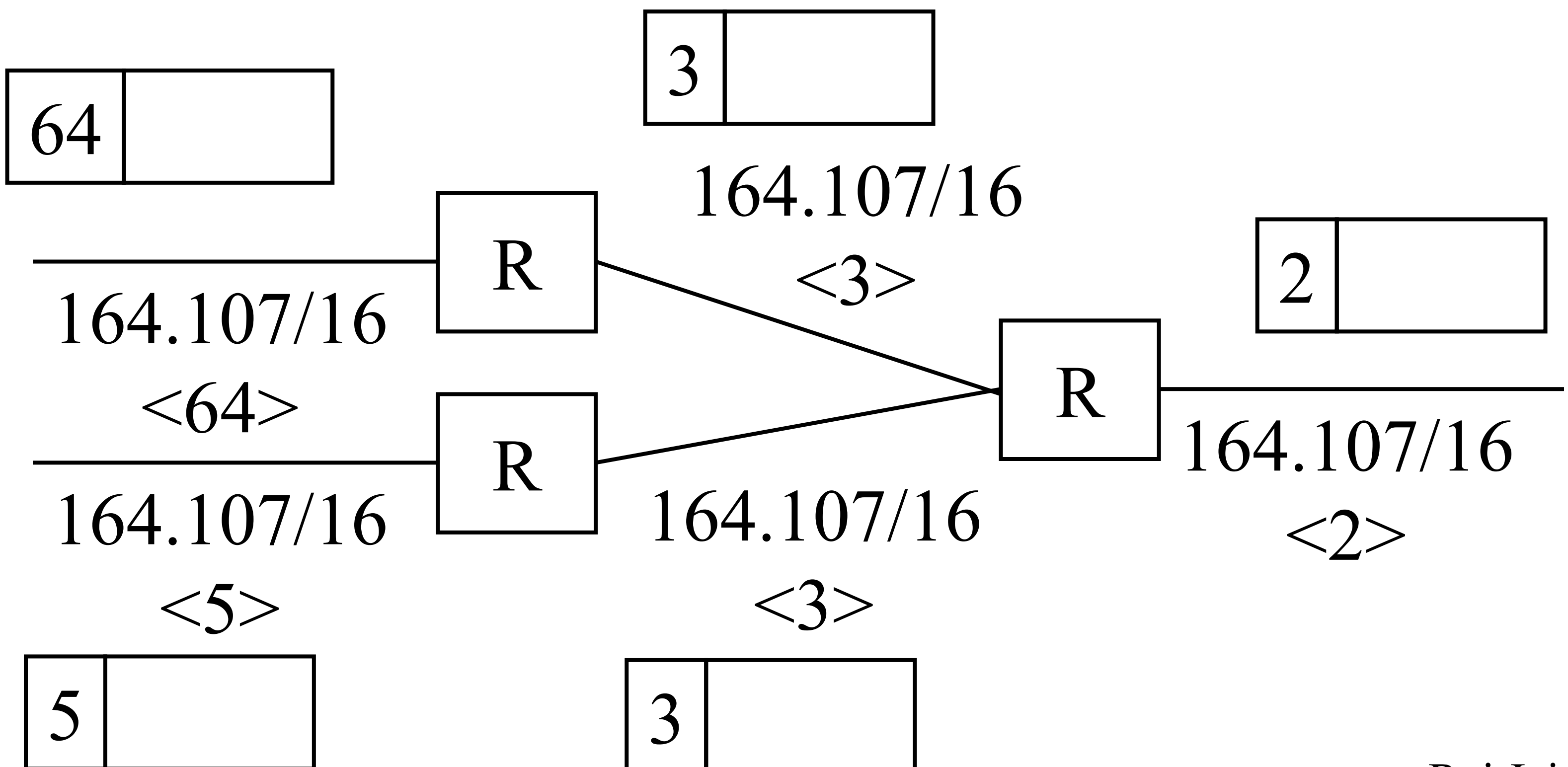
Raj Jain

Tag Switching (Cont)

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

Tag Switching (Cont)

- One VC per routing table entry



Raj Jain

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

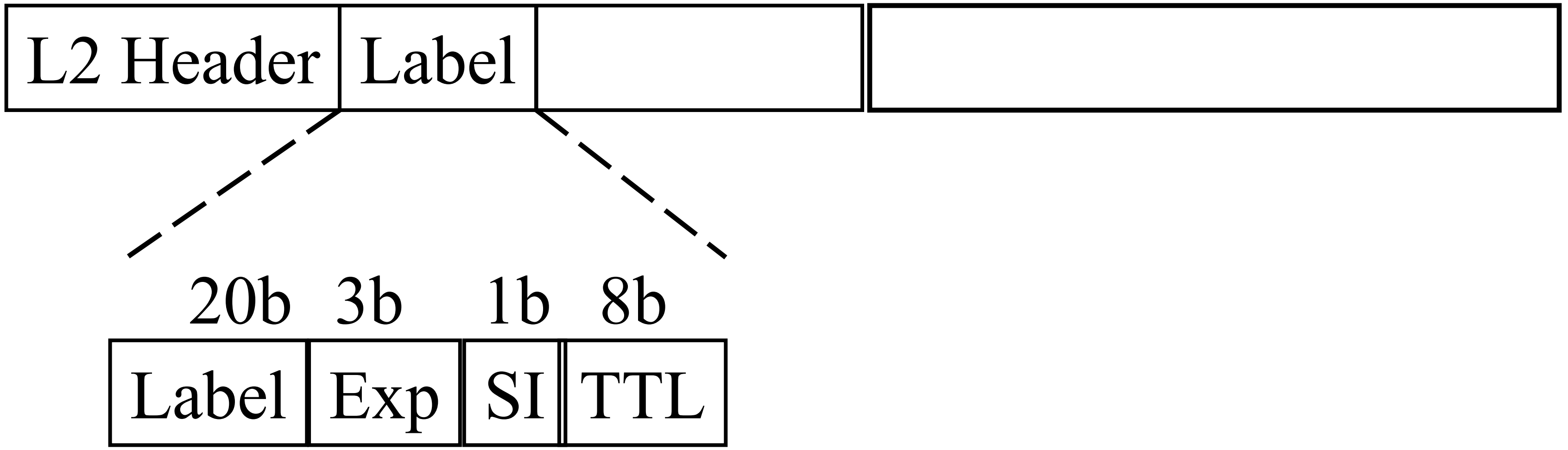
- Multiprotocol Label Switching
- IETF working group to develop switched IP forwarding
- Initially focused on IPv4 and IPv6. Technology extendible to other L3 protocols.
- Not specific to ATM. ATM or LAN.
- Not specific to a routing protocol (OSPF, RIP, ...)
- Optimization only. Labels do not affect 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
  $\Rightarrow$ 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



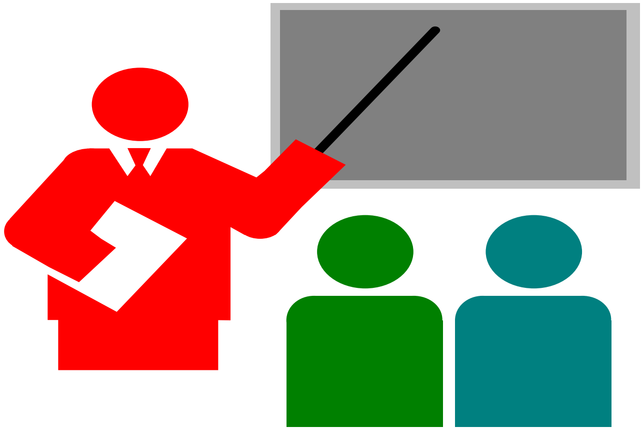
Raj Jain

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

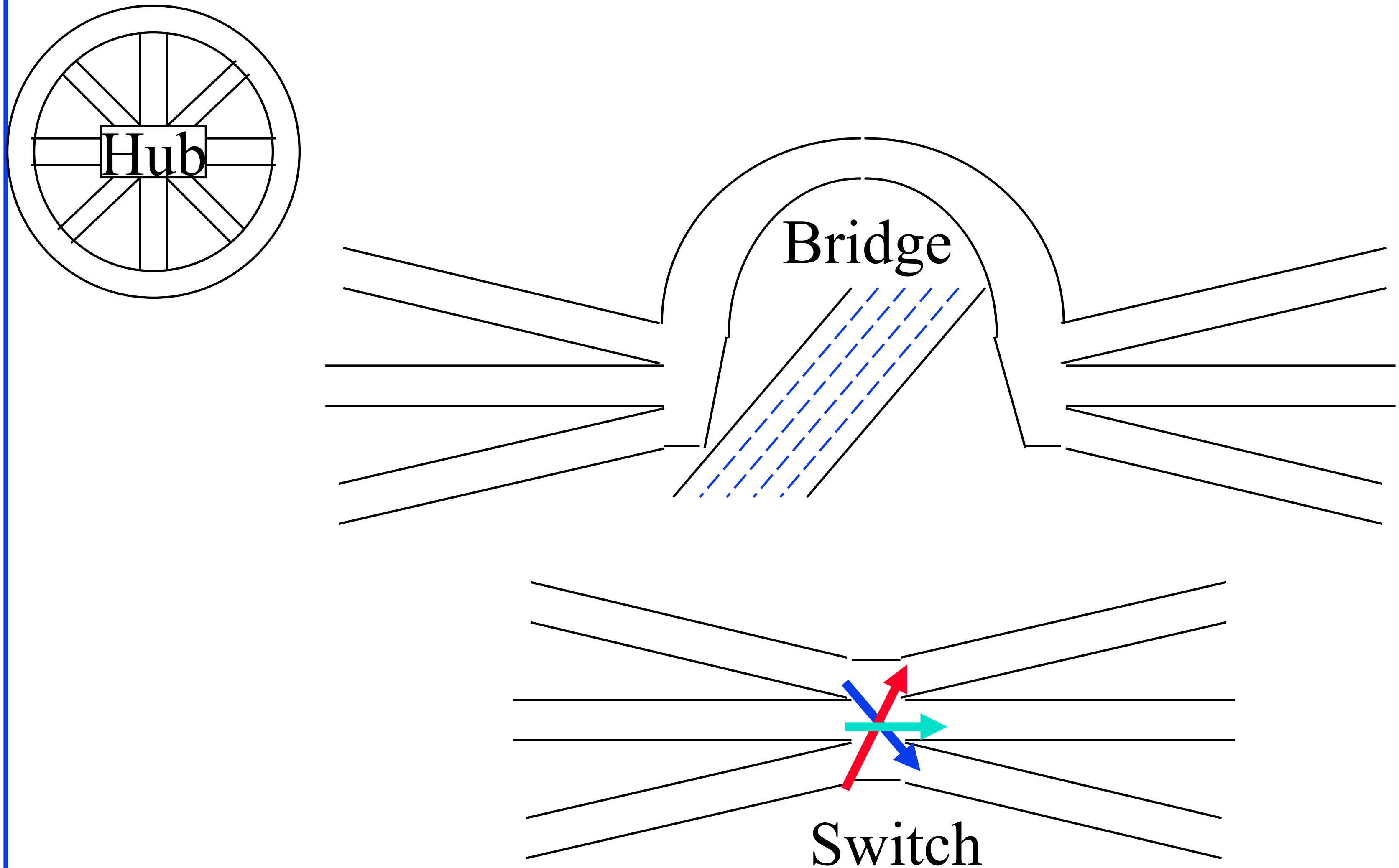
- See **http://www.cis.ohio-state.edu/~jain/refs/ipoa_ref.htm** and **http://www.cis.ohio-state.edu/~jain/refs/ipsw_ref.htm**
- Multiprotocol Label Switching (mpls) working group at IETF. Email: mpls-request@cisco.com

Gigabit Ethernet

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

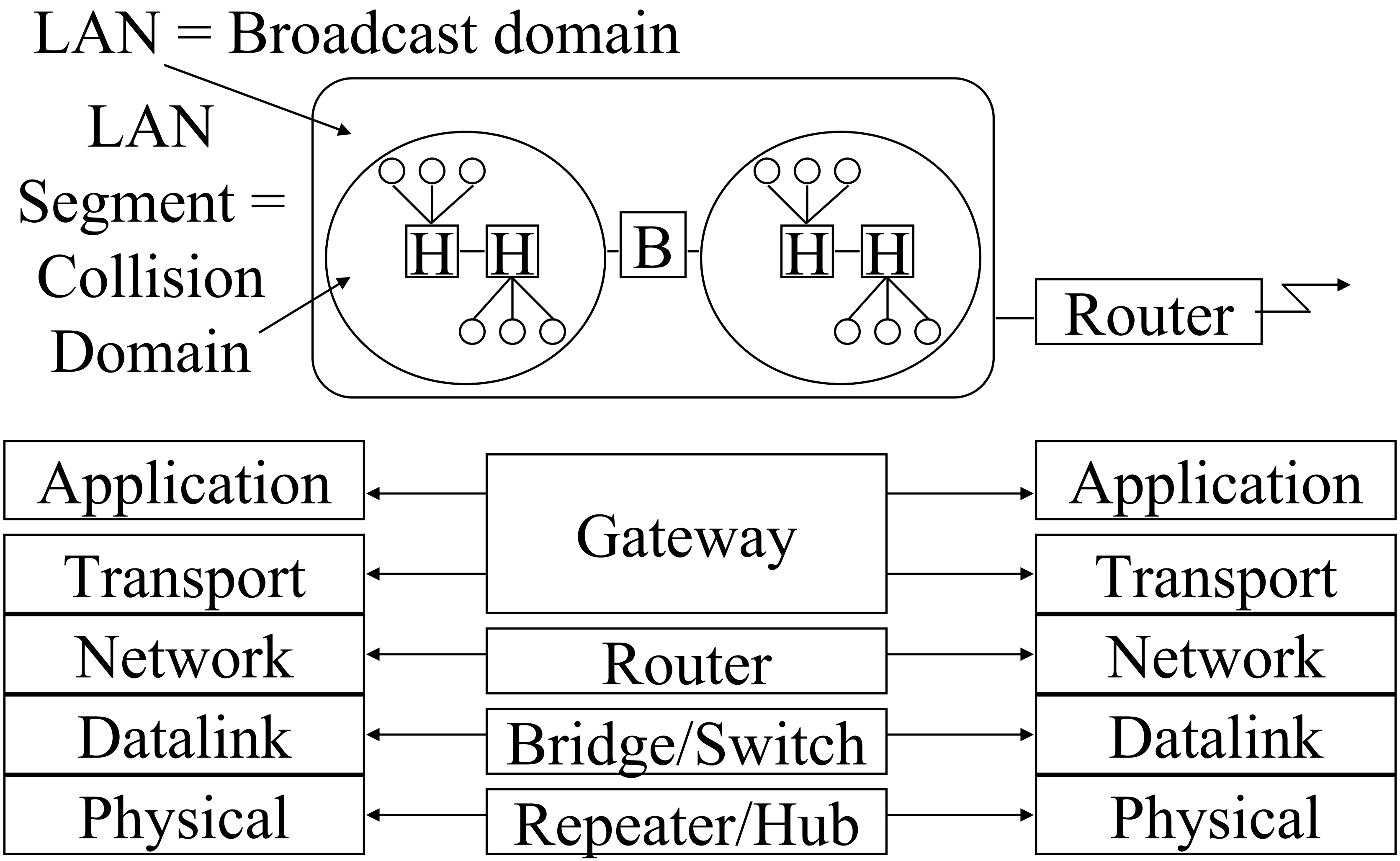
- LAN Interconnection Devices and Full duplex links
- Distance-Bandwidth Principle
- 10 Mbps to 100 Mbps
- Gigabit PHY and MAC Issues
- ATM vs Gigabit Ethernet
- 1000BASE-T for 1 Gbps over UTP5
- Link aggregation

Hub vs Bridge vs Switch



Raj Jain

Interconnection Devices

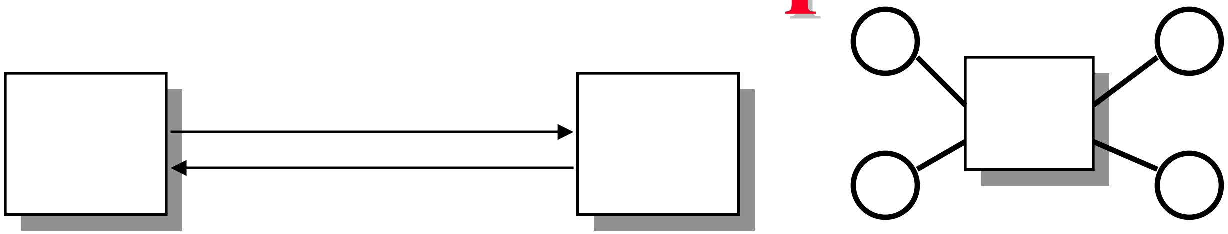


Interconnection Devices

- **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.”
- **Router:** Network layer device. IP, IPX, AppleTalk. Does not propagate MAC multicasts.
- **Switch**: Multiport bridge with parallel paths

These are functions. Packaging varies.

Full-Duplex LANs

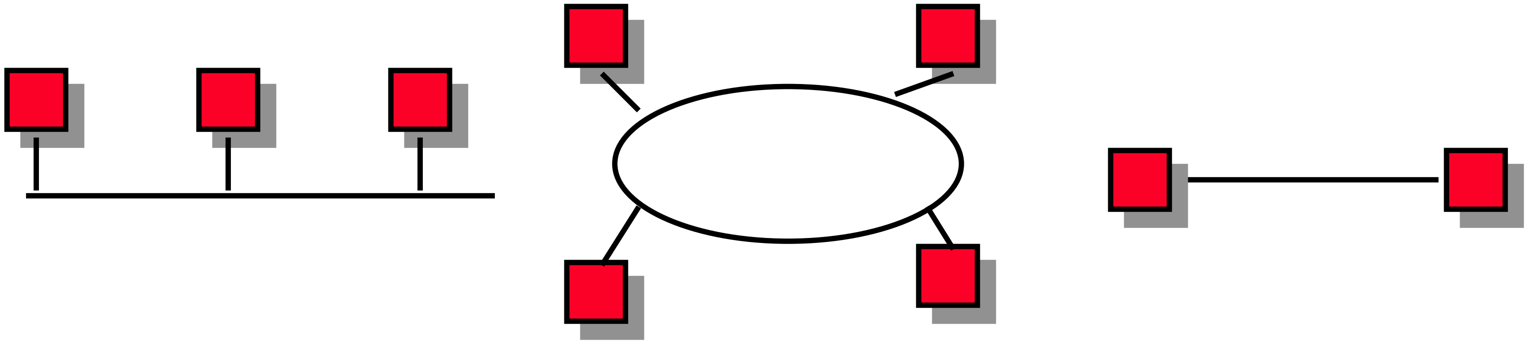


- Uses point-to-point links between TWO nodes
- Full-duplex bi-directional transmission
  Transmit any time
- Not yet standardized in IEEE 802
- Many switch/bridge/NICs with full duplex
- No collisions $\Rightarrow$ 50+ Km on fiber.
- Commonly used between servers and switches or between switches

The Magic Word α

Raj Jain

Distance-B/W Principle

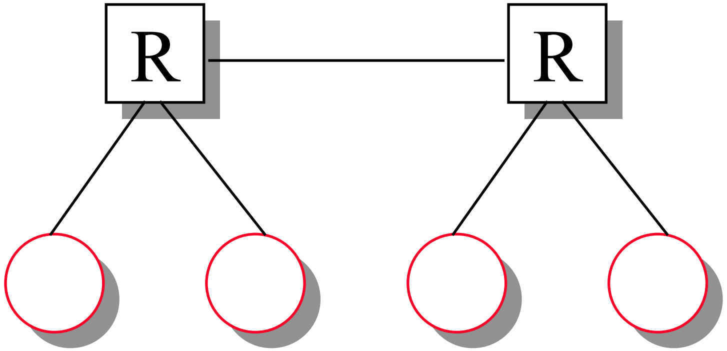


- Efficiency = Max throughput/Media bandwidth
- Efficiency is a non-increasing function of α
  α = Propagation delay /Transmission time
  = (Distance/Speed of light)/(Transmission size/Bits/sec)
  = Distance$\times$Bits/sec/(Speed of light)(Transmission size)
- Bit rate-distance-transmission size tradeoff.
- 100 Mb/s $\Rightarrow$ Change distance or frame size

Raj Jain

Ethernet vs Fast Ethernet

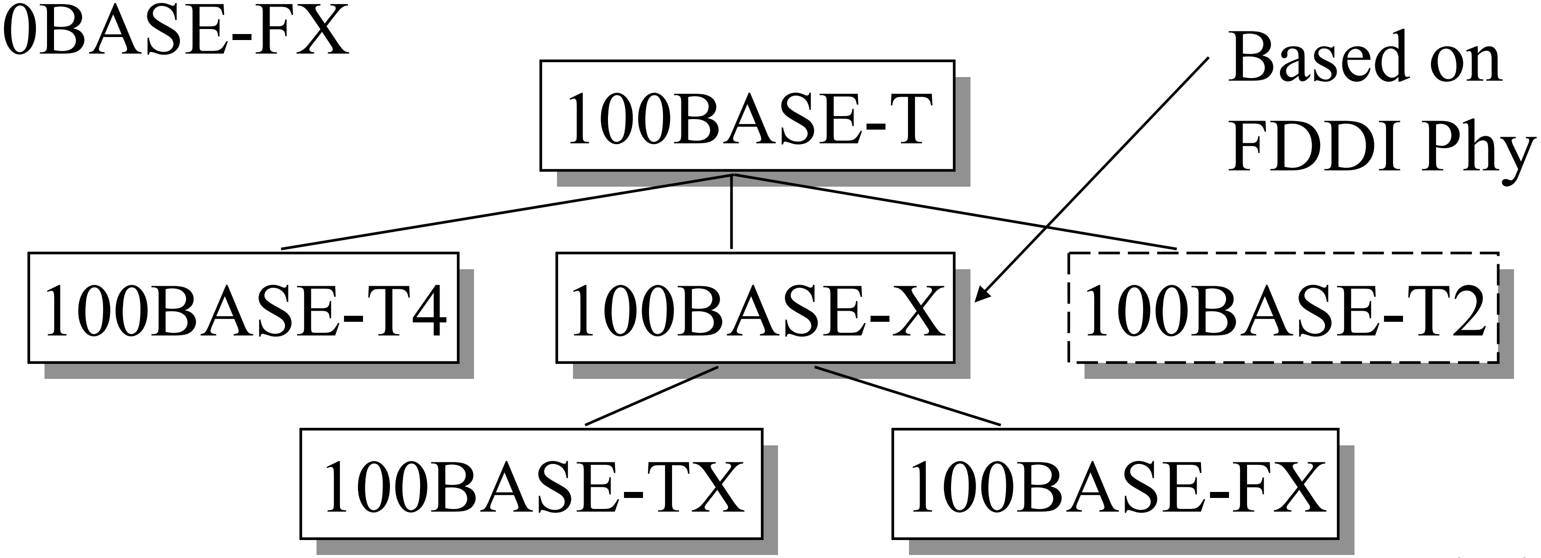
	Ethernet	Fast Ethernet
Speed	10 Mbps	100 Mbps
MAC	CSMA/CD	CSMA/CD
Network diameter	2.5 km	205 m
Topology	Bus, star	Star
Cable	Coax, UTP, Fiber	UTP, Fiber
Standard	802.3	802.3u
Cost	X	2X



Raj Jain

Fast Ethernet Standards

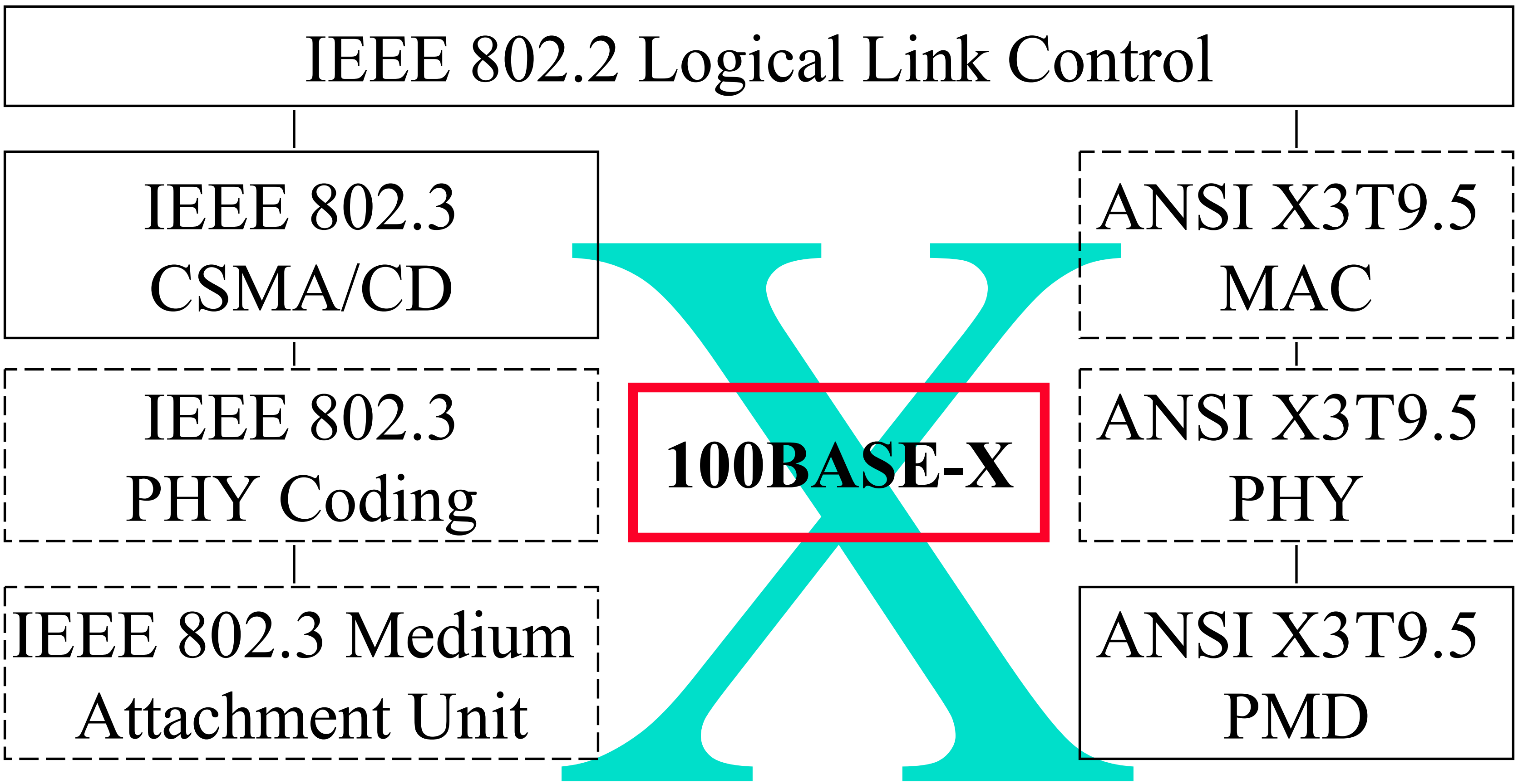
- **100BASE-T4:** 100 Mb/s over 4 pairs of CAT-3, 4, 5
- **100BASE-TX:** 100 Mb/s over 2 pairs of CAT-5, STP
- **100BASE-FX:** 100 Mbps CSMA/CD over 2 fibers
- **100BASE-X:** 100BASE-TX or 100BASE-FX
- **100BASE-T:** 100BASE-T4, 100BASE-TX, or 100BASE-FX



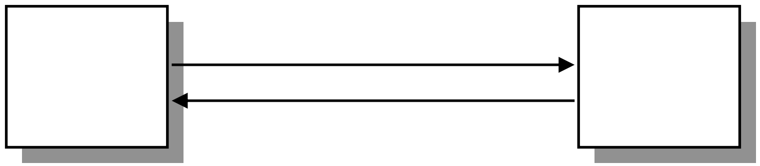
Raj Jain

100 BASE-X

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



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

Raj Jain

Gigabit Ethernet

- Being standardized by 802.3z
- Project approved by IEEE in June 1996
- 802.3 meets every three months ⇒ Too slow
  ⇒ 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

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 ⇒ Fiber Channel PHY
  ⇒ Shorter time to market
- Decision: 1,000,000,000 bps ⇒ 1.25 GBaud PHY
- Not multiple speed ⇒ Sub-gigabit Ethernet rejected
- 1000Base-X

Physical Media

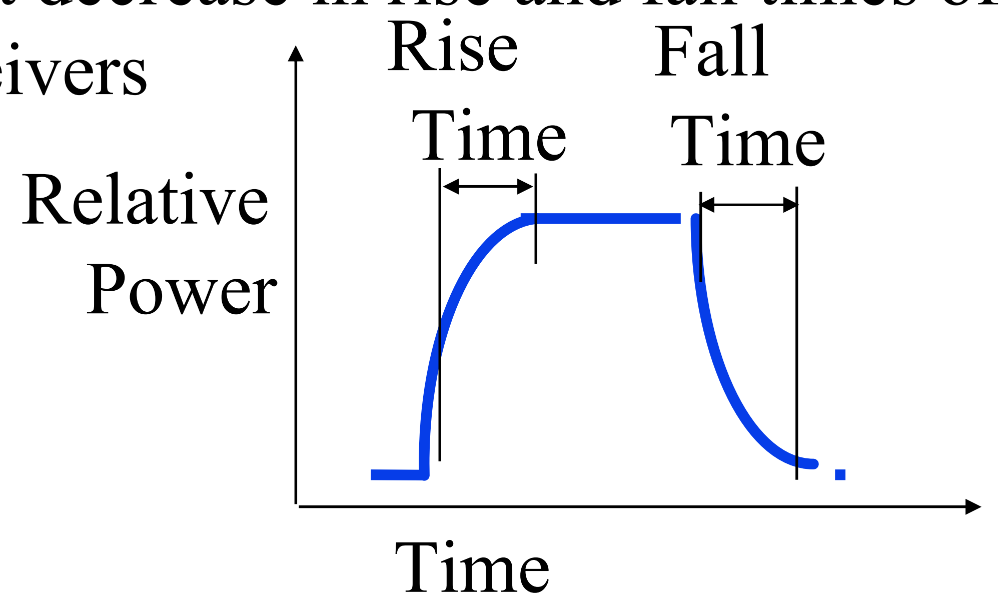
- Unshielded Twisted Pair (UTP-5): 4-pairs
- Shielded Twisted Pair (STP)
- Multimode Fiber: 50 μm and 62.5 μm
  - Use CD lasers
- Single-Mode Fiber
- Bit Error Rate better than 10^{-12}

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

PHY Issues

- Fiber Channel PHY:
  100 MBps = 800 Mbps
  ⇒ 1.063 GBaud using 8b10b
- Changes to get 500 m on 62.5-μm multimode fiber
  - Modest decrease in rise and fall times of the transceivers



Raj Jain

- 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
    $\Rightarrow$ Needed for campus backbone

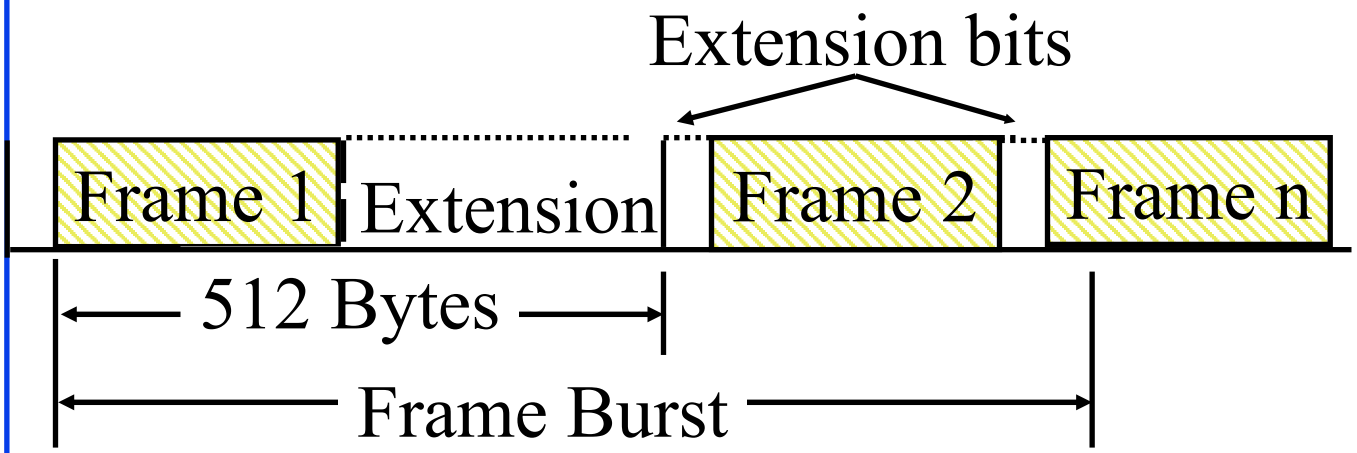
Media Access Control Issues

- Carrier Extension
- Frame Bursting
- Buffered Distributor

Carrier Extension

- 10 Mbps at 2.5 km $\Rightarrow$ Slot time = 64 bytes
- 1 Gbps at 200 m $\Rightarrow$ 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

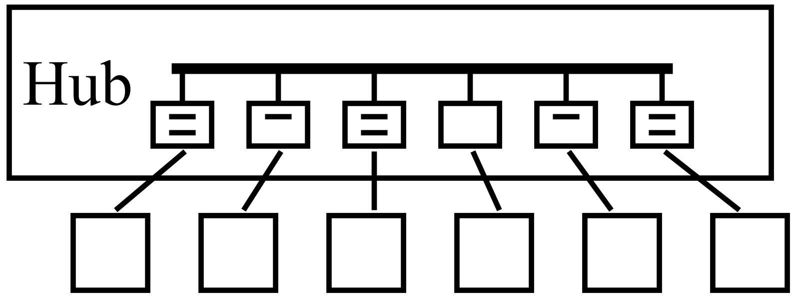
Frame Bursting



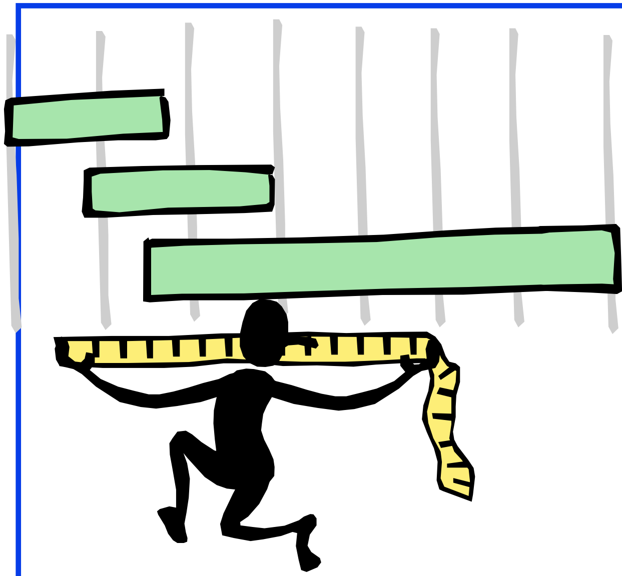
- Don't give up the channel after every frame
- After the slot time, continue transmitting additional frames (with minimum inter-frame gap)
- Interframe gaps are filled with extension bits
- No no new frame transmissions after 8192 bytes
- Three times more throughput for small frames

Raj Jain

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
- Status: Approved in July 1998.

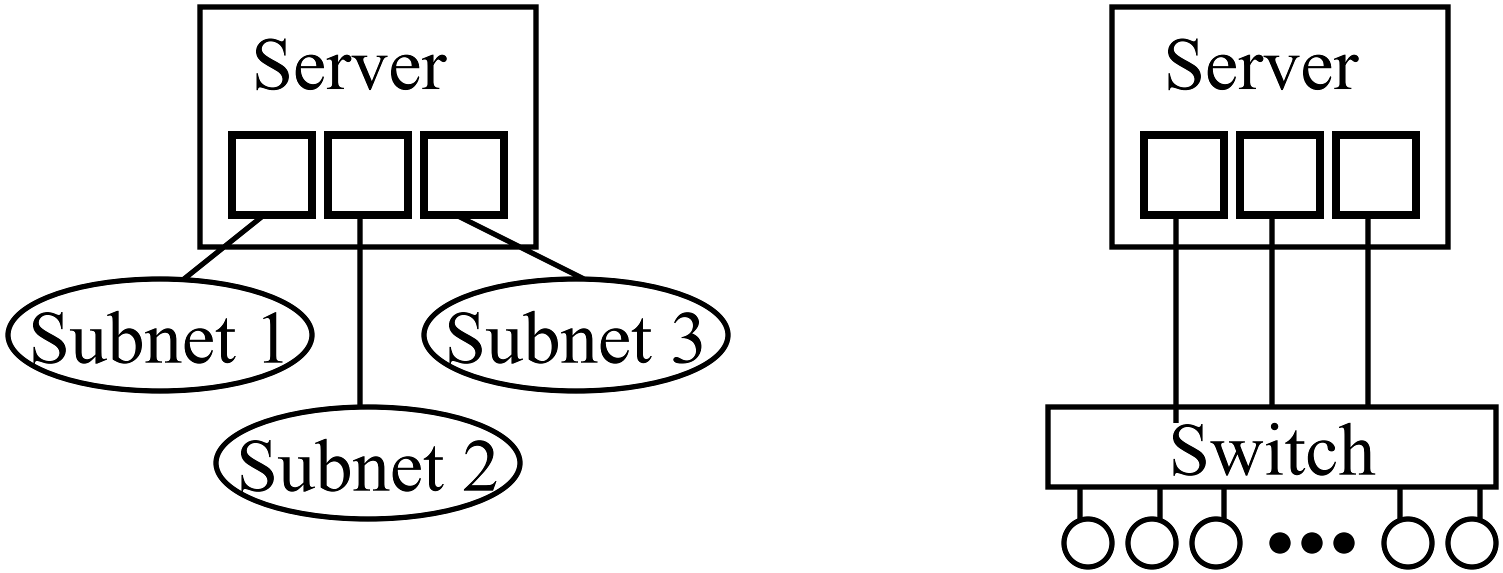
1000Base-X

- 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
  $\Rightarrow$ Network diameter of 200 m
- 250 Mbps/pair full duplex DSP based PHY
  $\Rightarrow$ 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 $\Rightarrow$ 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.

Design Parameter Summary

Parameter	10 Mbps	100 Mbps	1 Gbps
Slot time	512 bt	512 bt	4096 bt
Inter Frame Gap	9.6 μs	0.96 μs	0.096 μs
Jam Size	32 bits	32 bits	32 bits
Max Frame Size	1518 B	1518 B	1518 B
Min Frame Size	64 B	64 B	64 B
Burst Limit	N/A	N/A	8192 B

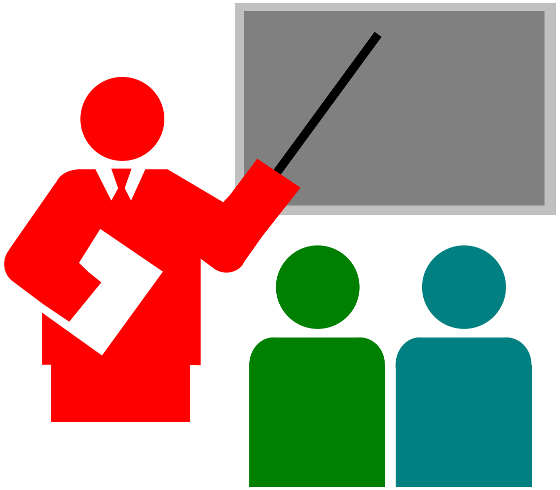
- bt = bit time

ATM vs Gb Ethernet

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

Raj Jain

Summary

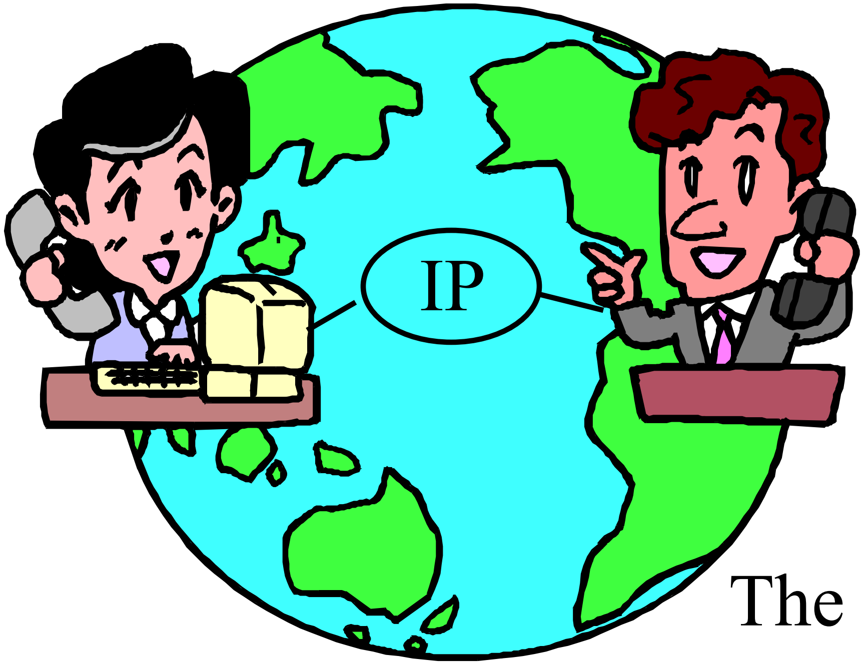


- Gigabit Ethernet runs at 1000 Mbps
- Both shared and full-duplex links
- Fully compatible with current Ethernet
- 1000BASE-T allows 1000 Mbps over 100m of UTP5
- Link aggregation will allow multiple links in parallel

References

- For a detailed list of references, see http://www.cis.ohio-state.edu/~jain/refs/gbe_refs.htm
- Gigabit Ethernet Overview, http://www.cis.ohio-state.edu/~jain/cis788-97/gigabit_ethernet/index.htm
- ”100BASE-X: MAC, PHY, Repeater, and Management Parameters for 1000 Mb/s Operation,” IEEE 802.3z, June 25, 1998.
- IEEE 802.3z Gigabit Task force, http://grouper.ieee.org/groups/802/3/z/index.html
- Gigabit Ethernet Consortium 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/

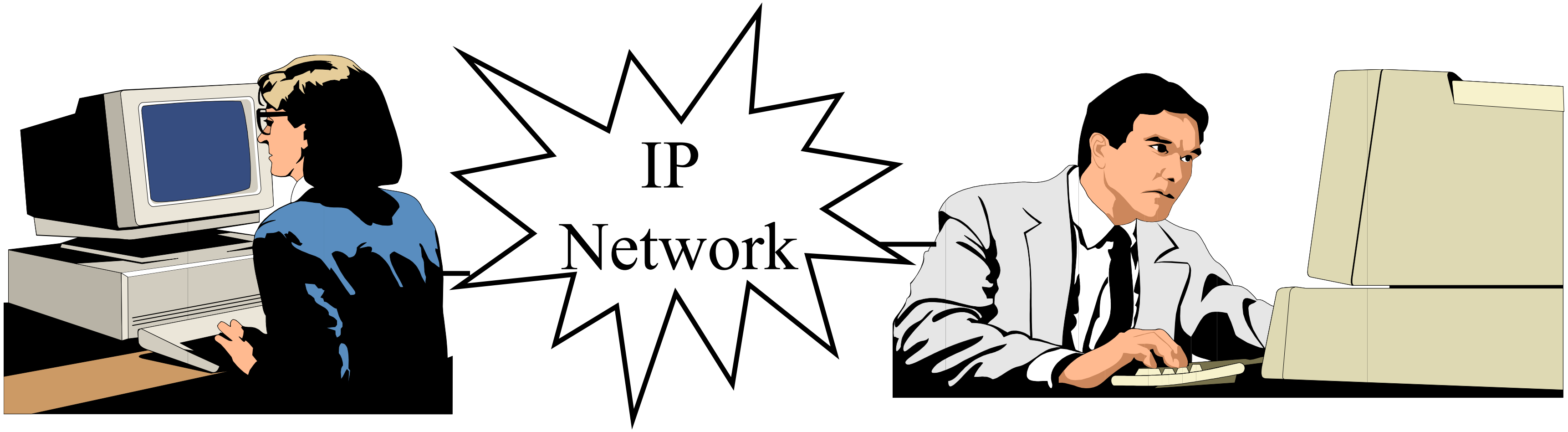
- Voice over IP: Why?
- Sample Products and Services
- 13 Technical Issues
- 4 Other Issues
- H.323 Standard
- Session Initiation Protocol (SIP)

Raj Jain

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]
- US VOIP service will grow from $30M in 1998 to $2B in 2004 [Forester Research]
  $2B in 2001 and $16B by 2004 [Frost & Sullivan]

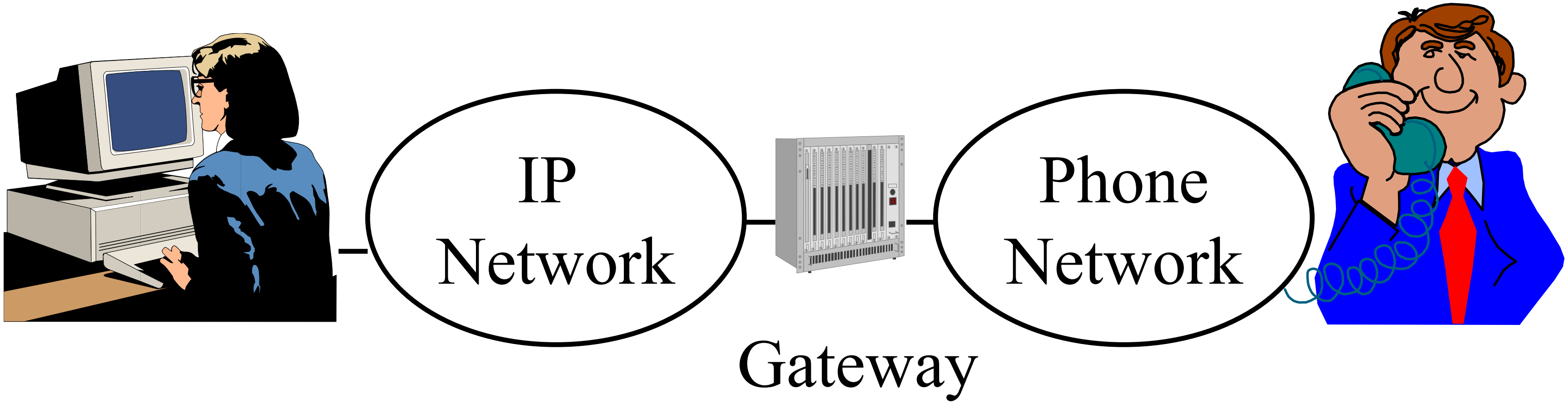
Scenario 1: PC to PC



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

Raj Jain

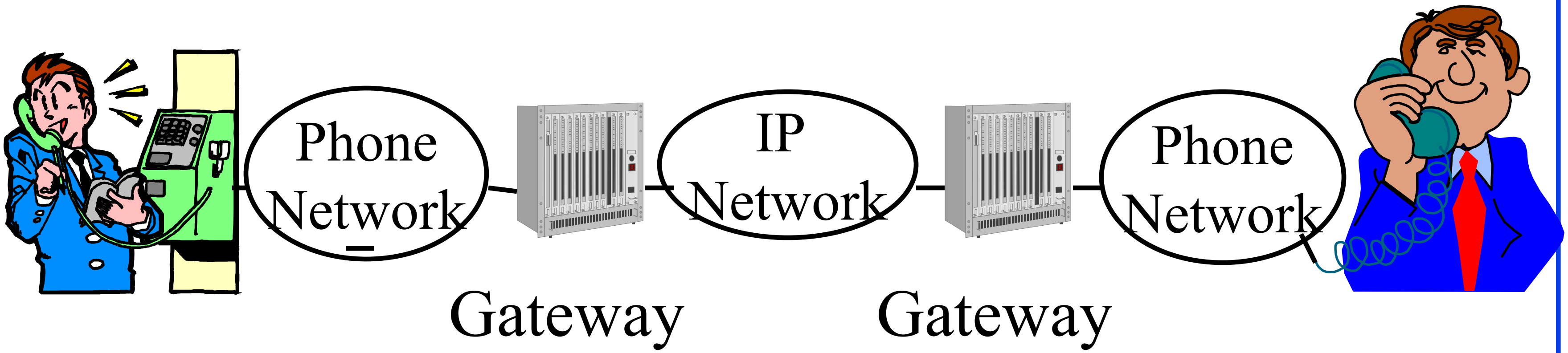
Scenario 2: PC to Phone



- Need a gateway that connects IP network to phone network (Router to PBX)

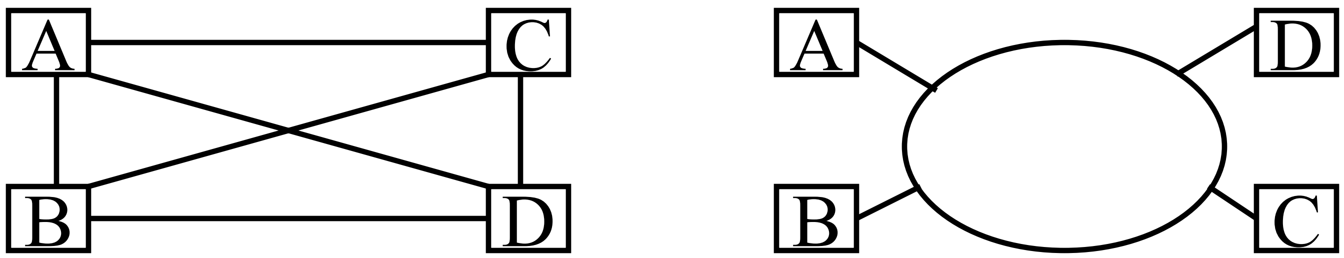
Raj Jain

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-insensitve charge
- Easy alternate routing ⇒ More reliability
- No 64kbps bandwidth limitation
  ⇒ Easy to provide high-fidelity voice

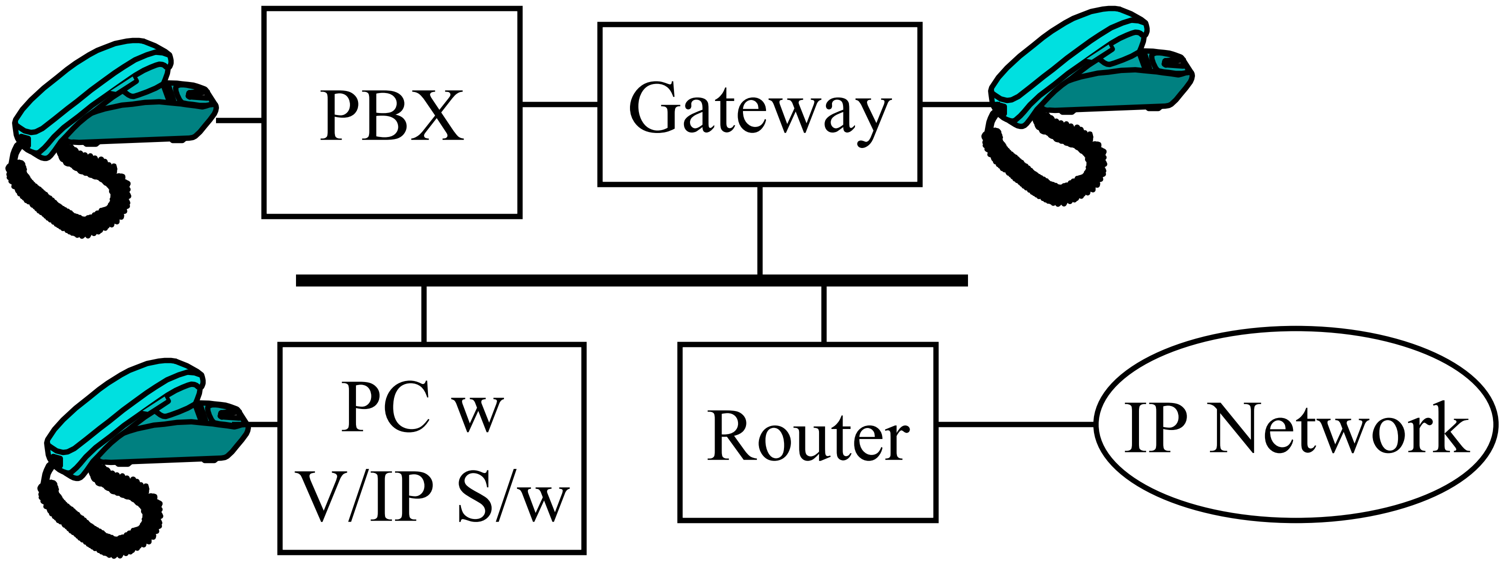
Applications

- 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

Products (Cont)



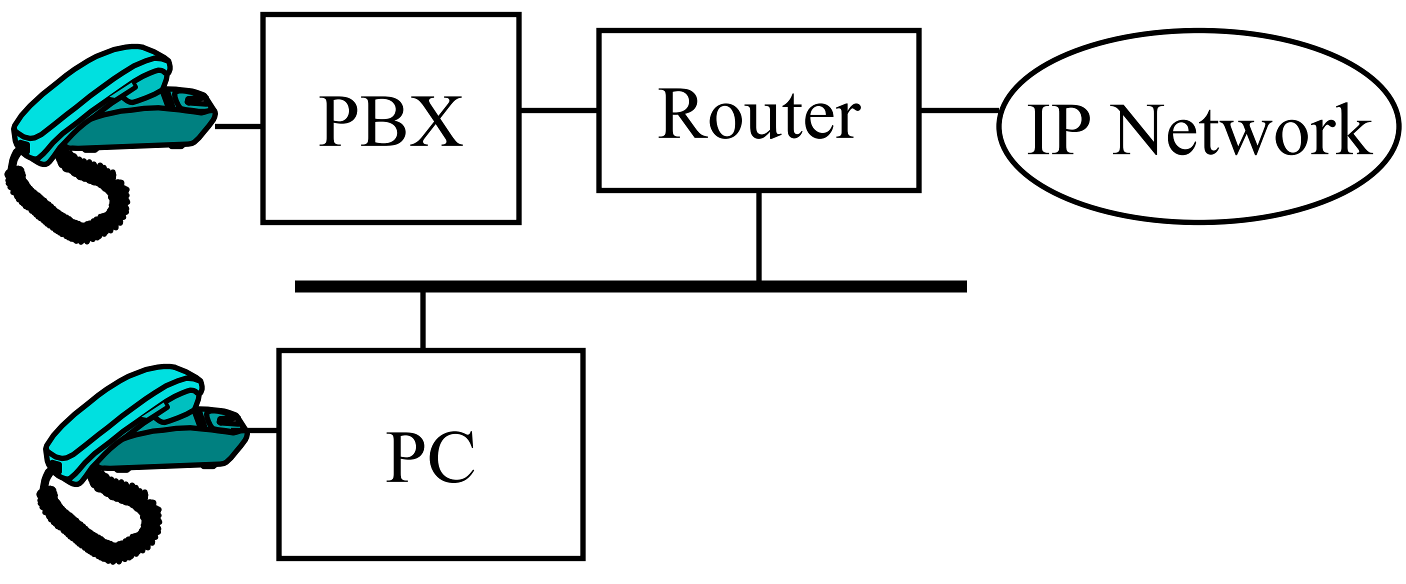
- Features:
  - Compression
  - Phone number to IP address translation.
  - Supports RSVP.
  - Limits number of calls.

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.

Services (Cont)

- 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

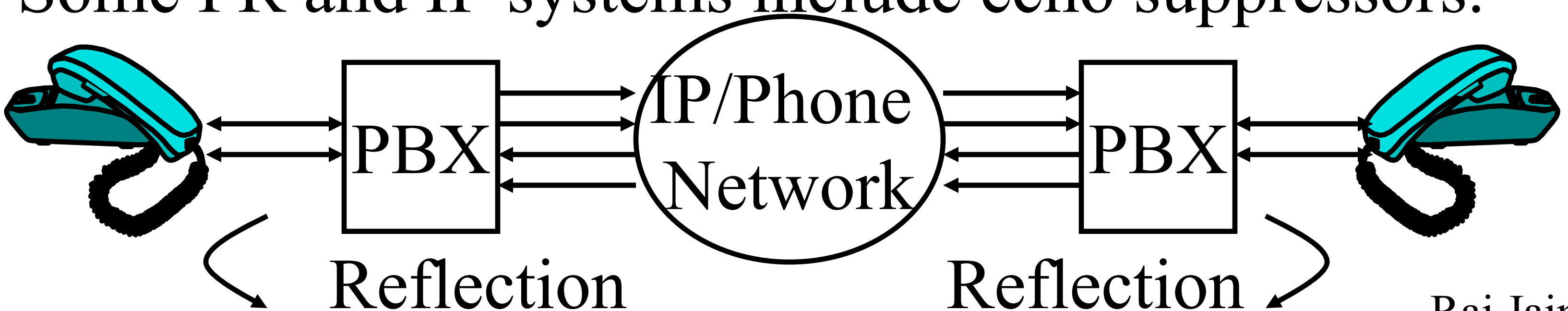
Technical Issues

1. Large Delay

- Normal Phone: 10 ms/kmile ⇒ 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 ⇒ 400 ms in the PC
- In a survey, 77% users found delay unacceptable.

Technical Issues (Cont)

2. Delay Jitter: Need priority for voice packets. Shorter packets? IP precedence (TOS) field.
3. Frame length: 9 kB at 64 kbps = 1.125 s
   Smaller MTU ⇒ 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.



Raj Jain

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).
- G.729: 8 kbps Conjugate-Structure Algebraic Code Excited Linear Prediction (CS-ACELP).

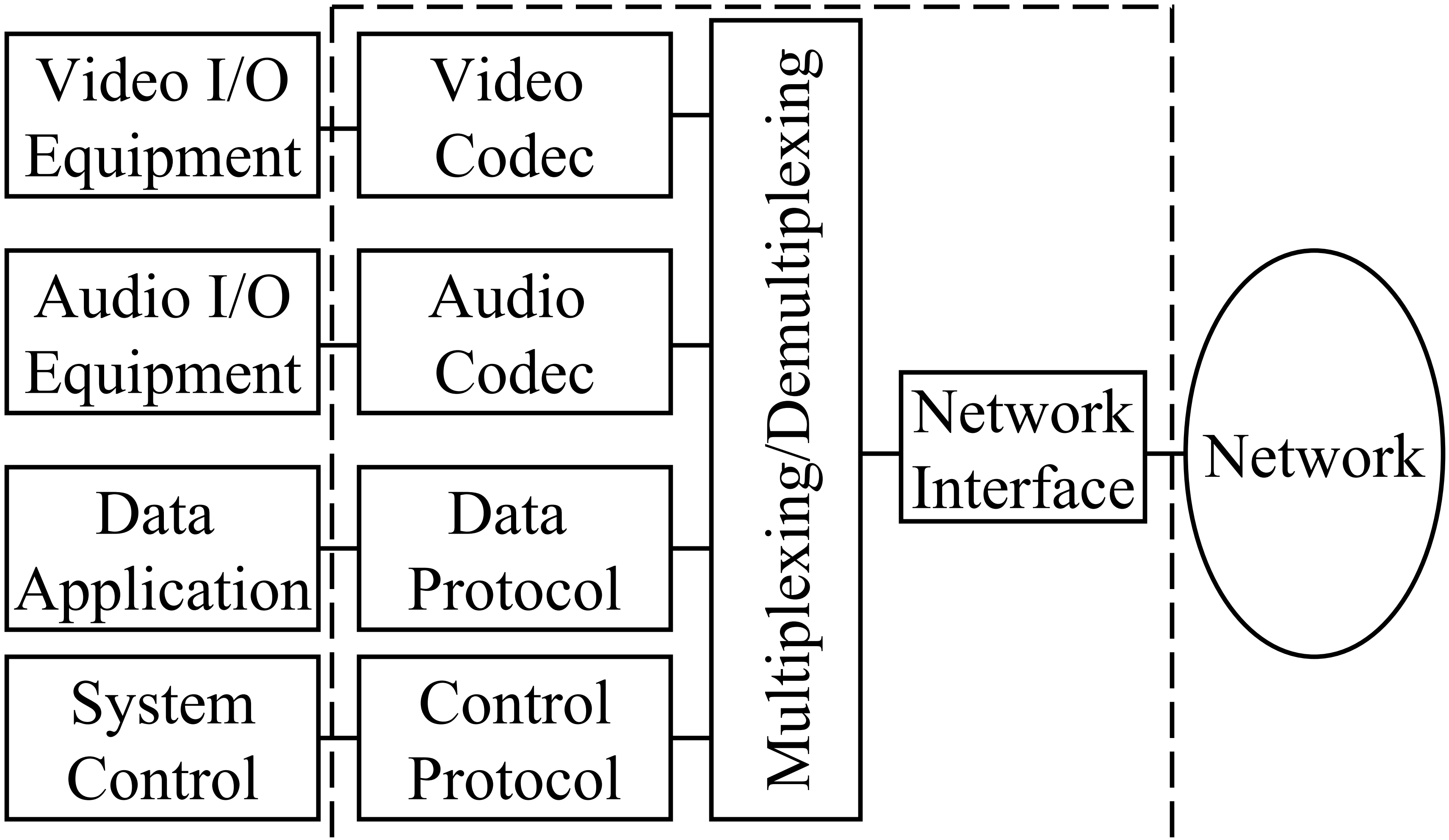
Compression (Cont)

- G.729A:
  - A reduced complexity version in Annex A of G.729.
  - 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



Raj Jain

Conferencing Standards

Network	ISDN	ATM	PSTN	LAN	POTs
Conf. Std.	H.320	H.321	H.322	H.323 V1/V2	H.324
Year Audio Codec	1990 G.711, G.722, G.728	1995 G.711, G.722, G.728	1995 G.711, G.722, G.728	1996/1998 G.711, G.722, G.723.1, G.728, G.729	1996 G.723.1, G.729
Audio Rates kbps Video Codec	64, 48-64 H.261	64, 48-64, 16 H.261, H.263	64, 48-64, 16 H.261, H.263	64, 48-64, 16, 8, 5.3/6.3 H.261 H.263	8, 5.3/6.3 H.261 H.263
Data Sharing	T.120	T.120	T.120	T.120	T.120
Control	H.230, H.242	H.242	H.242, H.230	H.245	H.245
Multiplexing	H.221	H.221	H.221	H.225.0	H.223
Signaling	Q.931	Q.931	Q.931	Q.931	-

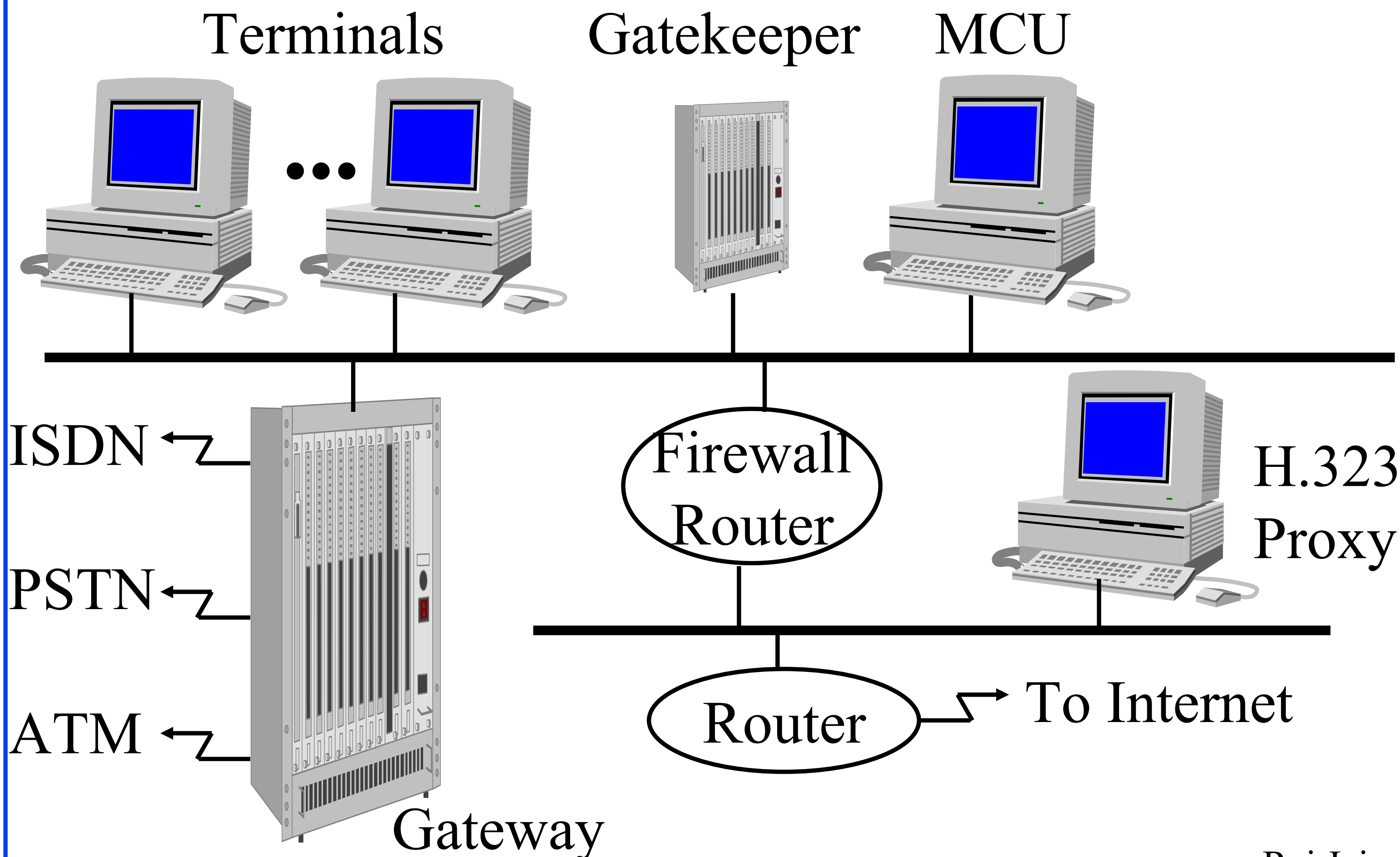
H.323 Protocols

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

<table>
<tr><td>Video</td><td>Audio</td><td colspan="4">Control and Management</td><td>Data</td></tr>
<tr><td>H.261
H.263</td><td>G.711, G.722,
G.723.1, G.728,
G.729</td><td rowspan="2">RTCP</td><td>H.225.0
RAS</td><td>H.225.0
Signaling</td><td>H.245
Control</td><td>T.124</td></tr>
<tr><td colspan="2">RTP</td><td colspan="3">X.224 Class 0</td><td>T.125</td></tr>
<tr><td colspan="3">UDP</td><td colspan="3">TCP</td><td rowspan="2">T.123</td></tr>
<tr><td colspan="6">Network (IP)</td></tr>
<tr><td colspan="7">Datalink (IEEE 802.3)</td></tr>
</table>

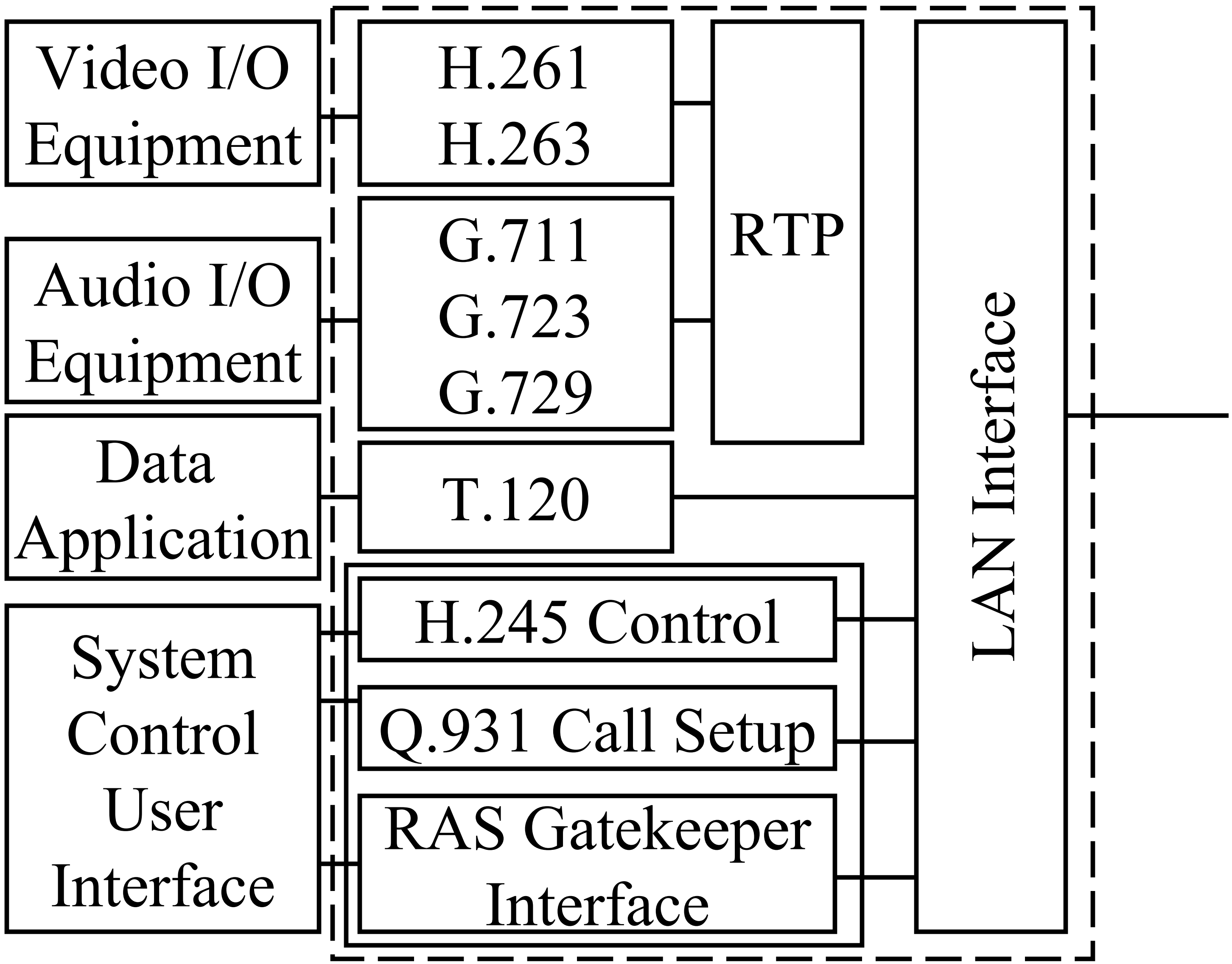
Raj Jain

H.323 Components



Raj Jain

H.323 Terminals

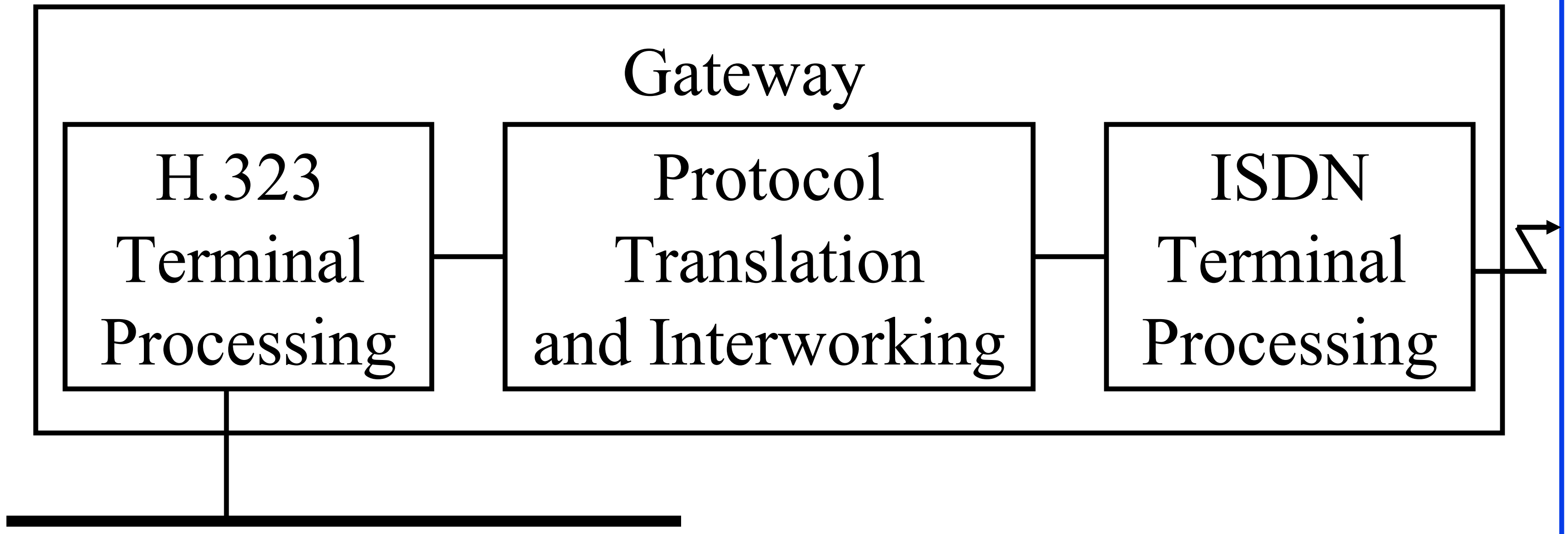


H.323 Terminals

- 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.



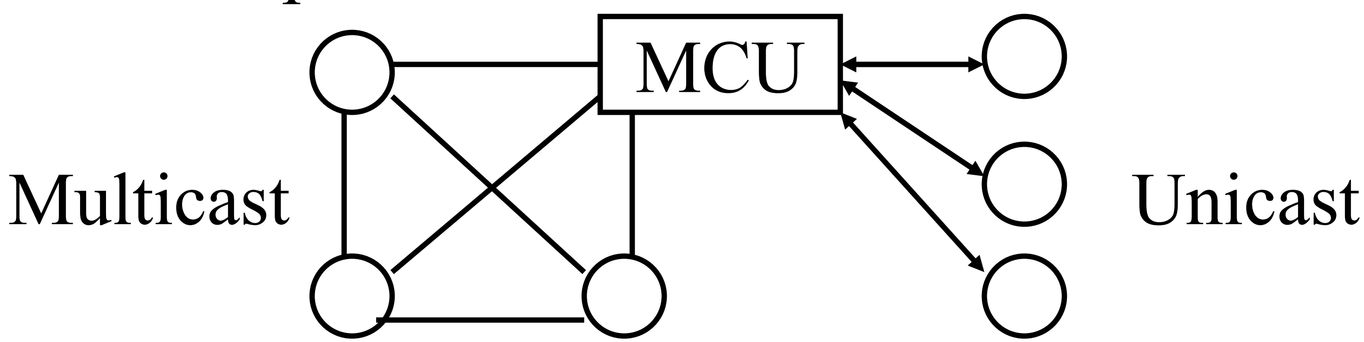
Raj Jain

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.



Raj Jain

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)

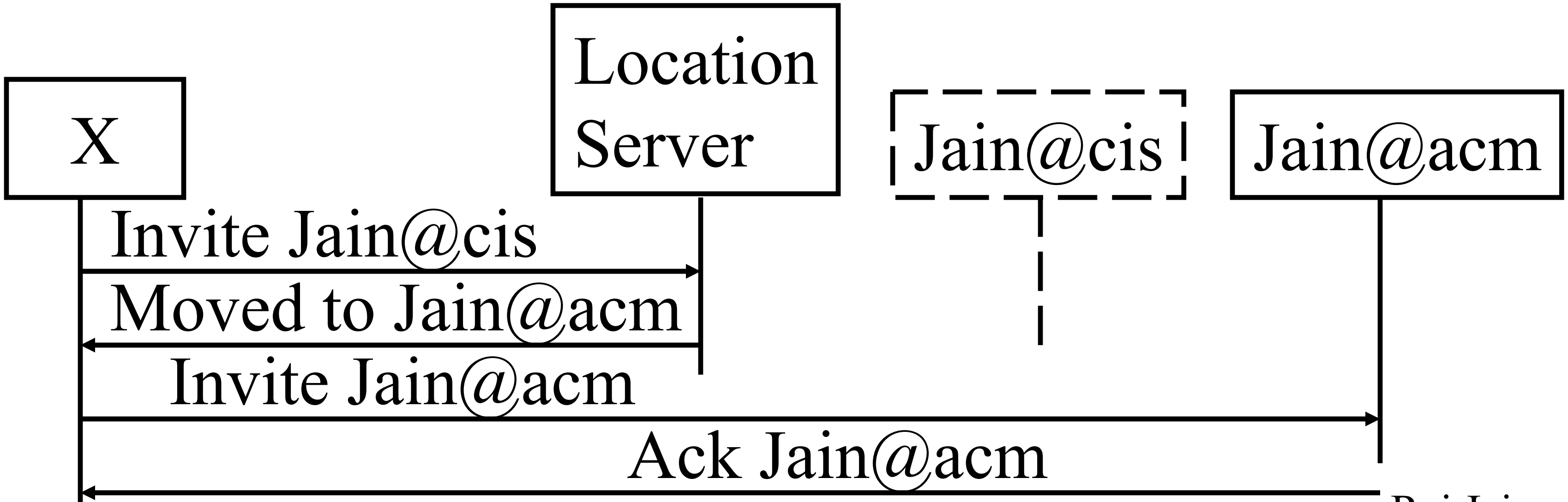
- SIP works in conjunction with other IP protocols for multimedia:
  - RSVP for reserving network resources
  - RTP/RTCP/RTSP for transporting real-time data
  - Session Announcement Protocol (SAP) for advertising multimedia session
  - Session description protocol (SDP) for describing multimedia session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

SIP (Cont)

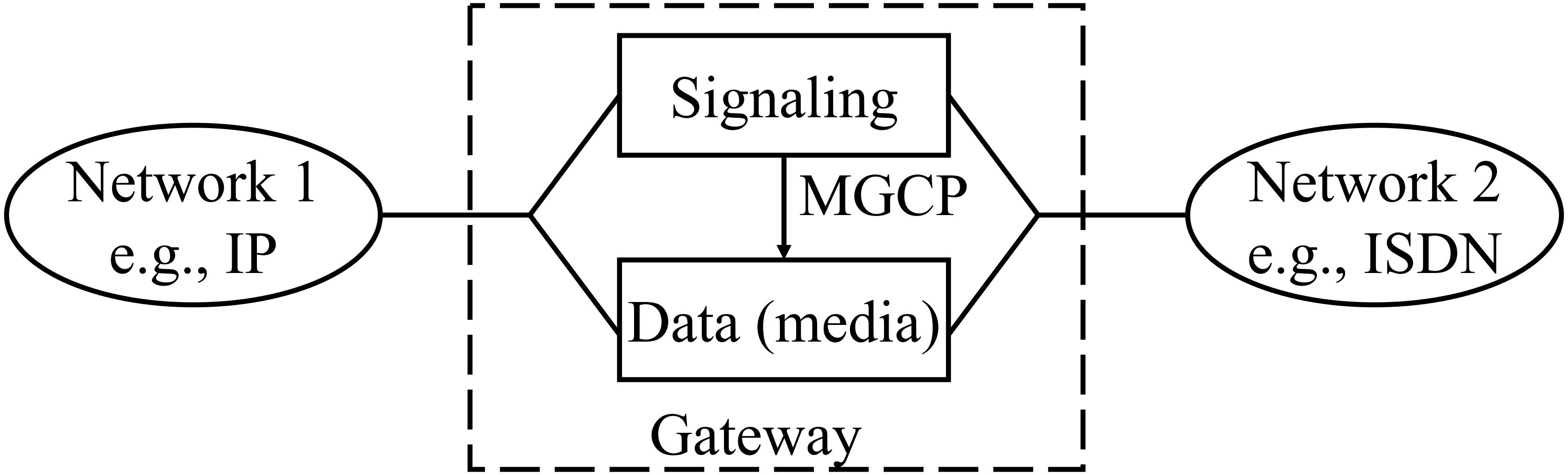
- SIP is text based (similar to HTTP)
  $\Rightarrow$ SIP messages can be easily generated by humans, CGI, Perl, or Java programs.
- SIP Uniform Resource Locators (URLs):
  Similar to email URLs
  sip:jain@cis.ohio-state.edu
  sip:+1-614-292-3989:123@osu.edu?subject=lecture
- SIP messages are sent to 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, ...



Media Gateway Control Protocol

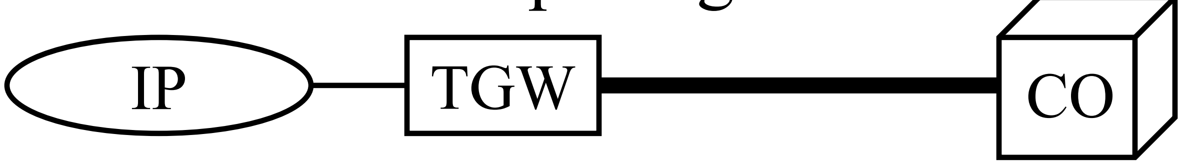


- Gateway = Signaling Fns + Media Transfer Fns
- Call Agents: Signaling functions ⇒ Intelligent
  ⇒ More complex ⇒ Fewer
  ⇒ Control multiple media gateways ⇒ Need MGCP
- MGCP =Simple Gateway Control Protocol (SGCP)
  + Internet Protocol Device Control (IPDC)

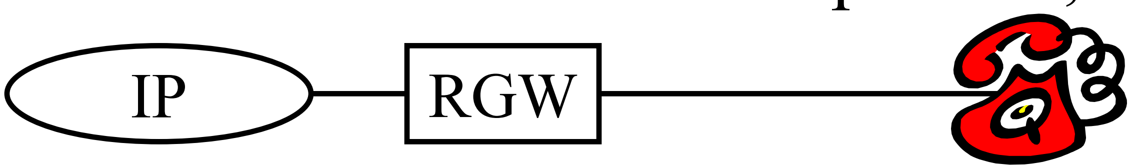
Raj Jain

Media Gateways: Examples

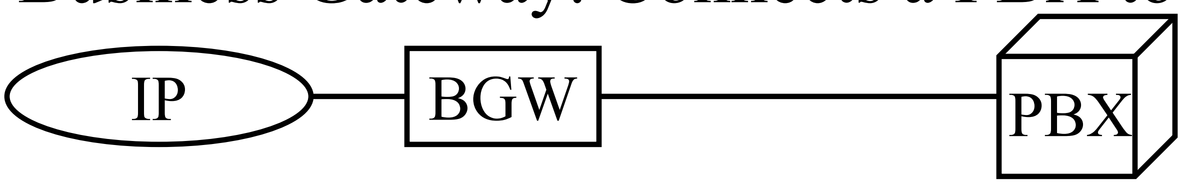
- Trunking Gateway: Connects a PSTN trunk to VOIP
  Terminates multiple digital circuits



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

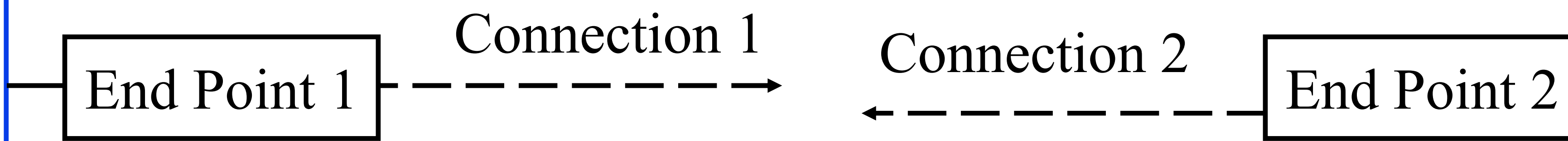


- Business Gateway: Connects a PBX to VOIP



- 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
  $\Rightarrow$ 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

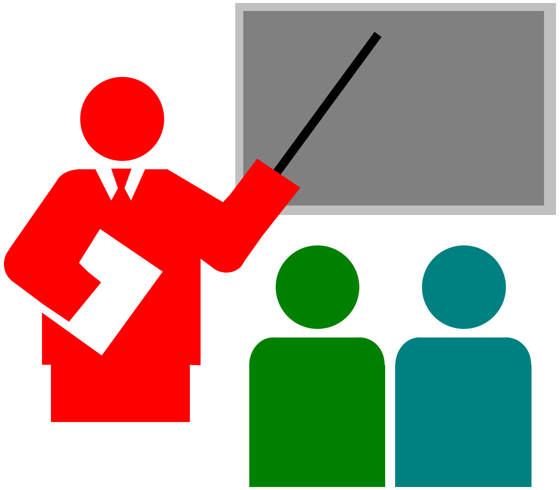
- SDP V2 [RFC2327]
- Used to describe media type and port # for connections and mbone sessions
- Includes: Version (v), Session name (s), Information (i), Owner (o), Connection information (c), media type, port, and coding (m), session attributes (a), ...
- Example:
  s = Netlab Seminars
  c = 224.5.17.11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

Raj Jain

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 for a detailed list of references.

Virtual Private Networks

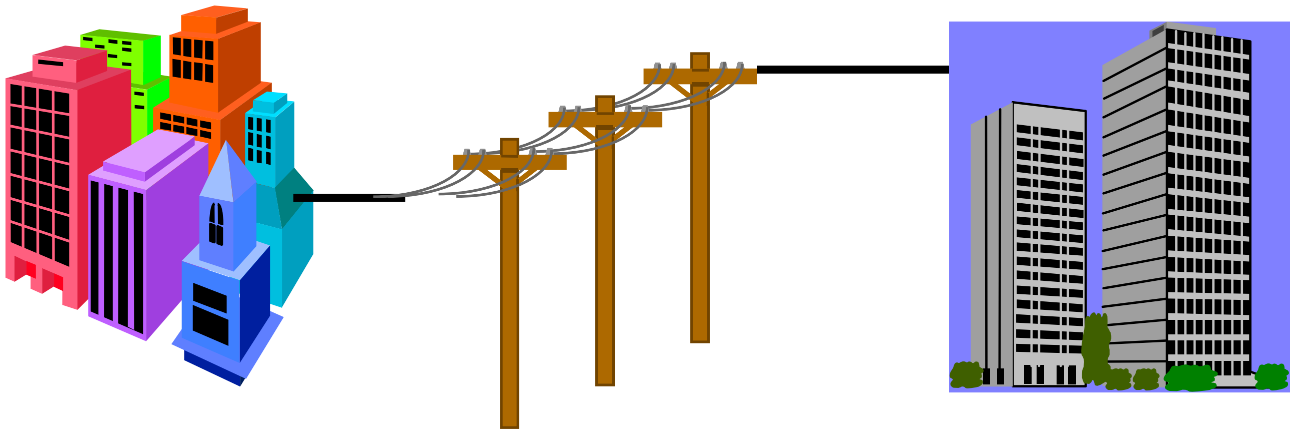
Raj Jain
The Ohio State University
Columbus, OH 43210
Jain@CIS.Ohio-State.Edu
http://www.cis.ohio-state.edu/~jain/

- 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

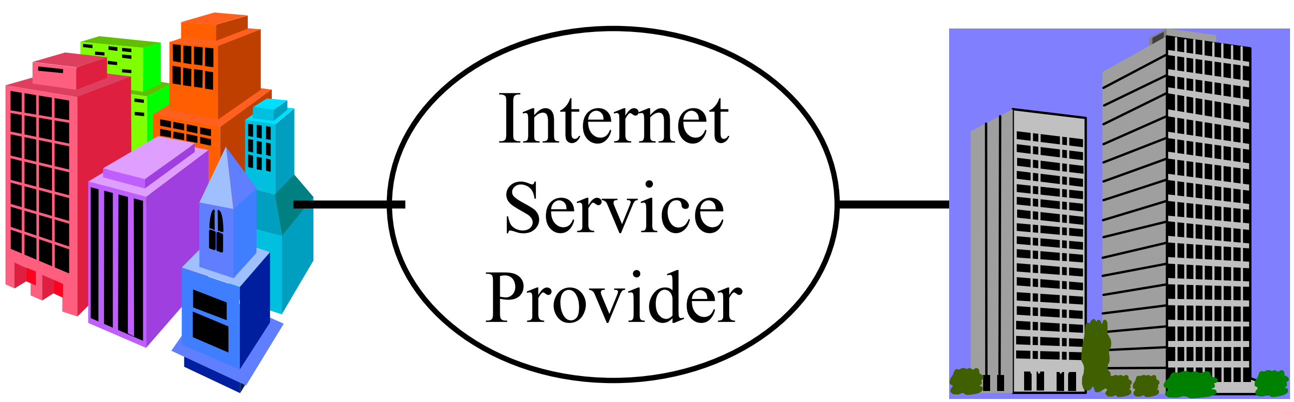
Raj Jain

What is a VPN?

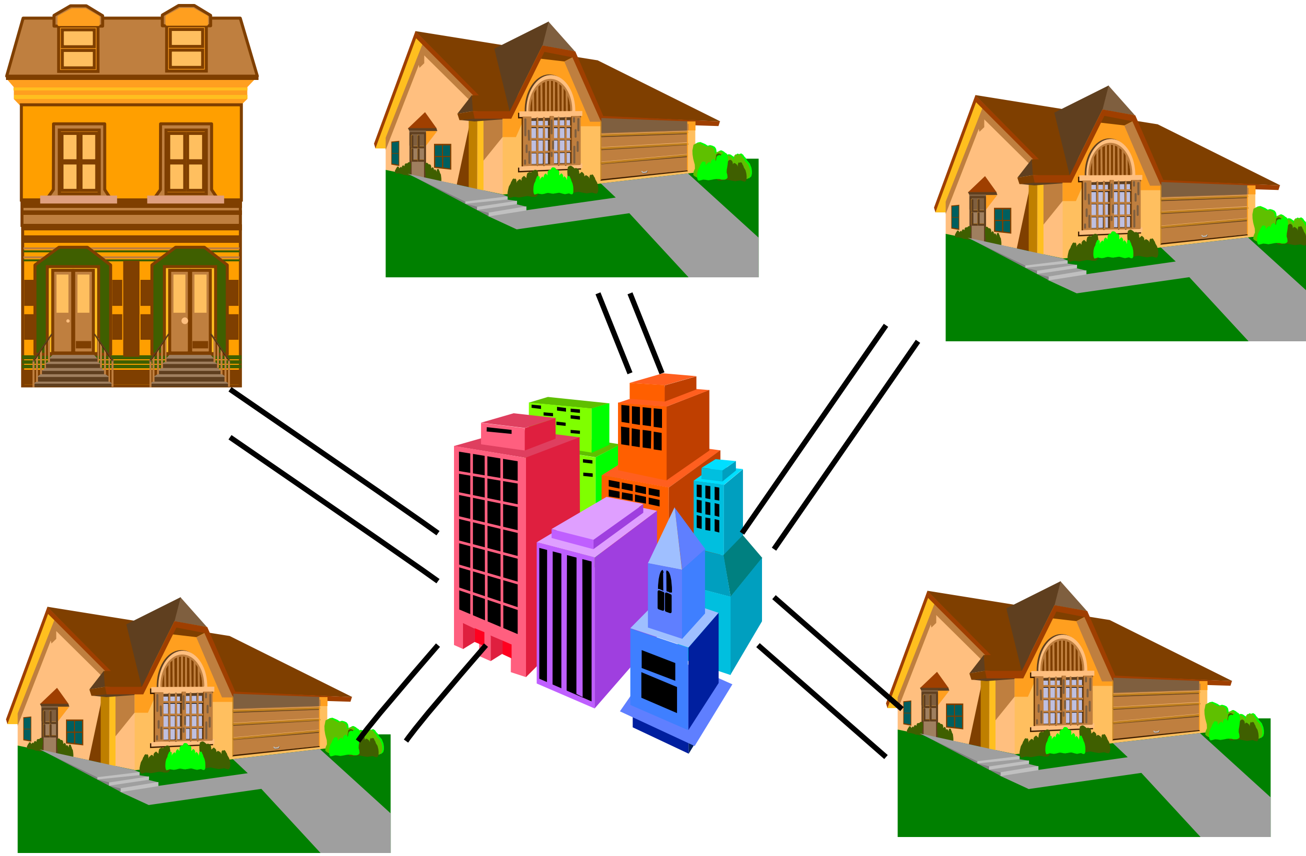
- Private Network: Uses leased lines



- *Virtual* Private Network: Uses public Internet



Private Road Network



- A Private network is like having a private road to all employees and branch offices
- Better to share the public roads.

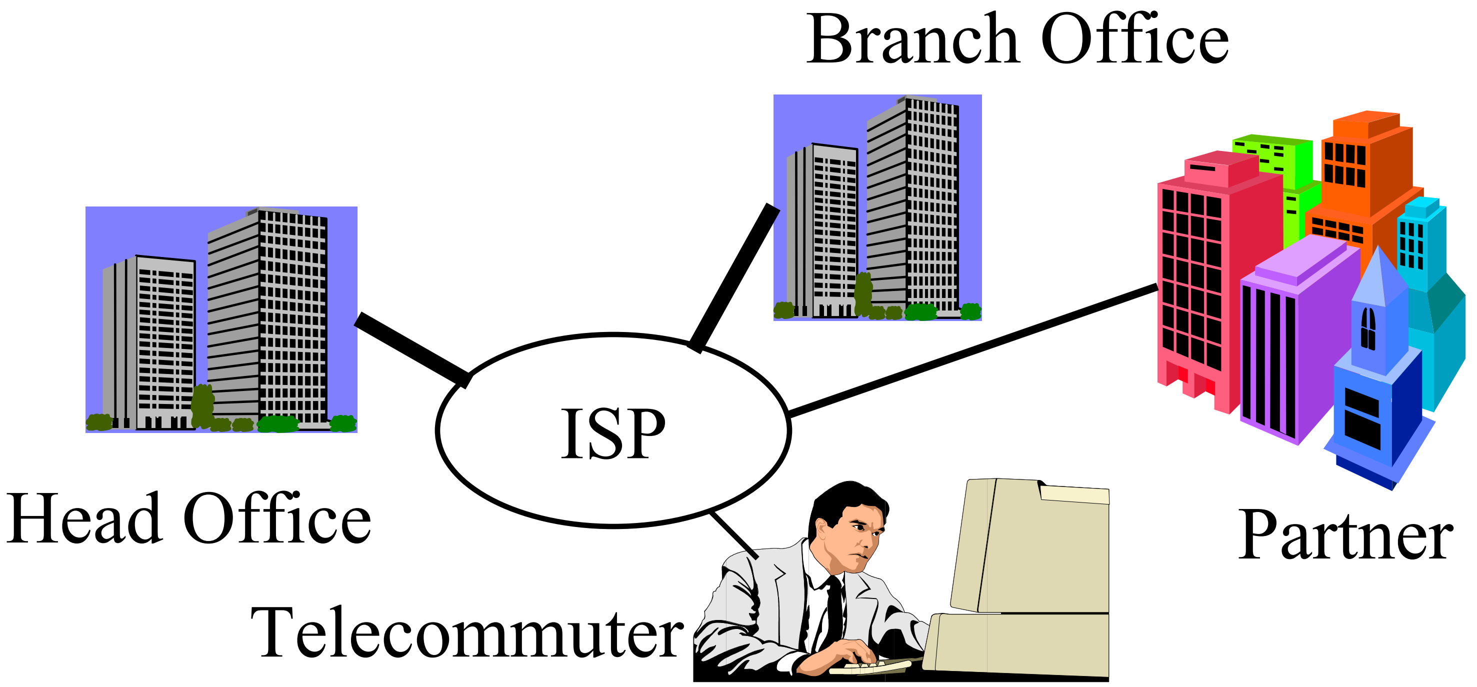
Raj Jain

Virtual Private Network

- VPNs are like having a private talk in a crowded room. You need to code your messages.

Types of VPNs

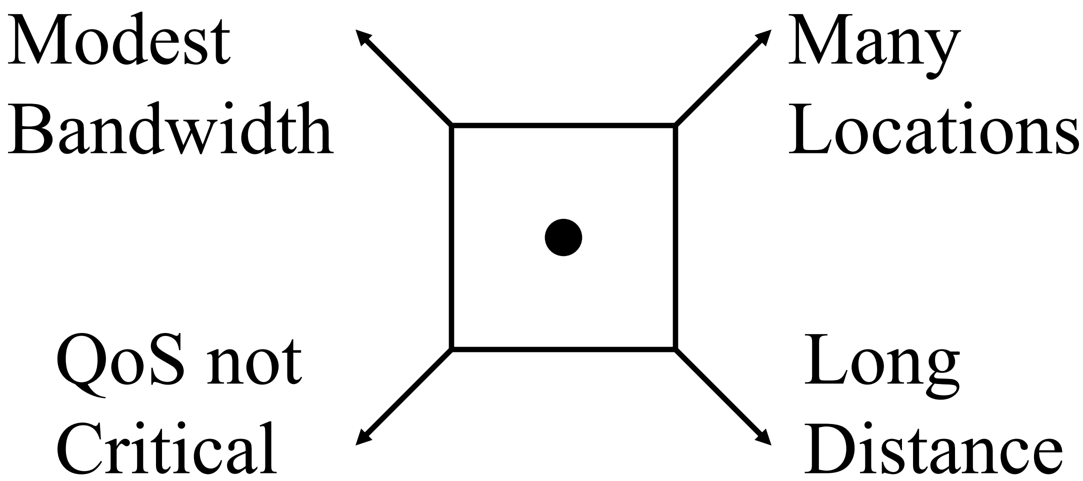
- WAN VPN: Branch offices
- Access VPN: Roaming Users
- Extranet VPNs: Suppliers and Customers



Why VPN?

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

When to VPN?



- More Locations, Longer Distances, Less Bandwidth/site, QoS less critical
  $\Rightarrow$ VPN more justifiable
- Fewer Locations, Shorter Distances, More Bandwidth/site, QoS more critical
  $\Rightarrow$ VPN less justifiable

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

Raj Jain

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
    $\Rightarrow$ Need key recovery

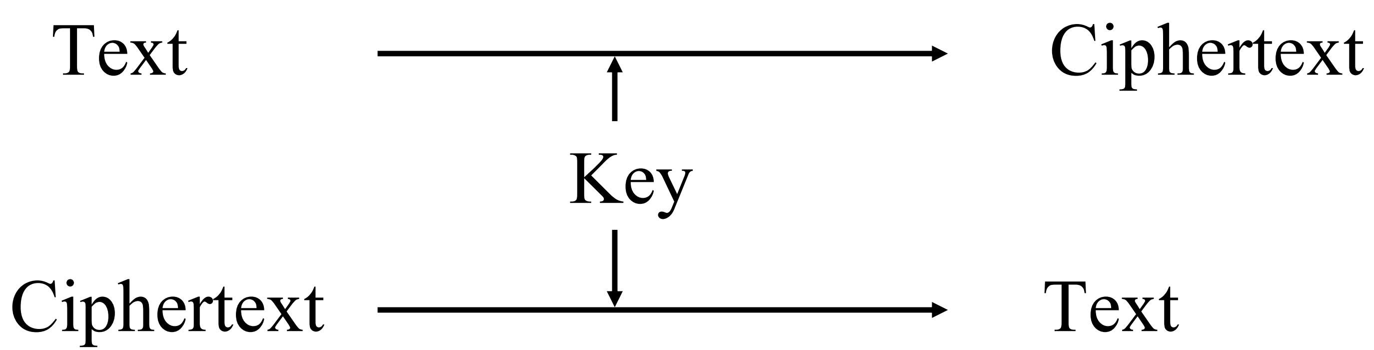
Security 101

- 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

Raj Jain

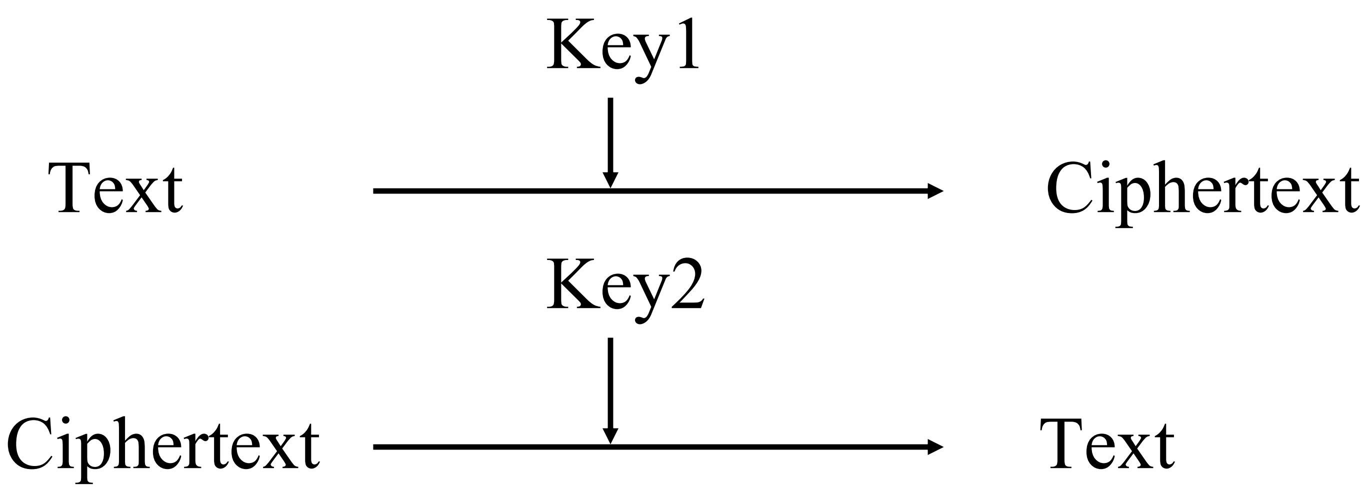
Secret Key Encryption

- 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
- Encrypted_Message = Encrypt(Key1, Message)
- Message = Decrypt(Key2, Encrypted_Message)



Public Key Encryption

- RSA: Encrypted_Message = m^3 mod 187
- Message = $\text{Encrypted\_Message}^{107}$ 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
  $= \{(125^{64} \bmod 187)(125^{32} \bmod 187)\ldots$
  $(125^{2} \bmod 187)(125)\} \bmod 187 = 5$
- $125^4 \bmod 187 = (125^2 \bmod 187)^2 \bmod 187$

Raj Jain

Public Key (Cont)

- One key is private and the other is public
- Message = Decrypt(Public_Key,
  Encrypt(Private_Key, Message))
- Message = Decrypt(Private_Key,
  Encrypt(Public_Key, Message))

Digital Signature

- Message Digest = Hash(Message)
- Signature = Encrypt(Private_Key, Hash)
- Hash(Message) = Decrypt(Public_Key, Signature)
  $\Rightarrow$ Authentic

$$\text{Text} \xrightarrow{\text{Hash}} \text{Digest} \xrightarrow{\text{Private Key}} \text{Signature}$$

$$\text{Signature} \xrightarrow{\text{Public Key}} \text{Digest} \xleftarrow{\text{Hash}} \text{Text}$$

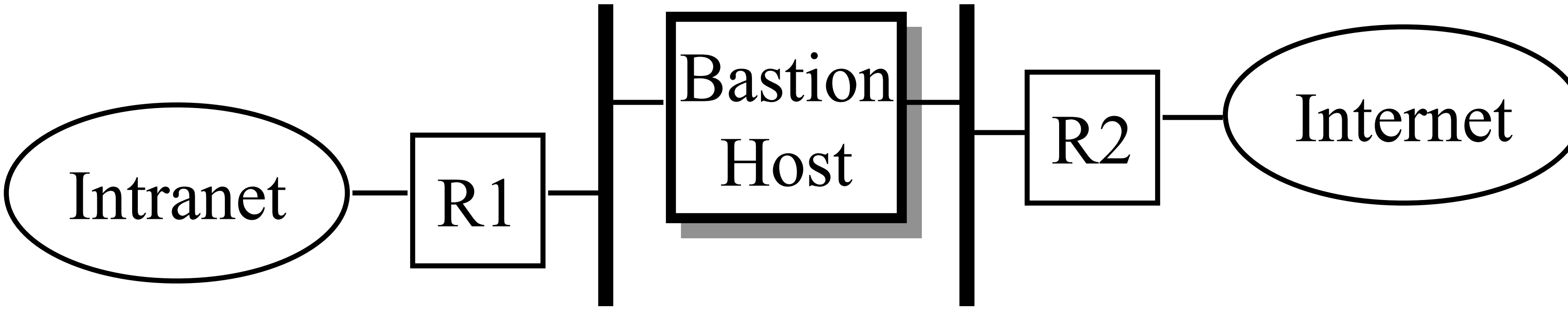
Certificate

- 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
  $\Rightarrow$ Hierarchy of trusted authorities

Confidentiality

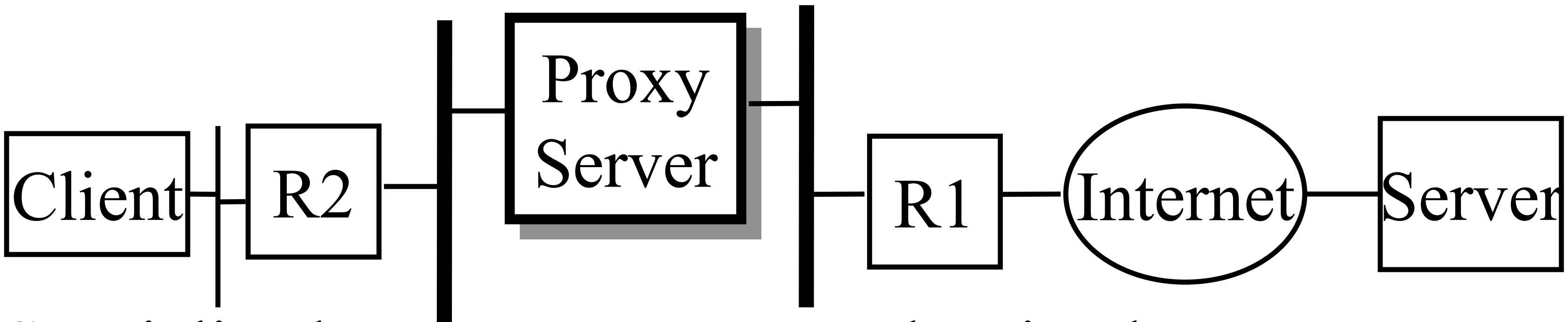
- User 1 to User 2:
- Encrypted_Message = Encrypt(Public_Key2, Encrypt(Private_Key1, Message))
- Message = Decrypt(Public_Key1, Decrypt(Private_Key2, Encrypted_Message)) $\Rightarrow$ Authentic and Private

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

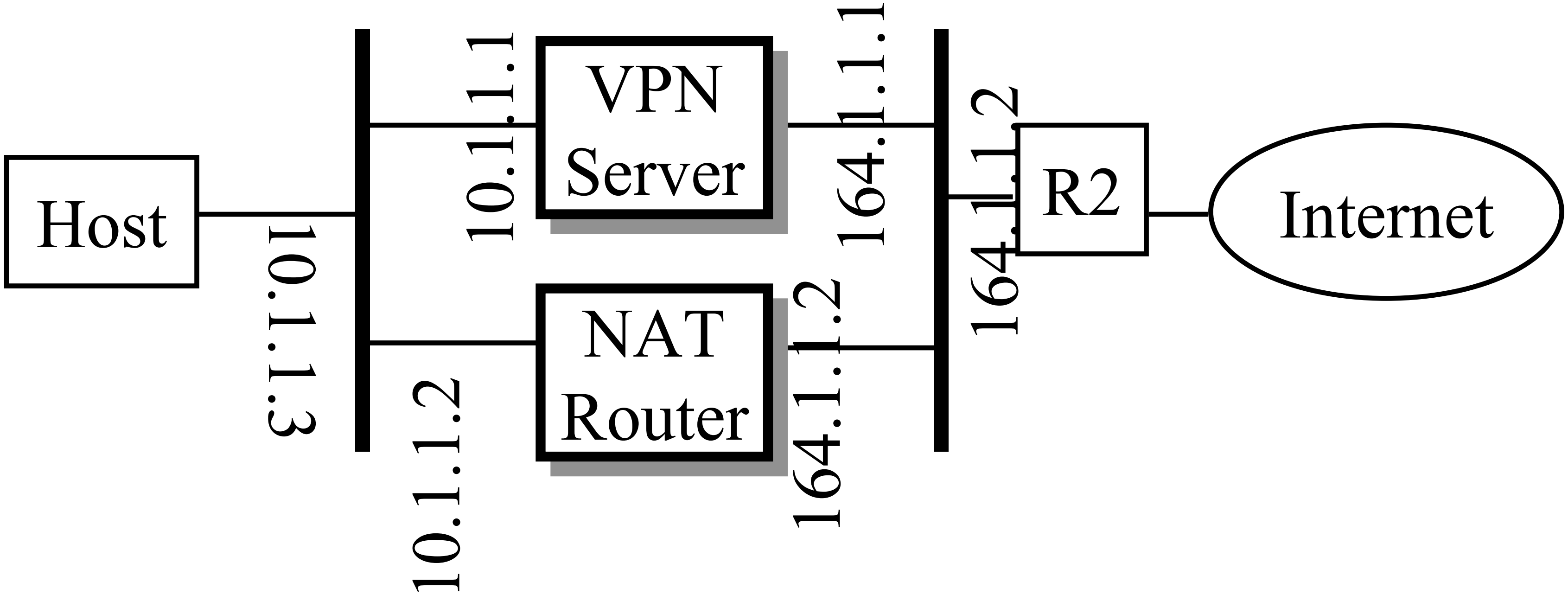
VPN Security Issues

- 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 $\Rightarrow$ More granular
- Granularity of Security: Departmental level, Application level, Role-based

Private Addresses

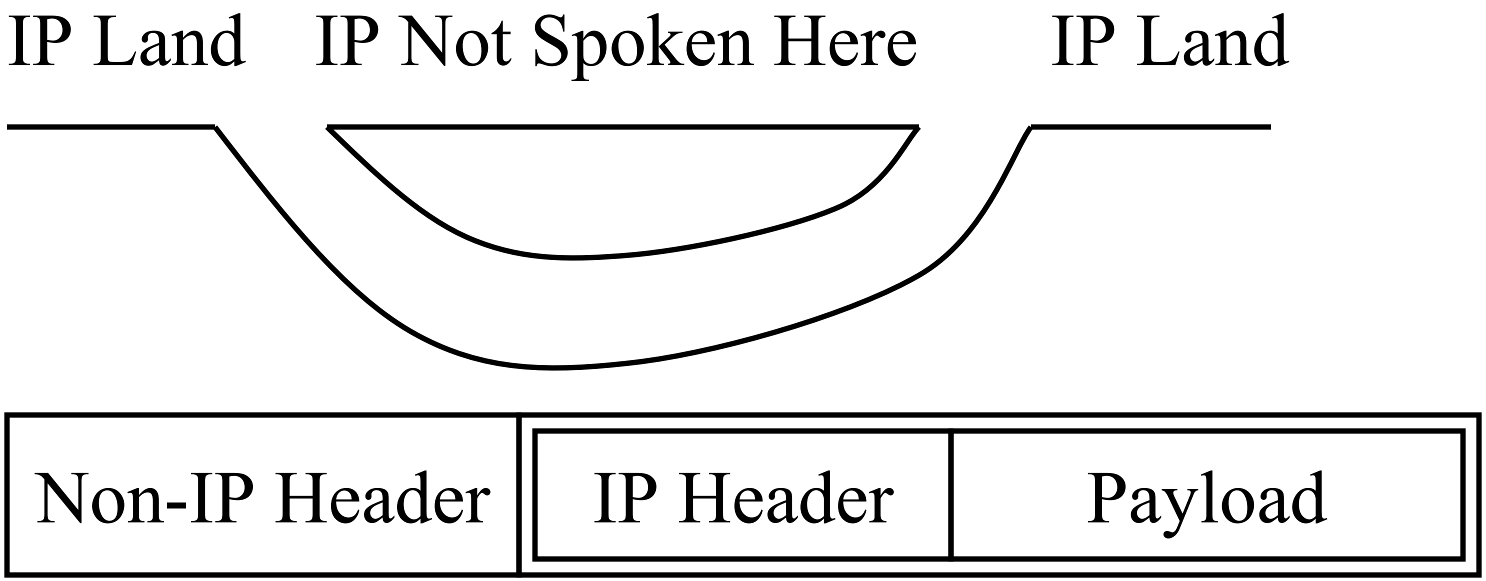
- 32-bit Address ⇒ 4 Billion addresses max
- Subnetting ⇒ Limit is much lower
- Shortage of IP address ⇒ Private addresses
- Frequent ISP changes ⇒ Private address
- Private ⇒ Not usable on public Internet
- RFC 1918 lists such addresses for private use
- Prefix = 10/8, 172.16/12, 192.168/16
- Example: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

Address Translation



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

Tunnel



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

VPN Tunneling Protocols

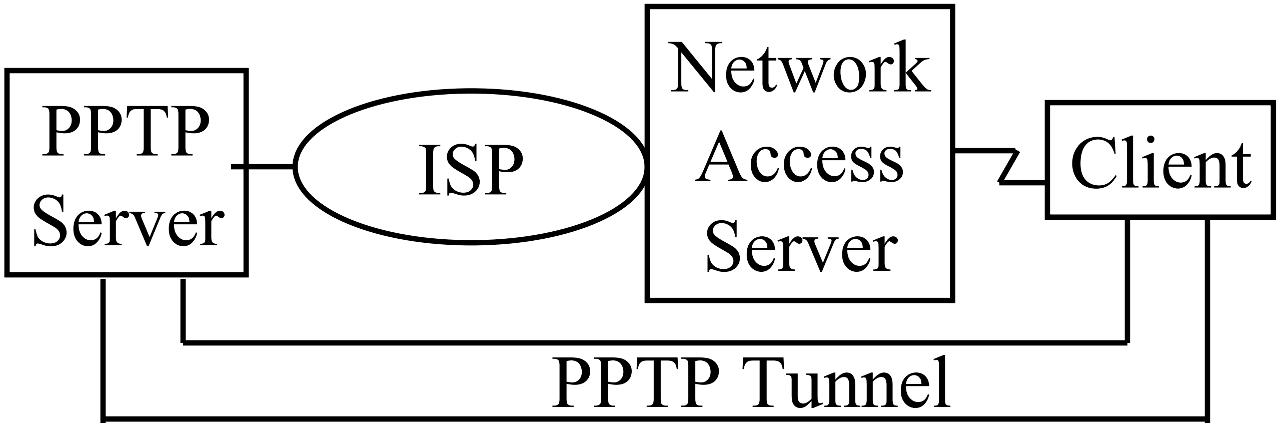
- GRE: Generic Routing Encaptulation (RFC 1701/2)
- PPTP: Point-to-point Tunneling Protocol
- L2F: Layer 2 forwarding
- L2TP: Layer 2 Tunneling protocol
- ATMP: Ascend Tunnel Management Protocol
- DLSW: Data Link Switching (SNA over IP)
- IPSec: Secure IP
- Mobile IP: For Mobile users

GRE

Delivery Header	GRE Header	Payload

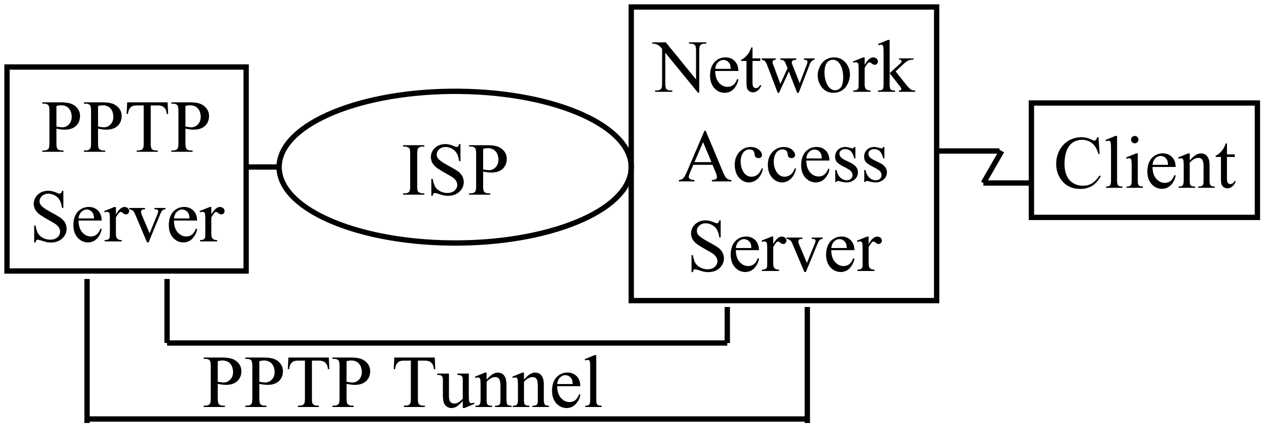
- Generic Routing Encaptulation (RFC 1701/1702)
- Generic $\Rightarrow$ X over Y for any X or Y
- Optional Checksum, Loose/strict Source Routing, Key
- Key is used to authenticate the source
- Over IPv4, GRE packets use a protocol type of 47
- Allows router visibility into application-level header
-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

PPTP



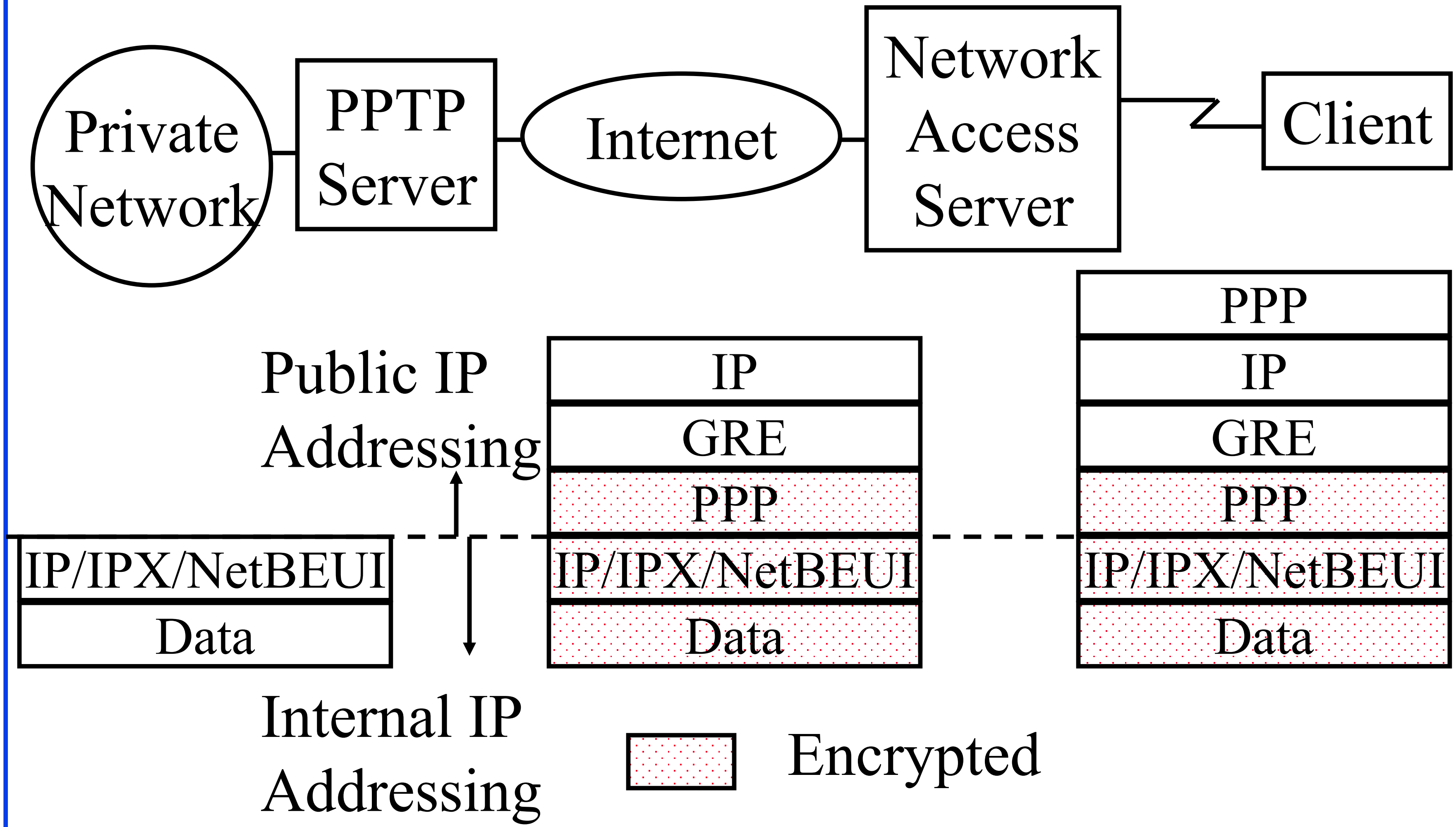
- PPTP = Point-to-point Tunneling Protocol
- Developed jointly by Microsoft, Ascend, USR, 3Com and ECI Telematics
- PPTP server for NT4 and clients for NT/95/98
- MAC, WFW, Win 3.1 clients from Network Telesystems (nts.com)

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

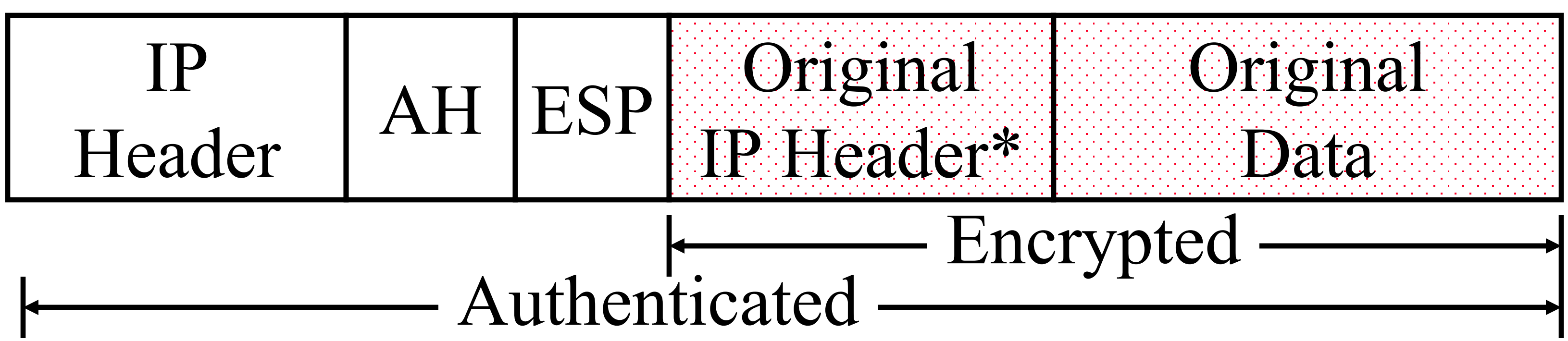


L2TP

- 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



* Optional

IPSec (Cont)

- Two Modes: Tunnel mode, Transport mode
- Tunnel Mode $\Rightarrow$ Original IP header encrypted
- Transport mode $\Rightarrow$ 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 $\Rightarrow$ Any user can use the tunnel
- Needs more time for standardization than L2TP

SOCKS

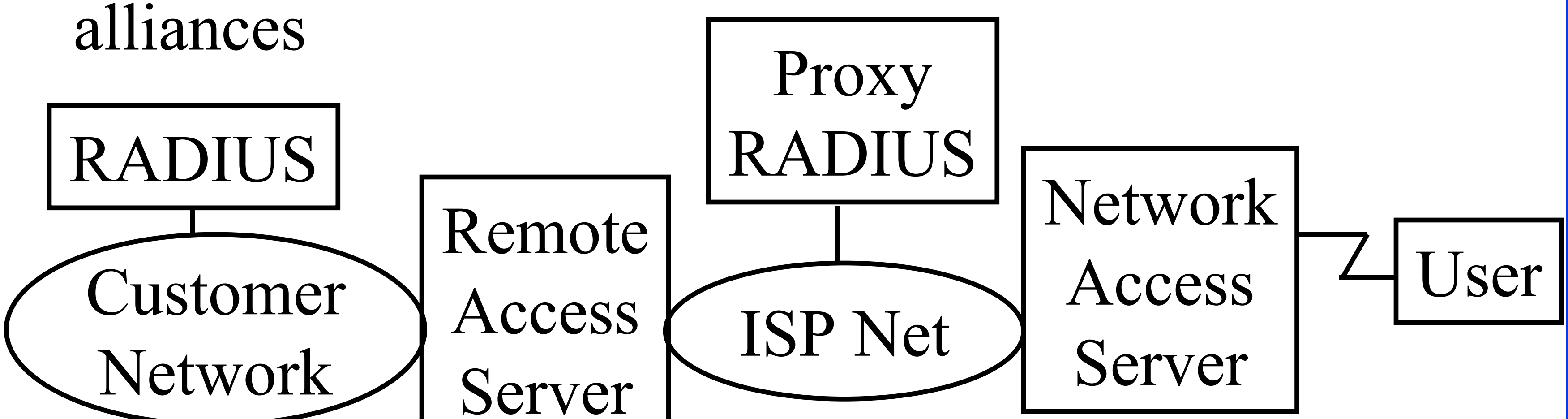
- Session layer proxy
- Can be configured to proxy any number of TCP or UDP ports
- Provides authentication, integrity, privacy
- Can provide address translation
- Developed by David Koblas in 1990. Backed by NEC
- Made public and adopted by IETF Authenticated Firewall Traversal (AFT) working group
- Current version v5 in RFC 1928
- Proxy $\Rightarrow$ Slower performance
- Desktop-to-Server $\Rightarrow$ 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



Raj Jain

DIAMETER

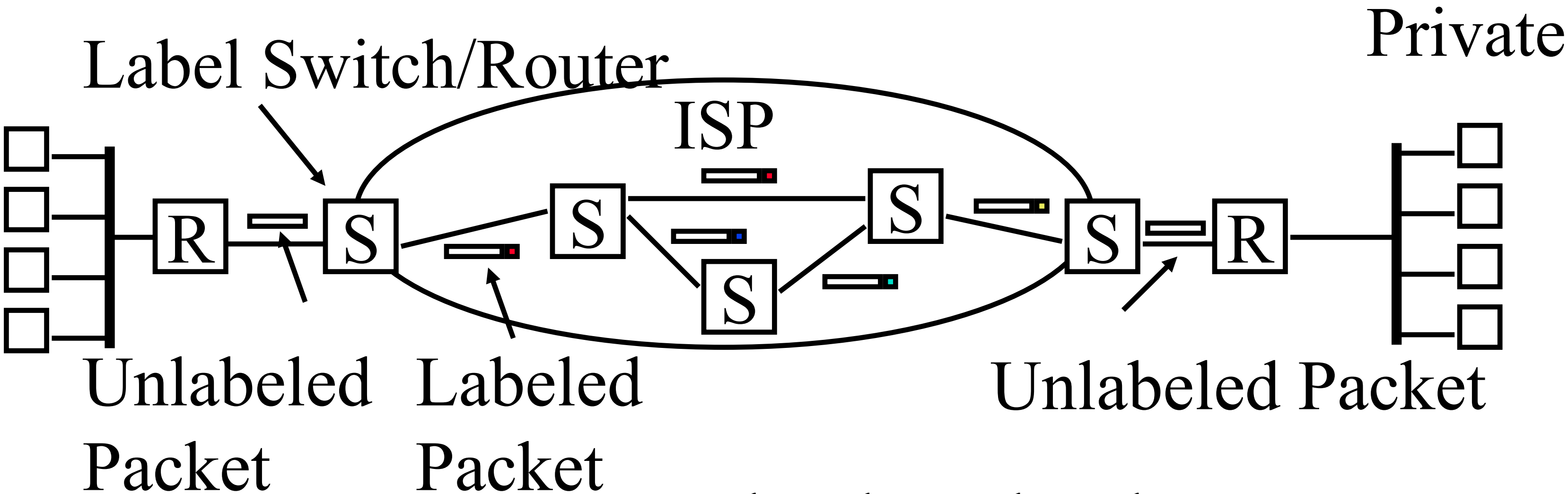
- Enhanced RADIUS
- Light weight
- Can use both UDP and TCP
- Servers can send unsolicited messages to Clients
  $\Rightarrow$ Increases the set of applications
- Support for vendor specific Attribute-Value-Pairs (AVPs) and commands
- Authentication and privacy for policy messages

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

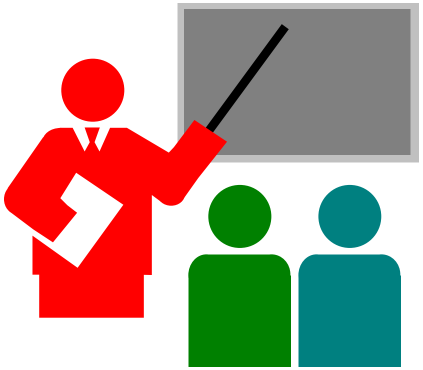
VPN Support with MPLS

- Multiprotocol Label Switching
- Allows packets to be switched using labels (tags)
  $\Rightarrow$ Creates connections across a network
- Labels contain Class of Service



20b	3b	1b	8b
Label	CoS	SI	TTL

Summary



- 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 ⇒ MPLS

References

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

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.

Final Review (Cont)

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