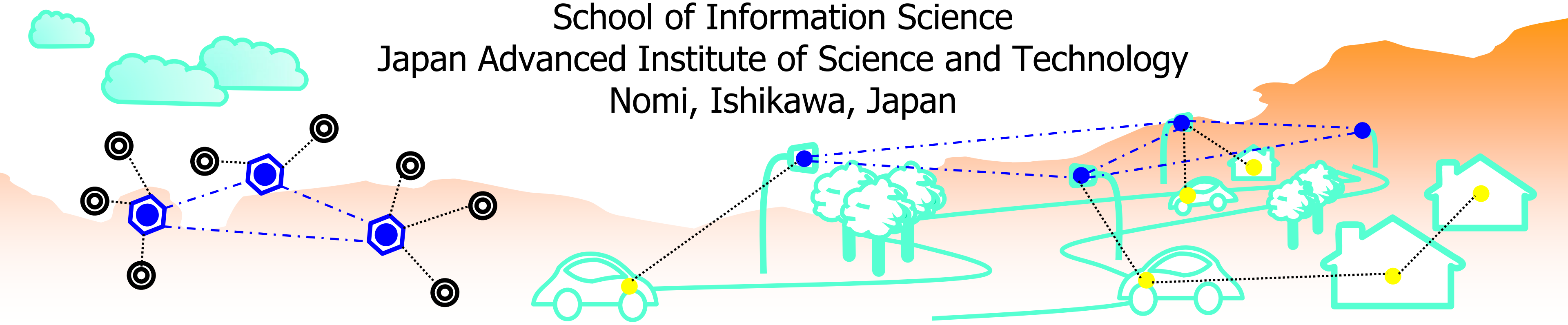
I226
Computer Networks

Chapter 9

Wide Area Networks and Security

Assoc. Prof. Yuto Lim

School of Information Science
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan



Objectives of this Chapter

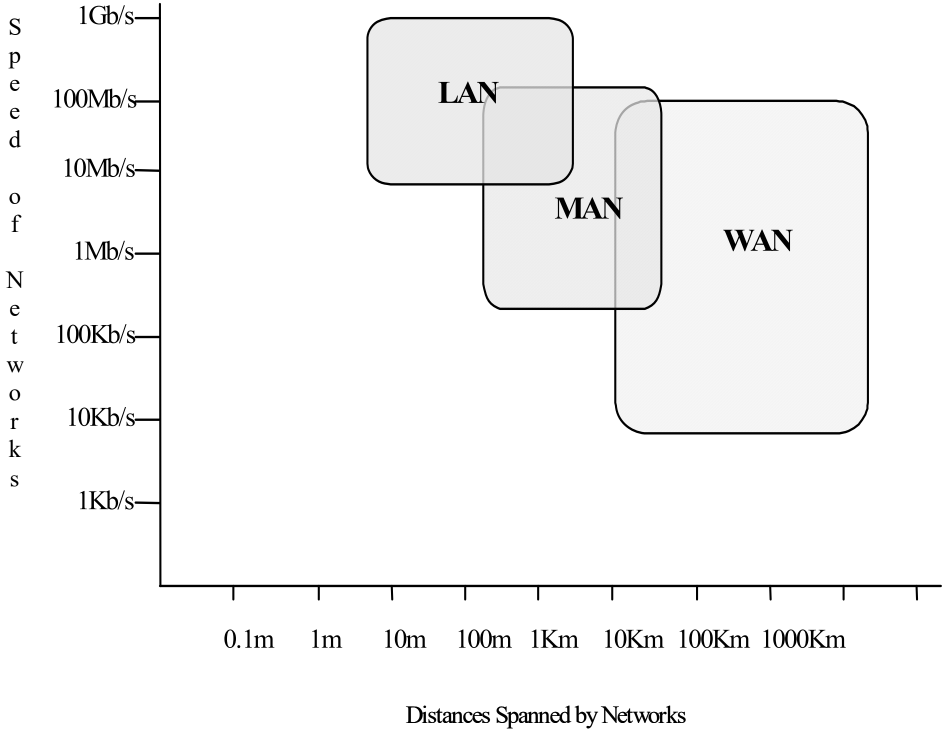
- Give the basic knowledge of WAN technology and its terminology
- Describe the examples of WAN technology, such as PSTN, X.25, Frame Relay, ISDN, T-Carriers, DSL, ATM, and SONET
- How to create a corporate network? Review the technologies of Firewall and VPN for Internet? Intranet? Extranet?
- Explain the extra features that needed to support WAN technology: Tunneling and NAT

Outline

- Introduction
- WAN Technology
  - Terminology, Device, Standard
  - Encapsulation, Communication
  - Topology, Consideration
- Example of WAN Technologies
  - PSTN, X.25, Frame Relay, ISDN, T-Carriers, DSL, ATM, SONET
- Firewall
- VPN
- Tunneling
- NAT

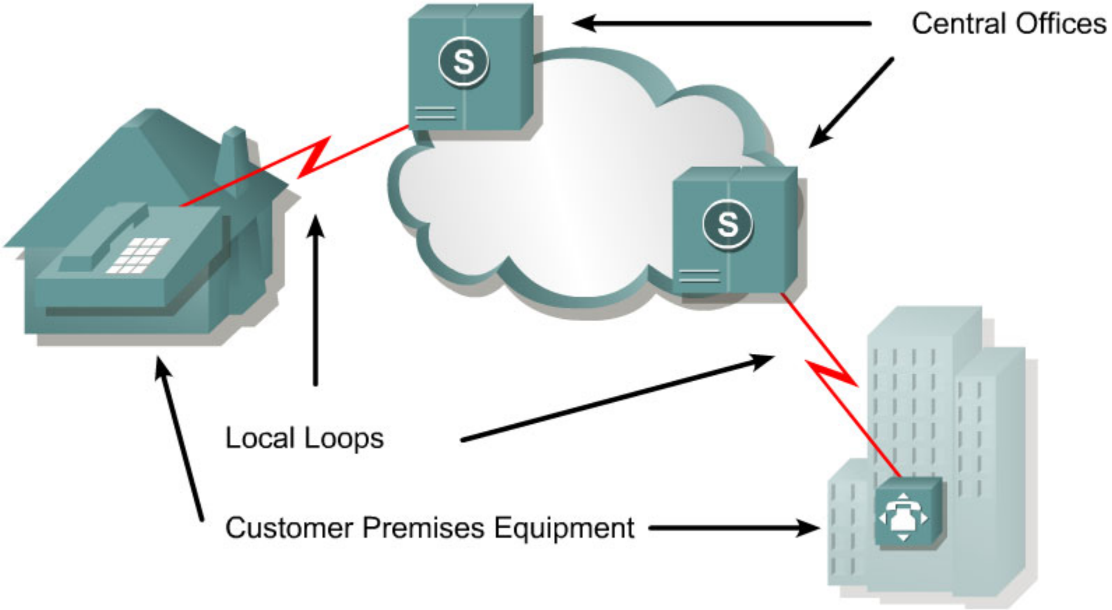
Introduction

- Networks are often classified according to how large they are
  - LAN connects hosts in a room, a building, or a campus
  - MAN connects hosts across a town or a city
  - WAN connects hosts across multiple cities, a state, a country, and the world
- LANs tend to be used for small networks (up to 100 computers). Their small size allows them to be fast because signals are less distorted over small distances
- MANs are also often used to connect LANs to Public Switched Data Networks (PSDN), which is the national networks provided by telephone companies for computer data



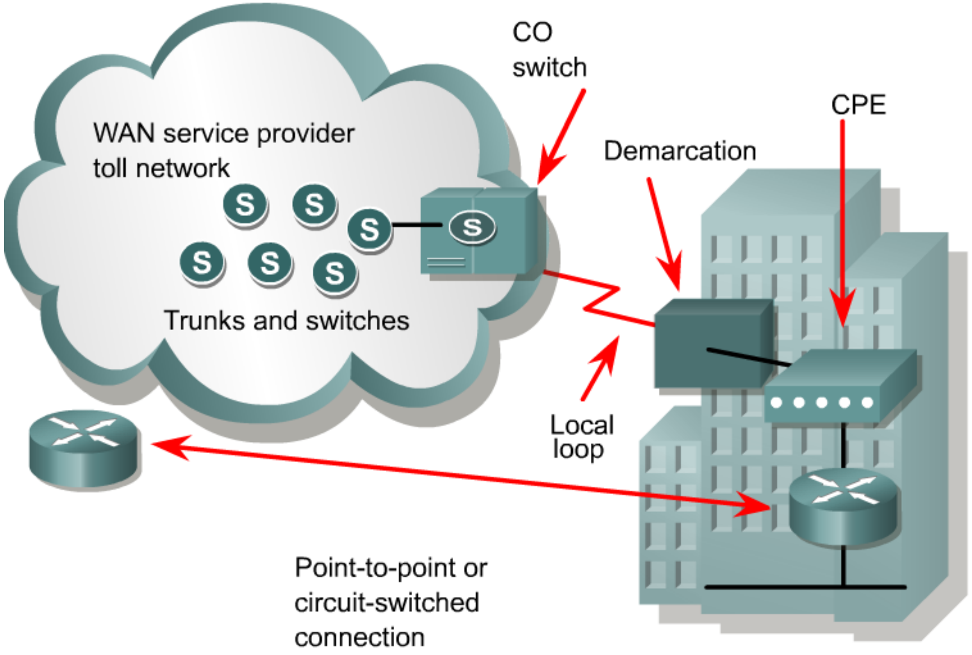
- Internet is the most obvious example of a WAN
- In summary, networks can also be classified according to how they operate

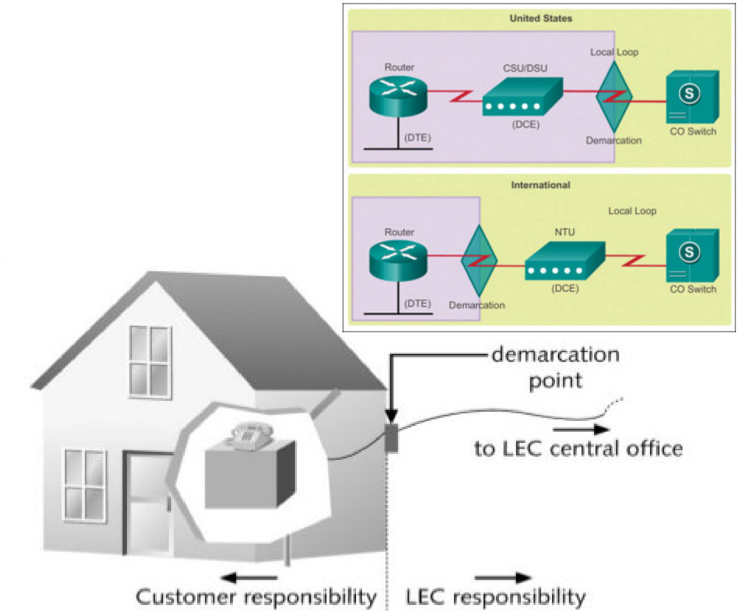
WAN Technology/Terminology (1/4)



- Devices on the subscriber premises are called customer premises equipment (CPE)
- Subscriber owns CPE or leases CPE from service provider
- Copper or fiber cable connects the CPE to the service provider’s nearest exchange or central office (CO)
- This cabling is often called the local loop, or “last-mile”

WAN Technology/Terminology (2/4)

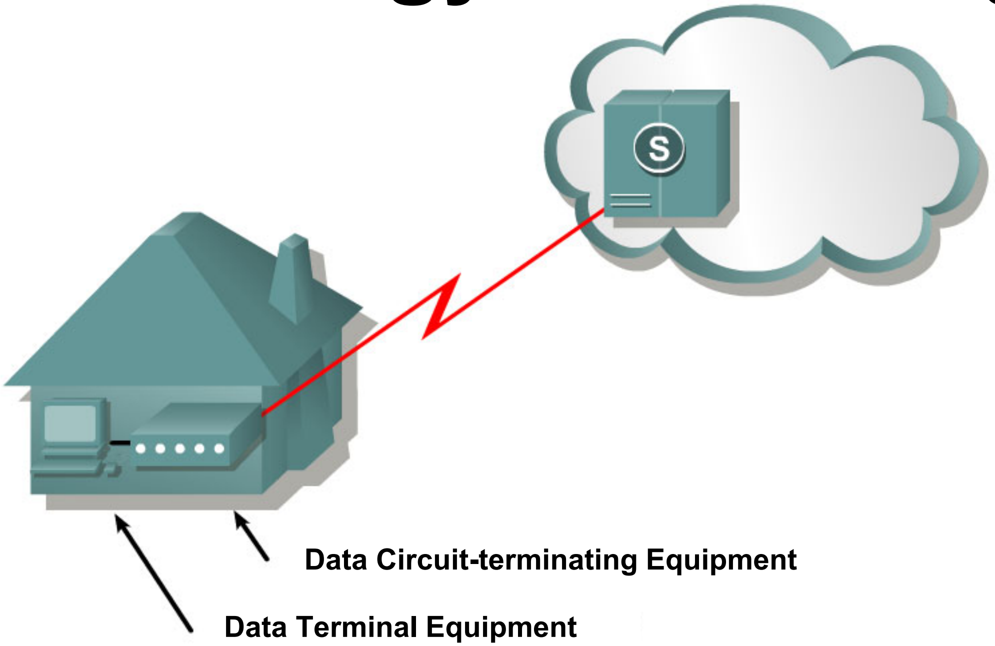

CO switch
WAN service provider toll network
Trunks and switches
CPE
Demarcation
Local loop
Point-to-point or circuit-switched connection



Demarcation point separates CPE from telephone company

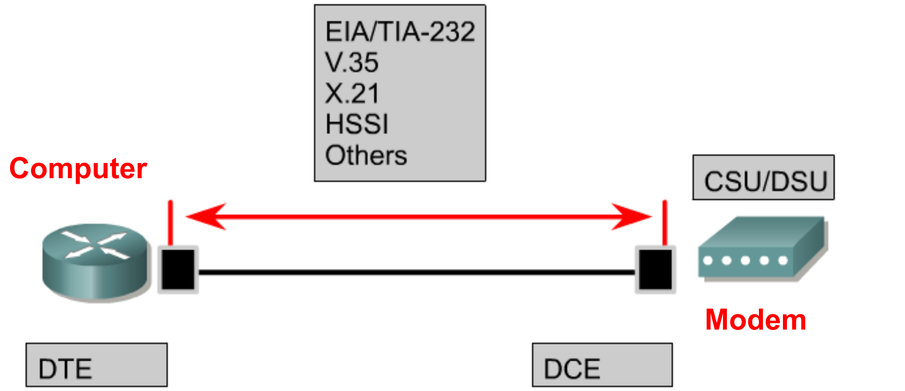
- Dialed call is connected locally to other local loops, or non-locally through a trunk to a primary center
- It then goes to a sectional center and on to a regional or international carrier center as the call travels to its destination

WAN Technology/Terminology (3/4)



- Devices that put data on the local loop are called data circuit-terminating equipment (DCE). It is also called data communications equipment or data carrier equipment
- Customer devices that pass the data to the DCE are called data terminal equipment (DTE)
- DCE primarily provides an interface for the DTE into the communication link on the WAN cloud

WAN Technology/Terminology (4/4)



EIA/TIA-232
V.35
X.21
HSSI
Others

Computer

CSU/DSU

Modem

DTE

DCE

Data Terminal Equipment
User device with interface connecting to the WAN link

Data Circuit-Terminating Equipment
End of the WAN provider's side of the communication facility

- DTE/DCE interface uses various physical layer protocols, e.g., High-Speed Serial Interface (HSSI), V.35
- These protocols establish the codes and electrical parameters the devices use to communicate with each other

Connecting a Modem to a Router

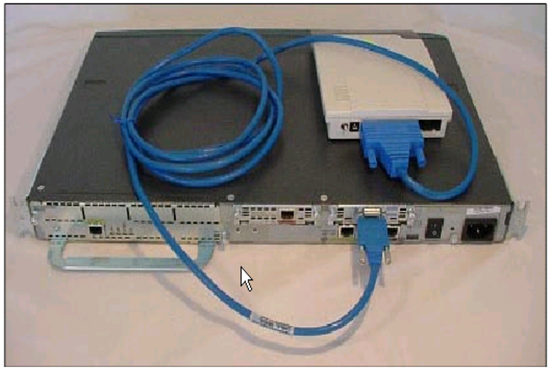
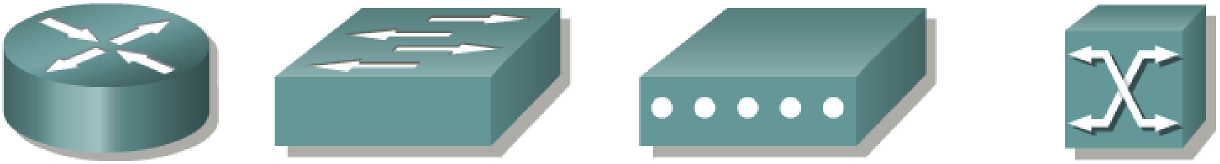


Figure: Connection between a Cisco 2620 series router and an external modem using an EIA/TIA-232 Smart Serial cable

Connecting a Modem to a Router

Figure: AUX (Auxiliary) is to connect a modem to a Cisco router's AUX port, typically a rollover cable and a RJ-45-to-DB-25 male DCE modem adapter are used

WAN Devices



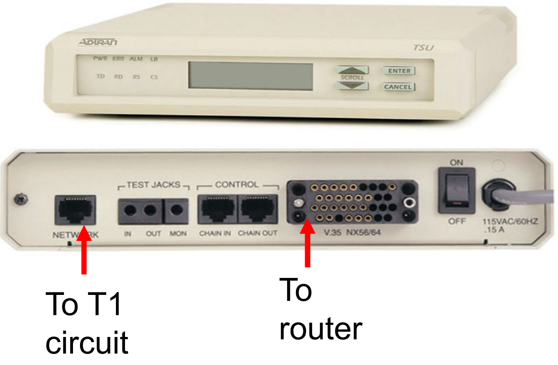
Router

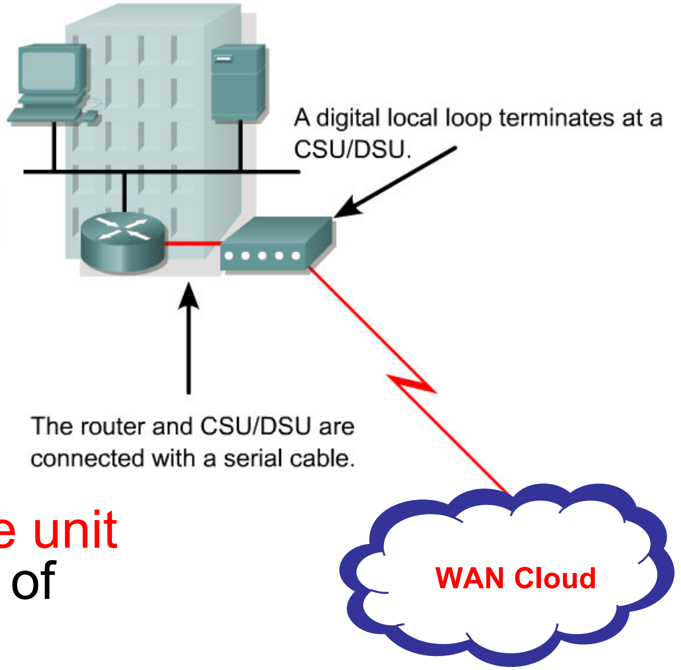
Switch (for X.25, Frame Relay, ATM)

Modem (CSU/DSU)

Communication Server

Figure: CSU/DSU may also be built into the interface card in the router

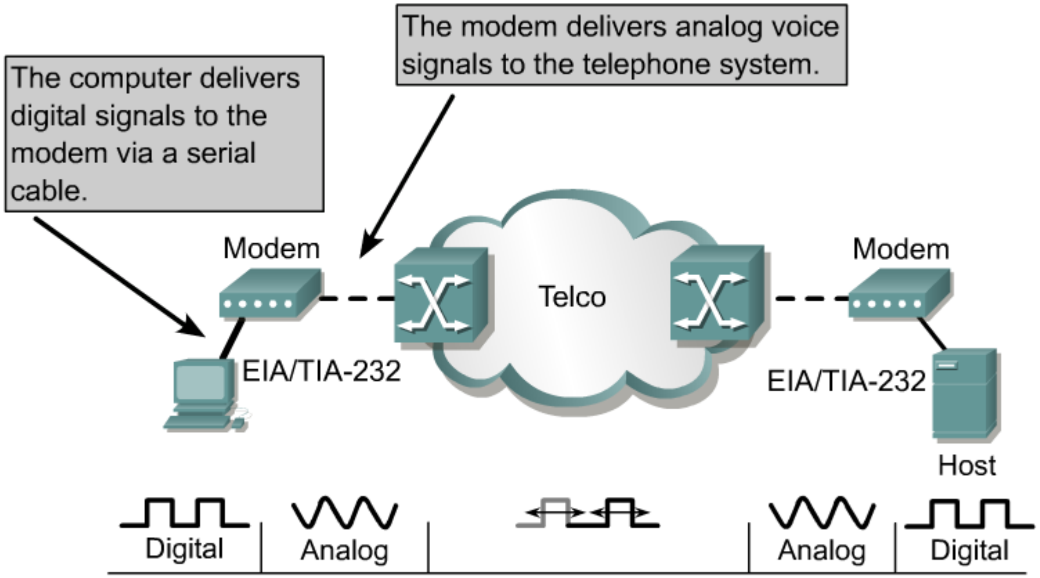



A digital local loop terminates at a CSU/DSU.
The router and CSU/DSU are connected with a serial cable.
WAN Cloud

- Channel service unit (CSU) and data service unit (DSU) that are combined into a single piece of equipment are required for digital lines

Modems

- Modems transmit data over voice-grade telephone lines by modulating and demodulating the signal
- Digital signals are superimposed on an analog voice signal that is modulated for transmission


The computer delivers digital signals to the modem via a serial cable.

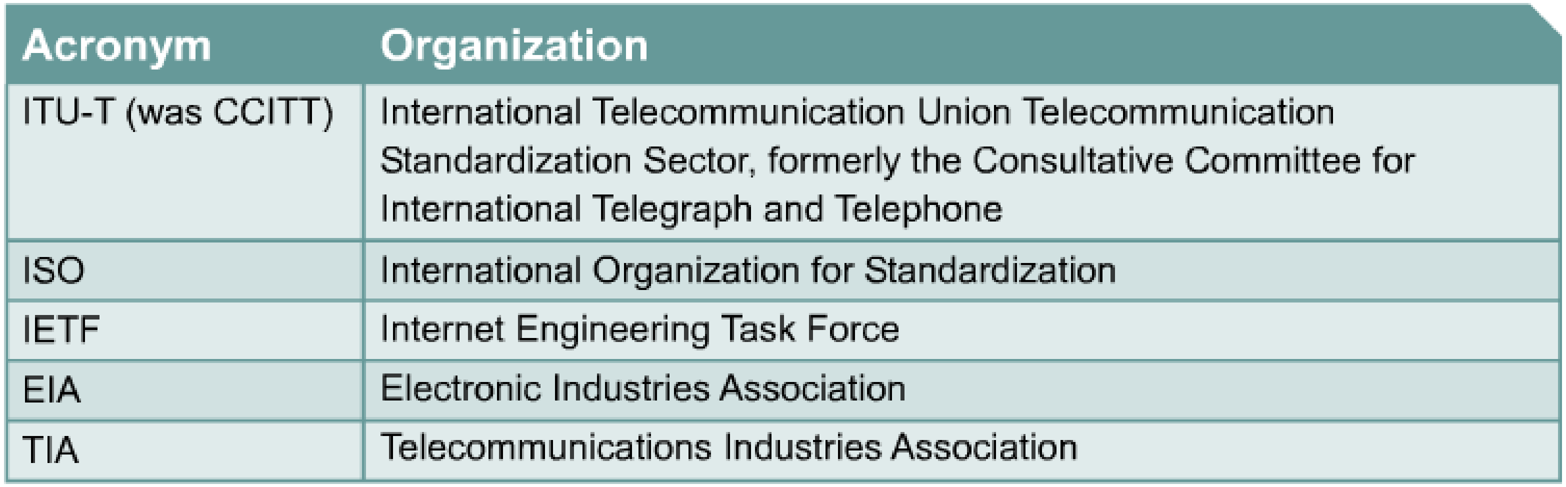
The modem delivers analog voice signals to the telephone system.

- Modulated signal can be heard as a series of whistles by turning on the internal modem speaker
- At the receiving end the analog signals are returned to their digital form, or demodulated

WAN Standards Organizations

- WAN standards typically describe both physical layer delivery methods and data link layer requirements, including physical addressing, flow control, and encapsulation

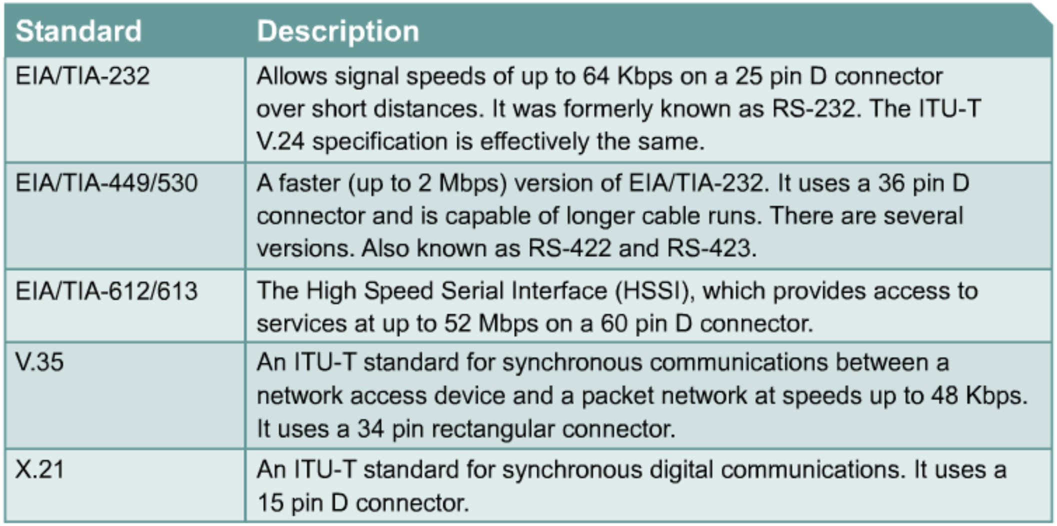
- WAN standards are defined and managed by a number of recognized authorities as below:



Acronym	Organization
ITU-T (was CCITT)	International Telecommunication Union Telecommunication Standardization Sector, formerly the Consultative Committee for International Telegraph and Telephone
ISO	International Organization for Standardization
IETF	Internet Engineering Task Force
EIA	Electronic Industries Association
TIA	Telecommunications Industries Association

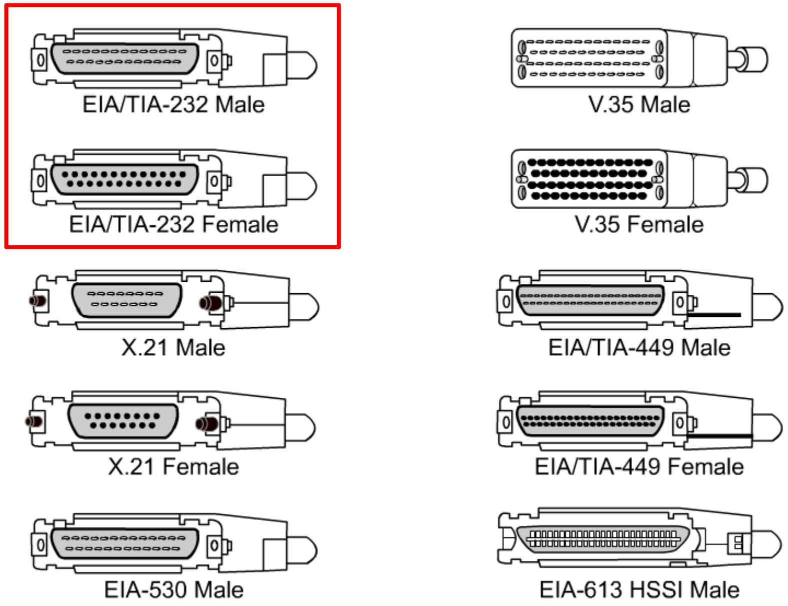
Physical Layer Standards

- Physical layer protocols describe how to provide electrical, mechanical, operational, and functional connections to the services provided by a communications service provider



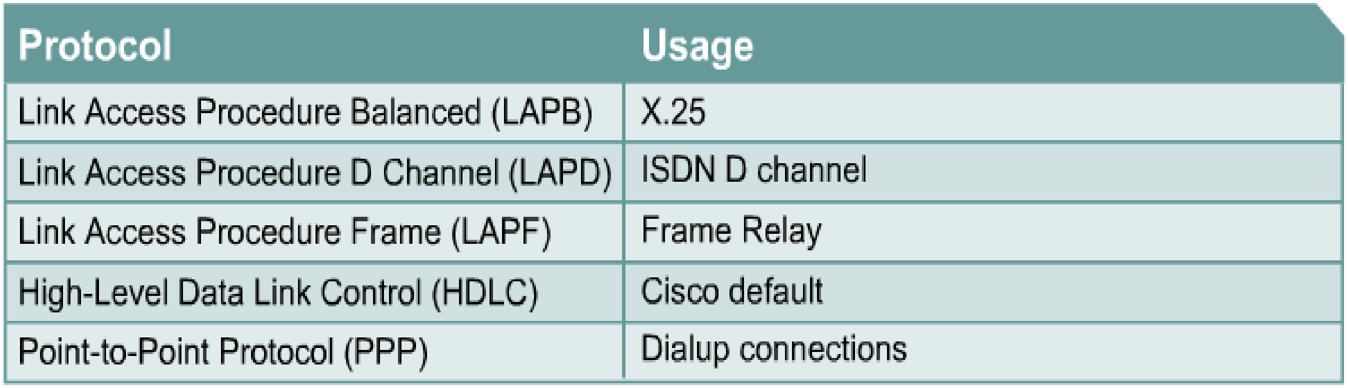
Standard	Description
EIA/TIA-232	Allows signal speeds of up to 64 Kbps on a 25 pin D connector over short distances. It was formerly known as RS-232. The ITU-T V.24 specification is effectively the same.
EIA/TIA-449/530	A faster (up to 2 Mbps) version of EIA/TIA-232. It uses a 36 pin D connector and is capable of longer cable runs. There are several versions. Also known as RS-422 and RS-423.
EIA/TIA-612/613	The High Speed Serial Interface (HSSI), which provides access to services at up to 52 Mbps on a 60 pin D connector.
V.35	An ITU-T standard for synchronous communications between a network access device and a packet network at speeds up to 48 Kbps. It uses a 34 pin rectangular connector.
X.21	An ITU-T standard for synchronous digital communications. It uses a 15 pin D connector.

Commonly well-known



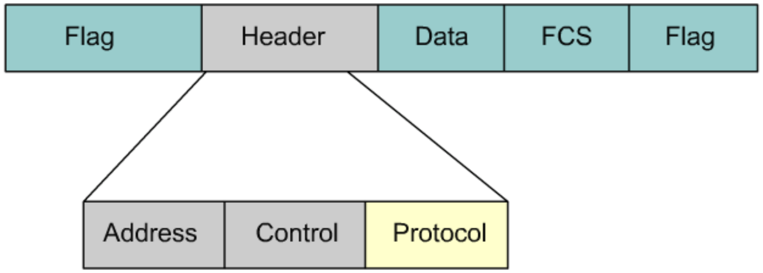
WAN Encapsulation Protocols

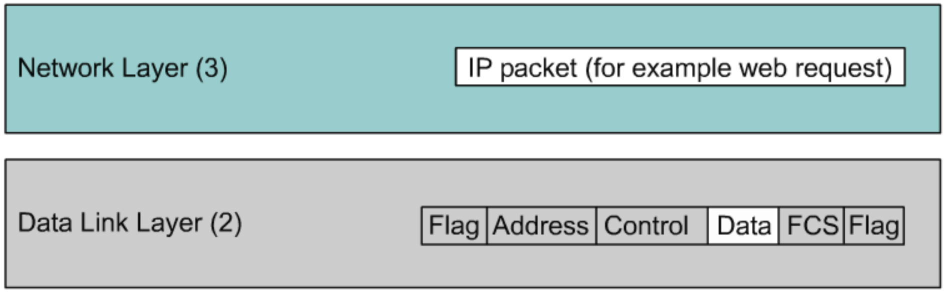
WAN Connection	Protocol (Usage)
Dedicated	PPP, HDLC (T1 Connection)
Circuit-Switched	PPP, LAPD (Dialup Connections, ISDN)
Packet-Switched	LAPB, LAPF (X.25, Frame Relay)



Protocol	Usage
Link Access Procedure Balanced (LAPB)	X.25
Link Access Procedure D Channel (LAPD)	ISDN D channel
Link Access Procedure Frame (LAPF)	Frame Relay
High-Level Data Link Control (HDLC)	Cisco default
Point-to-Point Protocol (PPP)	Dialup connections

WAN Encapsulation: HDLC Framing

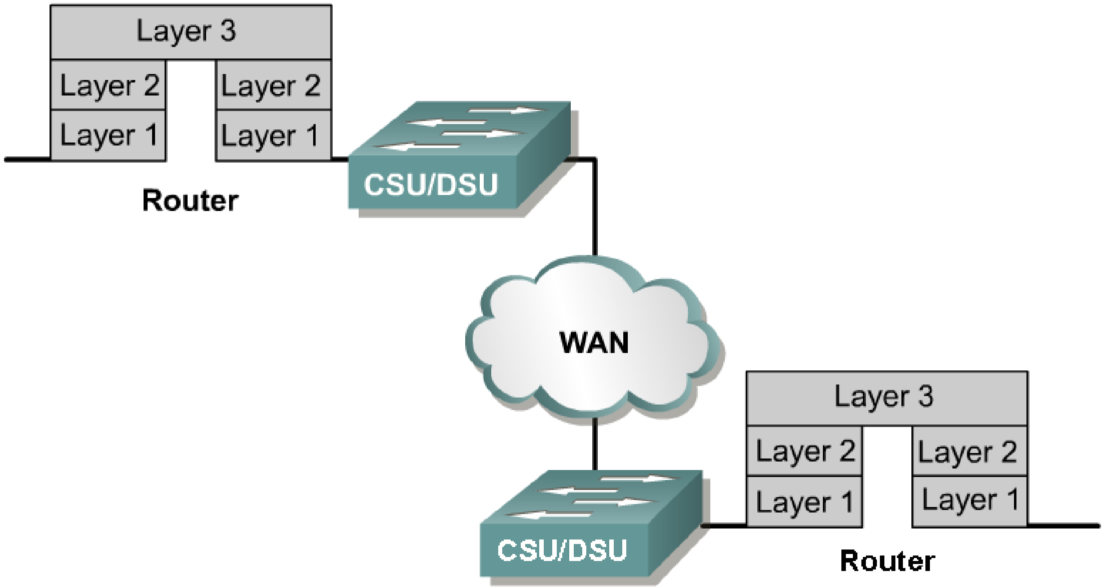




- Choice of encapsulation protocols depends on the WAN technology and the equipment
- Most framing is based on the HDLC standard
- Address field is not needed for WAN links, which are almost always point-to-point. Address field is still present and may be one or two bytes long
- Several data link protocols are used, including subsets and proprietary versions of HDLC
- Both PPP and the Cisco version of HDLC have an extra field in the header to identify the network layer protocol of the encapsulated data

WAN Communication

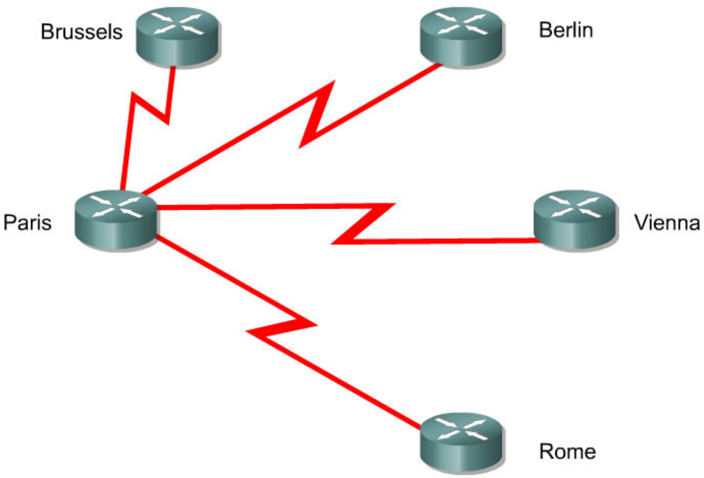
- WAN protocols operate at only the lower TWO layers of the OSI stack



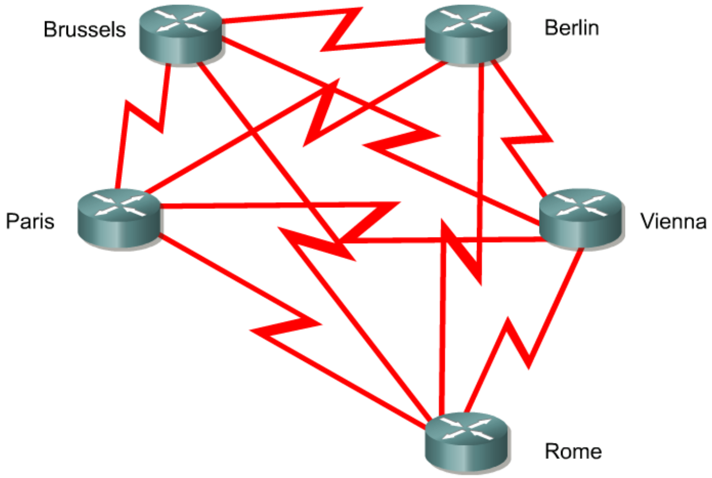
Technology	Charge	Max Bit Rate	Other
Leased Line	Distance, capacity	Unlimited	Permanent fixed capacity
Basic Telephone	Distance, time	33 kbps	Dialed, slow connection
ISDN	Distance, capacity	64 or 128 kbps <2 Mbps, PRI	Dialed, fast connection
X.25	Volume	<48 kbps	Switched fixed capacity
Frame Relay	Capacity	~~<4 Mbps~~	Permanent variable capacity
ATM	Capacity	~~<155 Mbps~~	Permanent variable capacity

>155 Mbps <45 Mbps

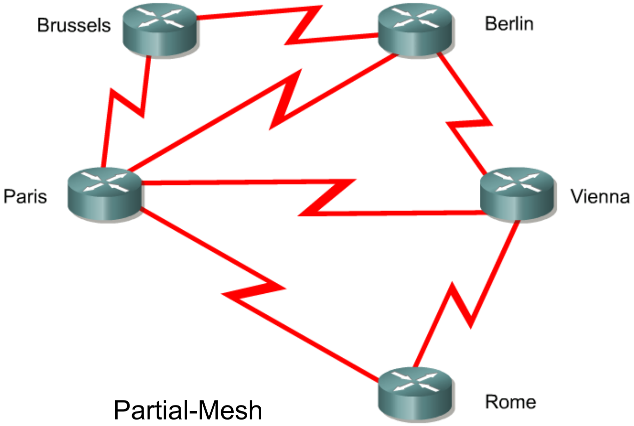
WAN Topologies



Star or Hub-and-Spoke



Full-Mesh

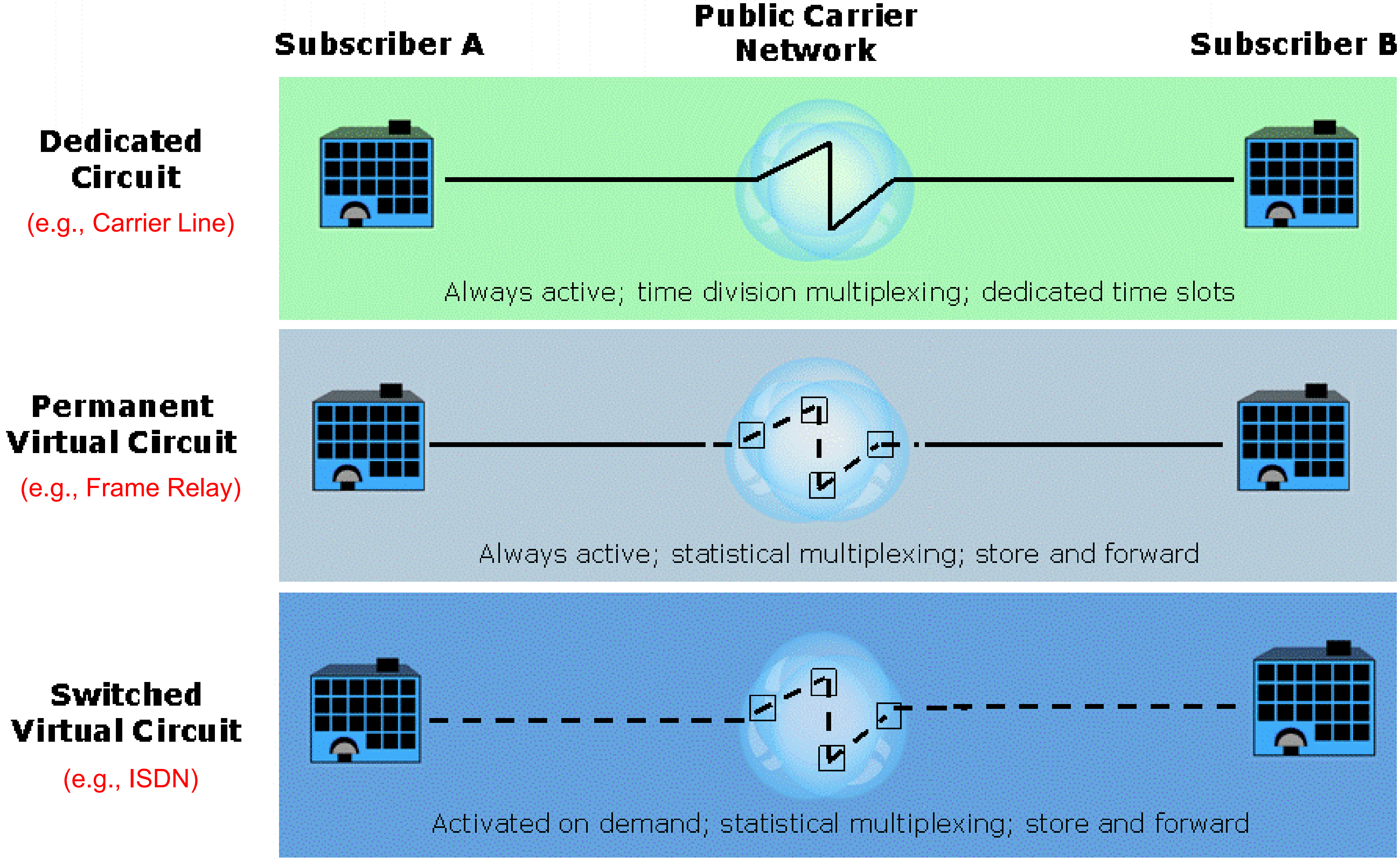


Partial-Mesh

WAN Considerations

- Many enterprise WANs have connections to Internet. This provides an alternative for inter-branch connections
- Since Internet probably exists everywhere that the enterprise has LANs, there are two ways that this traffic can be carried
  - Each LAN can have a connection to its local ISP, or
  - There can be a single connection from one of the core routers to an ISP
- Advantage: traffic is carried on the Internet rather than on the enterprise network, possibly leading to smaller WAN links
- Disadvantage: by permitting multiple links, the whole enterprise WAN is open to Internet-based attacks

Types of WAN Circuits



Dedicated Circuit

(e.g., Carrier Line)

Always active; time division multiplexing; dedicated time slots

Permanent Virtual Circuit

(e.g., Frame Relay)

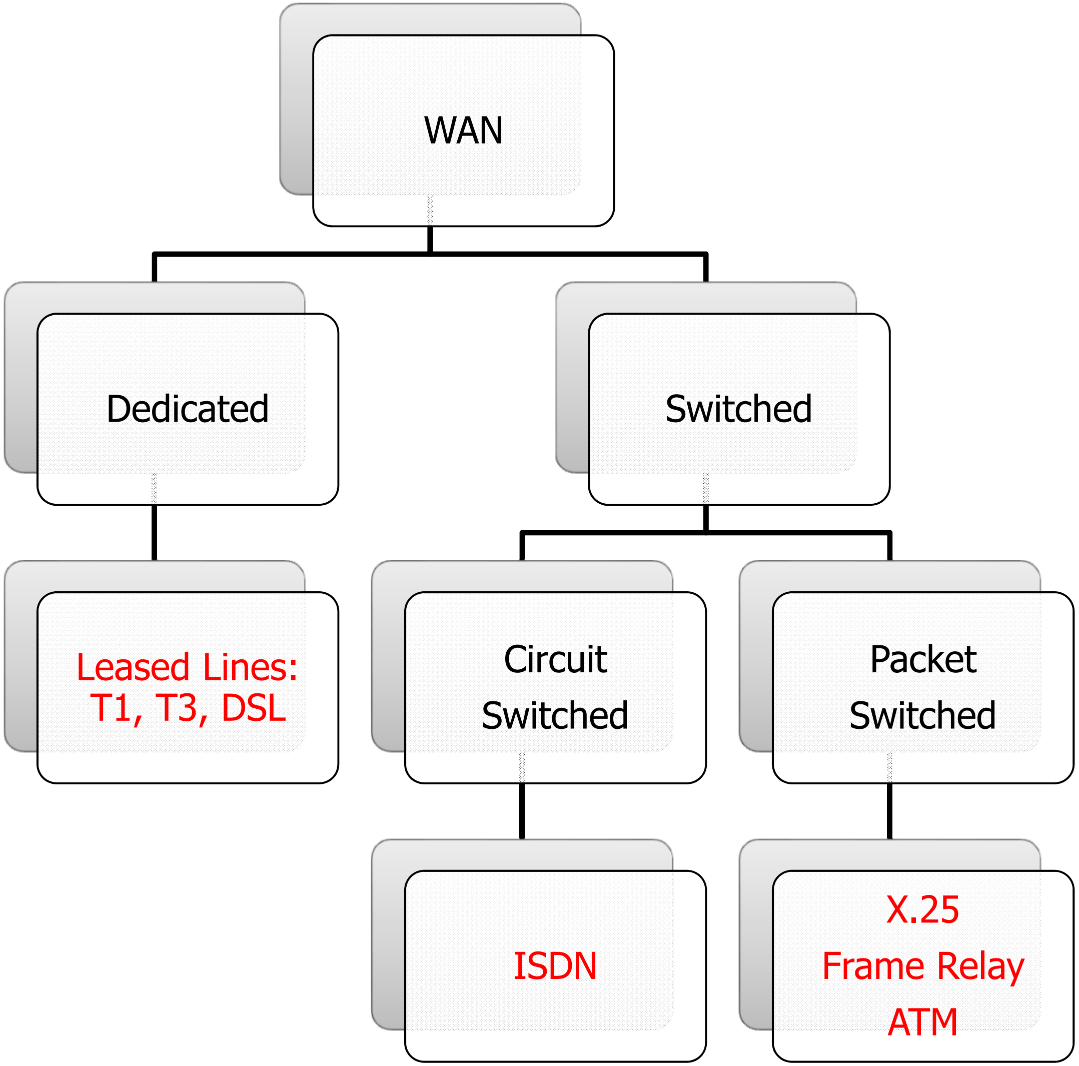
Always active; statistical multiplexing; store and forward

Switched Virtual Circuit

(e.g., ISDN)

Activated on demand; statistical multiplexing; store and forward

WAN Link Options



Public Switched Telephone Network

- PSTN
  - Network of lines, carrier equipment providing telephone service
  - POTS (plain old telephone service)
  - Encompasses entire telephone system
  - Originally: analog traffic
  - Today: digital data, computer controlled switching
- Dial-up connection
  - Used early on
  - Modem connects computer to distant network
    - Finite time period

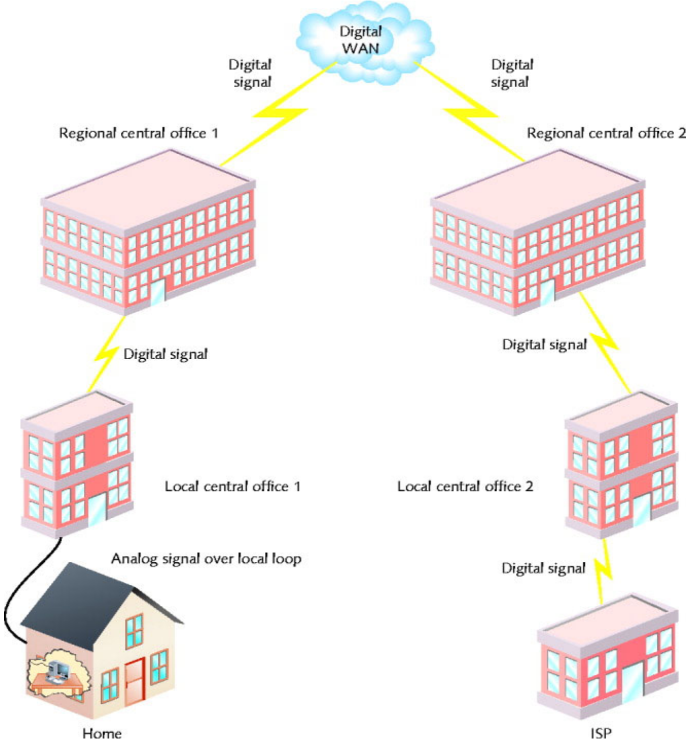


Figure: Long-distance dial-up connection

PSTN (cont.)

- PSTN elements
  - Cannot handle digital transmission
    - Requires modem
- Signal travels path btw modems
  - Over carrier's network
    - Includes CO (central office), remote switching facility
    - Signal converts back to digital pulses
- CO (central office)
  - Where telephone company terminates lines
  - Switches calls between different locations
- Local loop (last mile)
  - Portion connecting residence, business to nearest CO
    - Most likely uses copper wire, carries analog signal

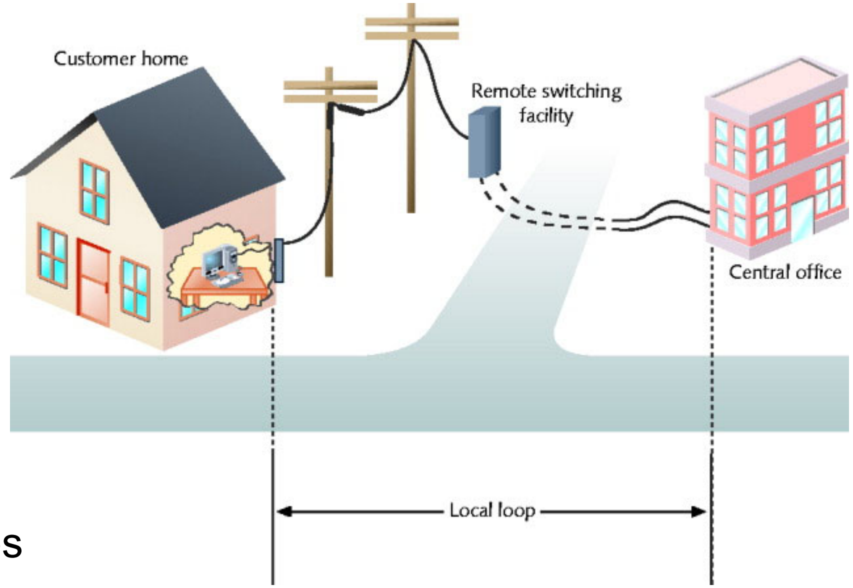


Figure: Local loop portion of the PSTN

- Advantage
  - Ubiquity, ease of use, low cost
- Disadvantage
  - Some circuit switching used
  - Marginal security

X.25

- X.25 ITU standard
  - Analog, packet-switching technology
    - Designed for long distance
  - Original standard: mid 1970s
    - Mainframe to remote computers: 64 Kbps throughput
  - Update: 1992
    - 2.048 Mbps throughput
    - Client, servers over WANs
  - Verifies transmission at every node
    - Excellent flow control, ensures data reliability
    - Slow and unreliable for time-sensitive applications

Frame Relay

- Frame relay
  - Updated X.25: digital, packet-switching
  - Protocols operate at data link layer
    - Supports multiple Network, transport layer protocols
- Both perform error checking
  - Frame relay: no reliable data delivery guarantee
  - X.25: errors fixed or retransmitted
- Throughput
  - X.25: 64 Kbps to 45 Mbps
  - Frame relay: customer chooses

X.25 and Frame Relay

- Both use virtual circuits
  - Based on potentially disparate physical links
    - Logically appear direct
  - Advantage: efficient bandwidth use
- Both configurable as SVCs (switched virtual circuits)
  - Connection established for transmission, terminated when complete
- Both configurable as PVCs (permanent virtual circuits)
  - Connection established before transmission, remains after transmission

X.25 and Frame Relay (cont.)

- Frame relay and X.25 advantage
  - Pay for bandwidth required
  - Less expensive technology
  - Long-established worldwide standard
- Frame relay and X.25 disadvantage
  - Throughput variability
    - Due to shared lines

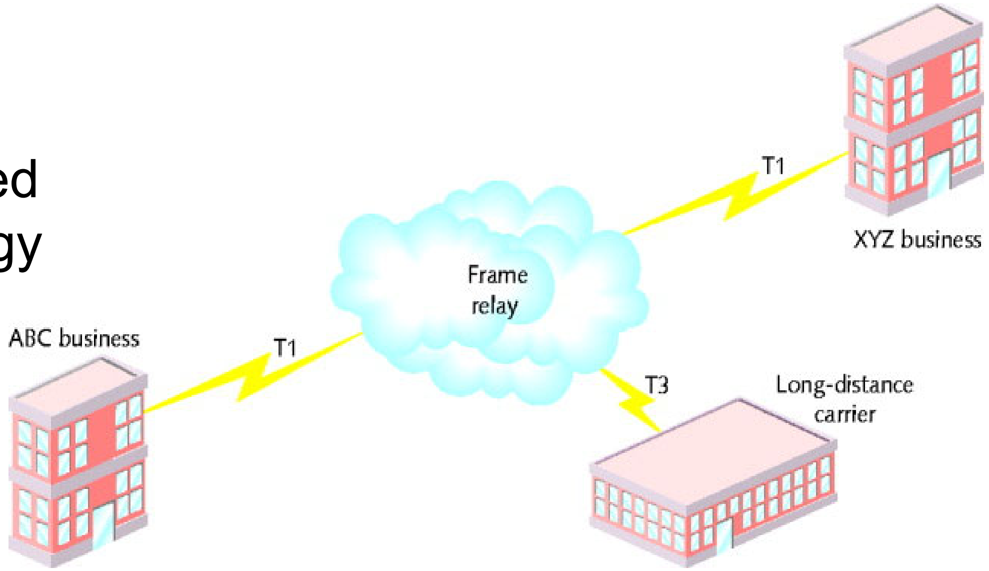


Figure : WAN using frame relay

- Frame relay and X.25 easily upgrade to T-carrier dedicated lines
  - Due to same connectivity equipment

Integrated Services Digital Network

- Digital data transmitted over PSTN
- Gained popularity: 1990s
  - Connecting WAN locations
    - Exchanges data, voice signals
- Protocols at physical, data link, transport layers
  - Signaling, framing, connection setup and termination, routing, flow control, error detection and correction
- Relies on PSTN for transmission medium
- Dial-up or dedicated connections
  - Dial-up relies exclusively on digital transmission

ISDN (cont.)

- Single line
  - Simultaneously: two voice calls, one data connection
- Two channel types
  - B channel: “bearer”
    - Circuit switching for voice, video, audio: 64 Kbps
  - D channel: “data”
    - Packet-switching for call information: 16 or 64 Kbps
- BRI (Basic Rate Interface) connection
- PRI (Primary Rate Interface) connection

ISDN (cont.)

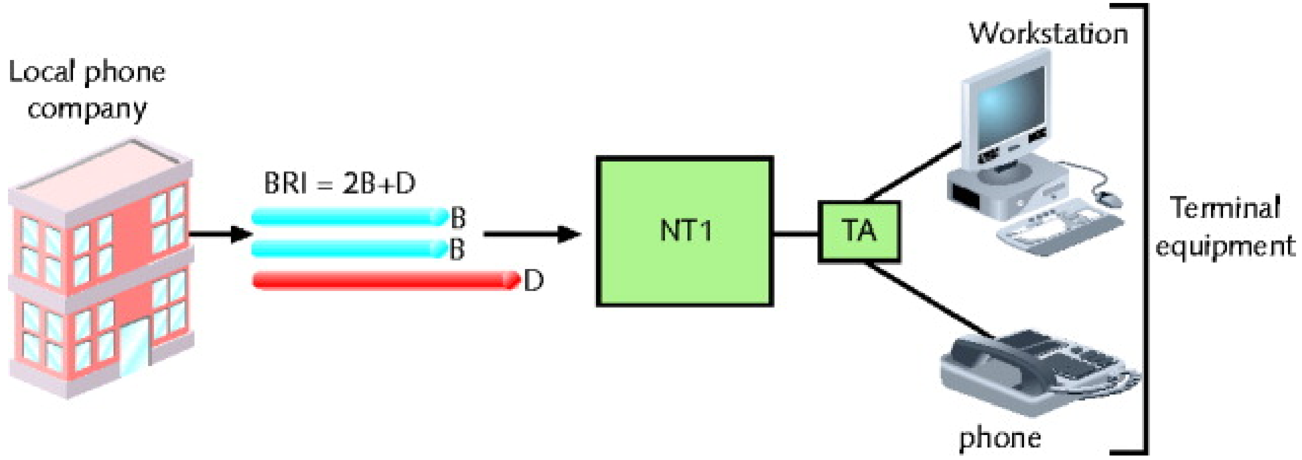


Figure: BRI link

- BRI: two B channels, one D channel (2B+D)
  - B channels treated as separate connections
    - Carry voice and data
  - Maximum throughput: 144 Kbps (128 + 16)
- Bonding
  - Two 64-Kbps B channels combined
    - Achieve 128 Kbps

ISDN (cont.)

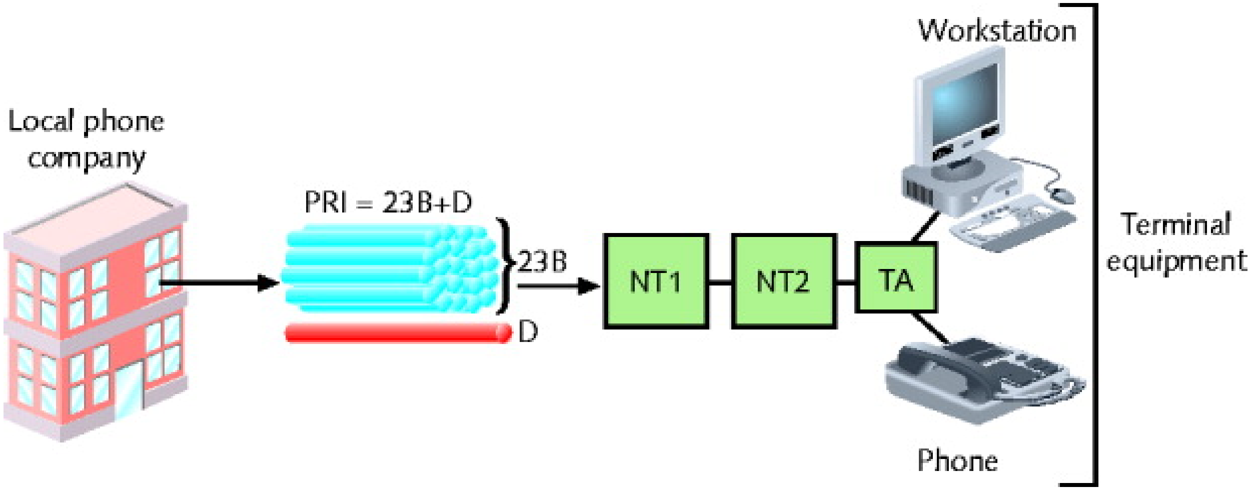


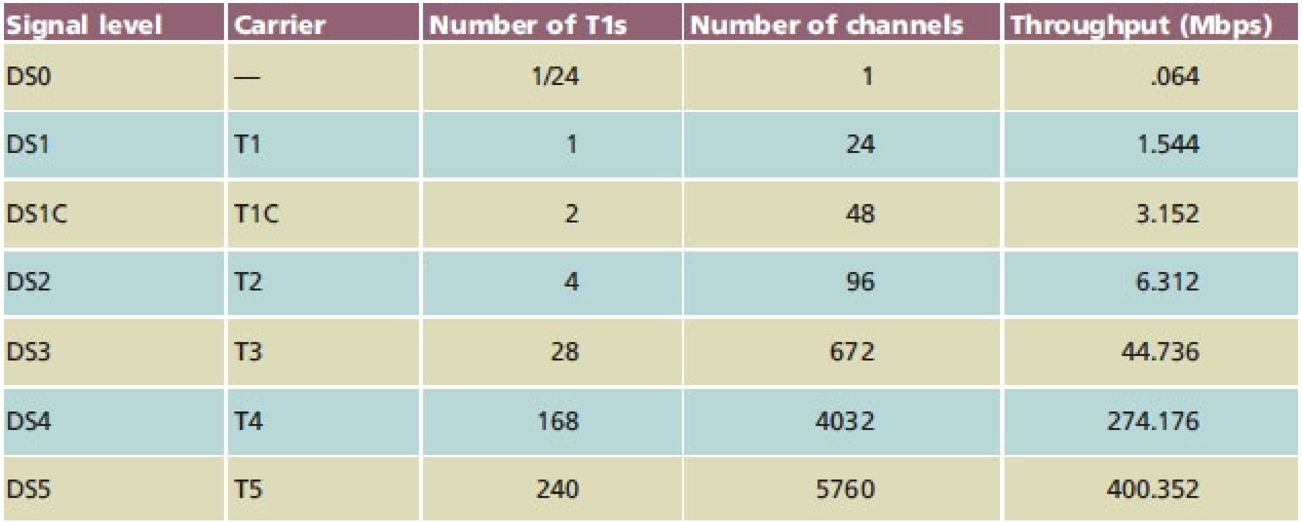
Figure: PRI link

- PRI: 23 B channels, one 64-Kbps D channel (23B+D)
  - Separate B channels independently carry voice, data
  - Maximum throughput: 1.544 Mbps
- PRI and BRI may interconnect

T-Carriers

- T1s, fractional T1s, T3s
- Physical layer operation
- Single channel divided into multiple channels
  - Using TDM (time division multiplexing) over two wire pairs
- Medium
  - Telephone wire, fiber-optic cable, wireless links

Type of T-Carriers



Signal level	Carrier	Number of T1s	Number of channels	Throughput (Mbps)
DS0	—	1/24	1	.064
DS1	T1	1	24	1.544
DS1C	T1C	2	48	3.152
DS2	T2	4	96	6.312
DS3	T3	28	672	44.736
DS4	T4	168	4032	274.176
DS5	T5	240	5760	400.352

Table: Carrier specifications

- Many available
  - Most common: T1 and T3
- T1: 24 voice or data channels
  - Maximum data throughput: 1.544 Mbps
- T3: 672 voice or data channels
  - Maximum data throughput: 44.736 Mbps (45 Mbps)
- T-carrier speed dependent on signal level
  - Physical layer electrical signaling characteristics
  - DS0 (digital signal, level 0)
    - One data, voice channel

Type of T-Carriers (cont.)

- T1 use
  - Connects branch offices, connects to carrier
  - Connects telephone company COs, ISPs
- T3 use
  - Data-intensive businesses
- T3 provides 28 times more throughput (expensive)
  - Multiple T1's may accommodate needs
- T1 costs vary by region
- Fractional T1 lease
  - Use some T1 channels, charged accordingly

T-Carrier Connectivity

- T-carrier line requires connectivity hardware
  - Customer site, switching facility
  - Purchased or leased
  - Cannot be used with other WAN transmission methods
- T-carrier line requires different media
  - Throughput dependent
- Wiring
  - Plain telephone wire
    - UTP or STP copper wiring
    - STP preferred for clean connection
  - Coaxial cable, microwave, fiber-optic cable
  - T1s using STP require repeater every 6000 feet
  - Multiple T1s
    - Coaxial cable, microwave, fiber-optic cabling
  - T3s require microwave, fiber-optic cabling

T-Carrier Connectivity (cont.)

- Smart Jack
  - Terminate T-carrier wire pairs
    - Customer’s demarc (demarcation point)
    - Inside or outside building
  - Connection monitoring point

Figure: T1 smart jack

Figure : CSU/DSU

T-Carrier Connectivity (cont.)

- CSU/DSU (Channel Service Unit/Data Service Unit)
  - Two separate devices
  - Combined into single stand-alone device
    - Interface card
  - T1 line connection point
    - At customer's site
- CSU
  - Provides digital signal termination
  - Ensures connection integrity
- DSU
  - Converts T-carrier frames into frames LAN can interpret (vice versa)
  - Connects T-carrier lines with terminating equipment
  - Incorporates multiplexer

T-Carrier Connectivity (cont.)

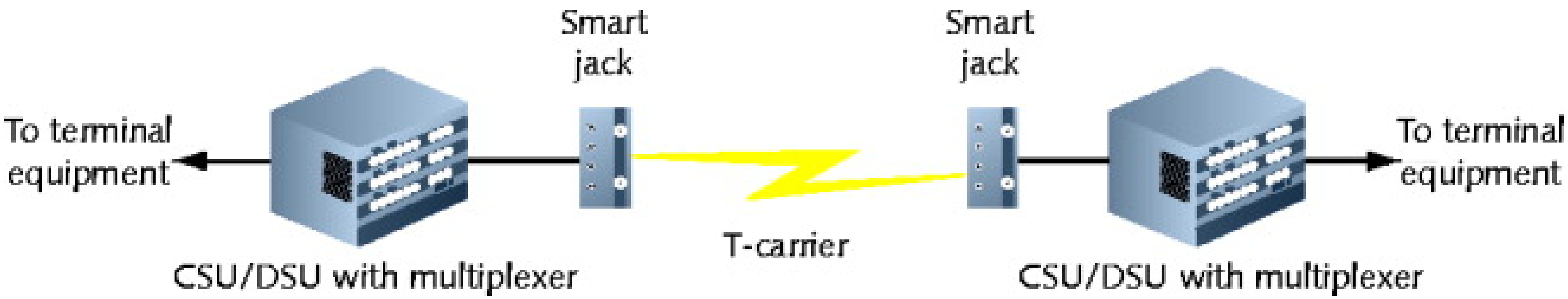


Figure: Point-to-point T-carrier connection

- Incoming T-carrier line
  - Multiplexer separates combined channels
- Outgoing T-carrier line
  - Multiplexer combines multiple LAN signals
- Terminal equipment
  - Switches, routers, bridges
  - Best option: router, Layer 3 or higher switch
    - Accepts incoming CSU/DSU signals
    - Translates Network layer protocols
    - Directs data to destination
- CSU/DSU may be integrated with router, switch
  - Expansion card
  - Faster signal processing, better performance
  - Less expensive, lower maintenance solution

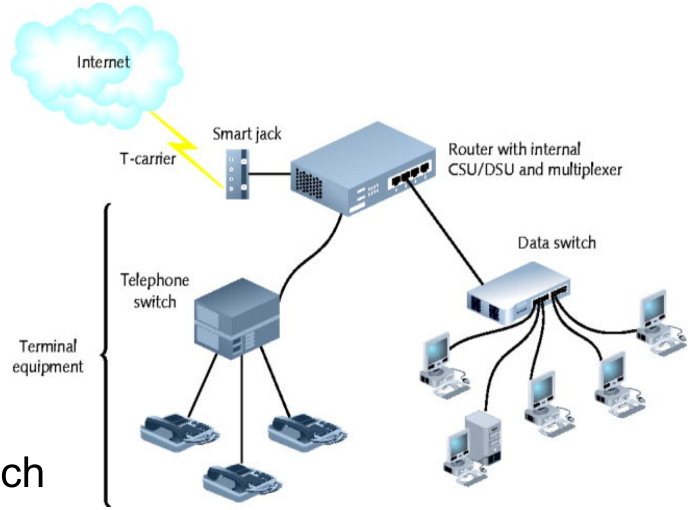


Figure: T-carrier connecting to a LAN through a router

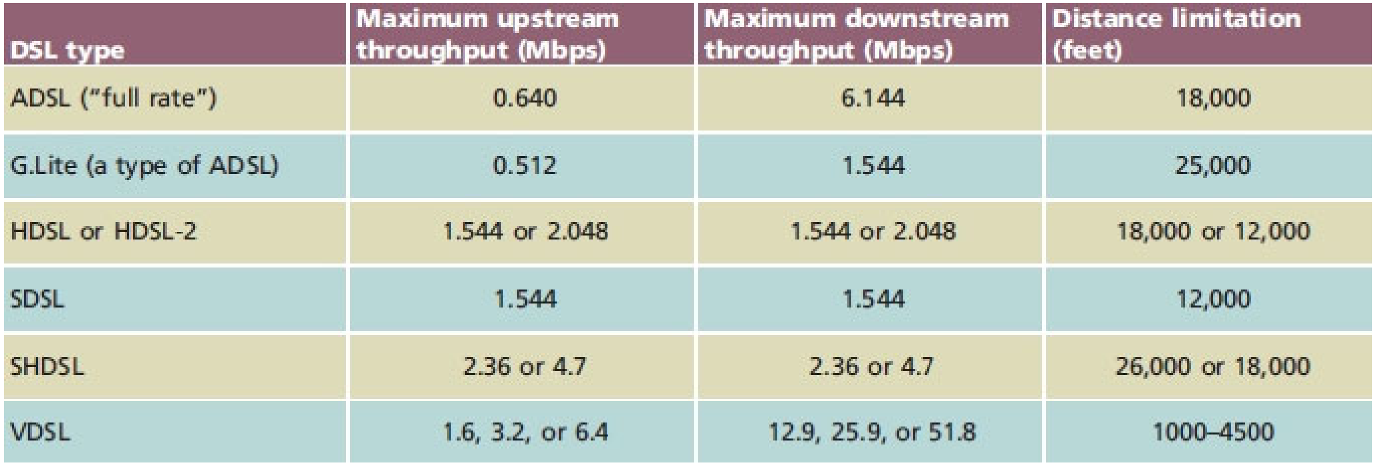
Digital Subscriber Line (DSL)

- Operates over PSTN
- Directly competes with ISDN, T1 services
- Requires repeaters for longer distances
- Best suited for WAN local loop
- Supports multiple data, voice channels
  - Over single line
  - Higher, inaudible telephone line frequencies
- Uses advanced data modulation techniques
  - Data signal alters carrier signal properties
  - Amplitude or phase modulation

Types of DSL

- xDSL refers to all DSL varieties
  - ADSL, G.Lite, HDSL, SDSL, VDSL, SHDSL
- Two DSL categories
  - Asymmetrical and symmetrical
- Downstream
  - Data travels from carrier's switching facility to customer
- Upstream
  - Data travels from customer to carrier's switching facility
- Downstream, upstream throughput rates may differ
  - Asymmetrical
    - More throughput in one direction
    - Downstream throughput higher than upstream throughput
    - Best use: video conferencing, web surfing
  - Symmetrical
    - Equal capacity for upstream, downstream data
    - Examples : HDSL, SDSL, SHDSL
    - Best use: uploading, downloading significant data amounts

Types of DSL (cont.)



DSL type	Maximum upstream throughput (Mbps)	Maximum downstream throughput (Mbps)	Distance limitation (feet)
ADSL ("full rate")	0.640	6.144	18,000
G.Lite (a type of ADSL)	0.512	1.544	25,000
HDSL or HDSL-2	1.544 or 2.048	1.544 or 2.048	18,000 or 12,000
SDSL	1.544	1.544	12,000
SHDSL	2.36 or 4.7	2.36 or 4.7	26,000 or 18,000
VDSL	1.6, 3.2, or 6.4	12.9, 25.9, or 51.8	1000–4500

Table: Comparison of DSL types

- How DSL types vary
  - Data modulation techniques
  - Capacity
  - Distance limitations
  - Use of PSTN

DSL Connectivity

- ADSL: common example on home computer
  - Establish TCP connection
  - Transmit through DSL modem
    - Internal or external
    - Splitter separates incoming voice, data signals
    - May connect to hub, switch, router
  - DSL modem forwards modulated signal to local loop
    - Signal continues over four-pair UTP wire
    - Distance less than 18,000 feet: signal combined with other modulated signals in telephone switch
  - Carrier's remote switching facility
    - Splitter separates data signal from voice signals
    - Request sent to DSLAM (DSL access multiplexer)
    - Request issued from carrier's network to Internet backbone

Figure: DSL modem

DSL Connectivity (cont.)

- DSL competition
  - T1, ISDN, broadband cable
- DSL installation
  - Hardware, monthly access costs
    - Slightly less than ISDN, significantly less than T1s
- DSL drawbacks
  - Not available in all areas
  - Upstream throughput lower than broadband cable
    - Consumers use broadband Internet access service

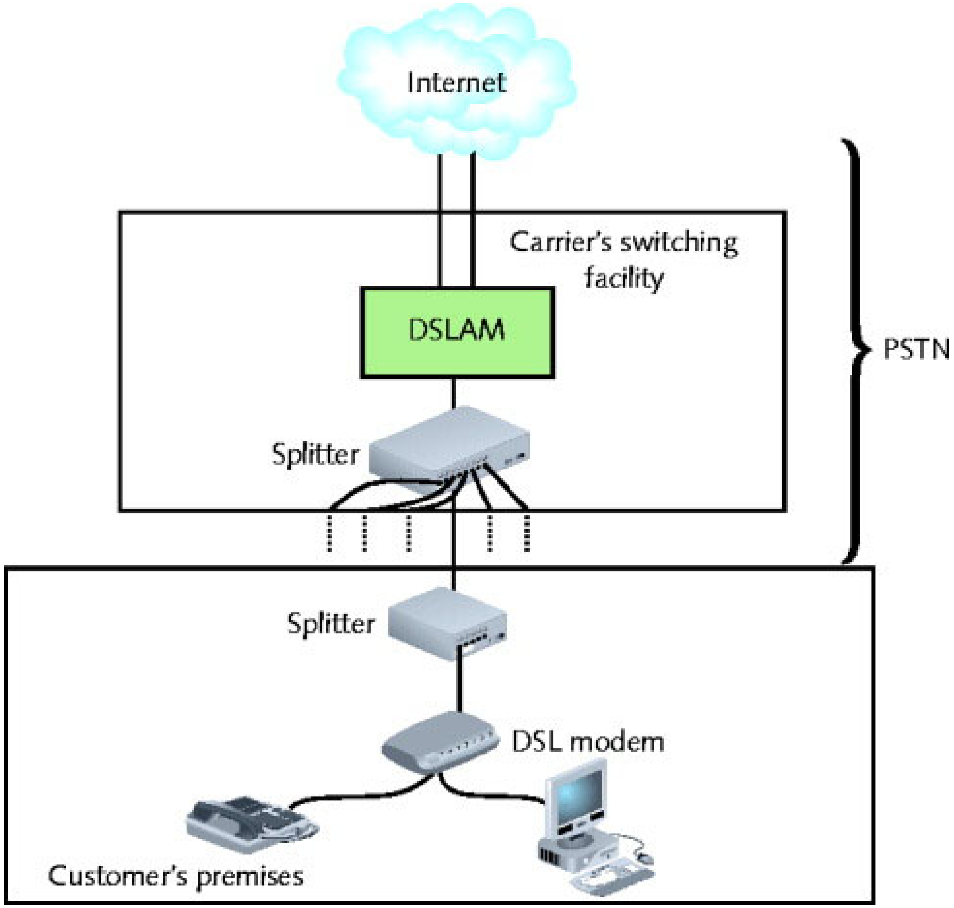


Figure: DSL connection

Asynchronous Transfer Mode (ATM)

- Functions in Data Link layer
- Asynchronous communications method
  - Nodes do not conform to predetermined schemes
    - Specifying data transmissions timing
  - Each character transmitted
    - Start and stop bits
- Specifies Data Link layer framing techniques
- Fixed packet size
  - Sets ATM apart from Ethernet
  - Packet (cell)
    - 48 data bytes plus 5-byte header
- Smaller packet size requires more overhead
  - Decrease potential throughput
  - Cell efficiency compensates for loss

ATM (cont.)

- ATM relies on virtual circuits
  - ATM considered packet-switching technology
  - Virtual circuits provide circuit switching advantage
    - Reliably available point-to-point connection
  - Reliable connection
- Allows specific QoS guarantee
  - Important for time-sensitive applications
- Compatibility
  - Other leading network technologies
  - Cells support multiple higher-layer protocol
  - LANE (LAN Emulation)
    - Allows integration with Ethernet, token ring network
    - encapsulates incoming Ethernet or token ring frames
    - Converts to ATM cells for transmission
- Throughput is 25 Mbps to 622 Mbps
- Cost is relatively expensive

Synchronous Optical Network (SONET)

- Four key strengths
  - WAN technology integration
  - Fast data transfer rates
  - Simple link additions, removals
  - High degree of fault tolerance
- Synchronous
  - Data transmitted, received by nodes conforms to timing scheme
- Advantage
  - Interoperability

SONET (cont.)

- Fault tolerance
  - Double-ring topology over fiber-optic cable
- SONET ring
  - Begins, ends at telecommunications carrier's facility
  - Connects organization's multiple WAN sites in ring fashion
  - Connect with multiple carrier facilities
    - Additional fault tolerance
  - Terminates at multiplexer
    - Easy SONET ring connection additions, removals

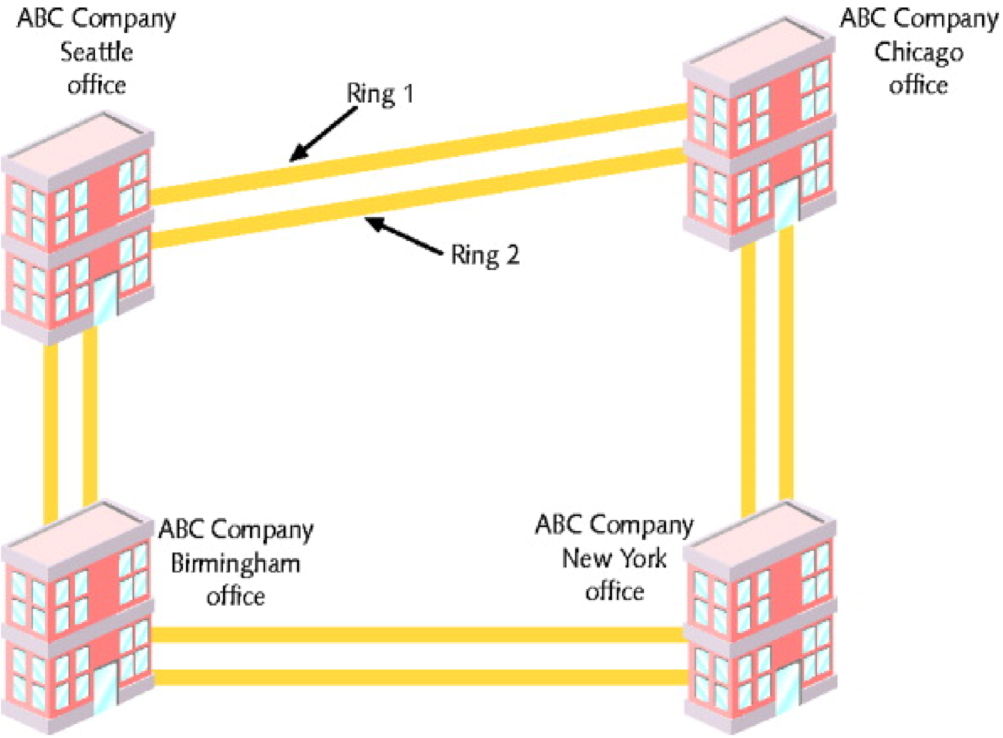

ABC Company Seattle office
Ring 1
ABC Company Chicago office
Ring 2
ABC Company Birmingham office
ABC Company New York office

Figure: SONET ring

SONET (cont.)

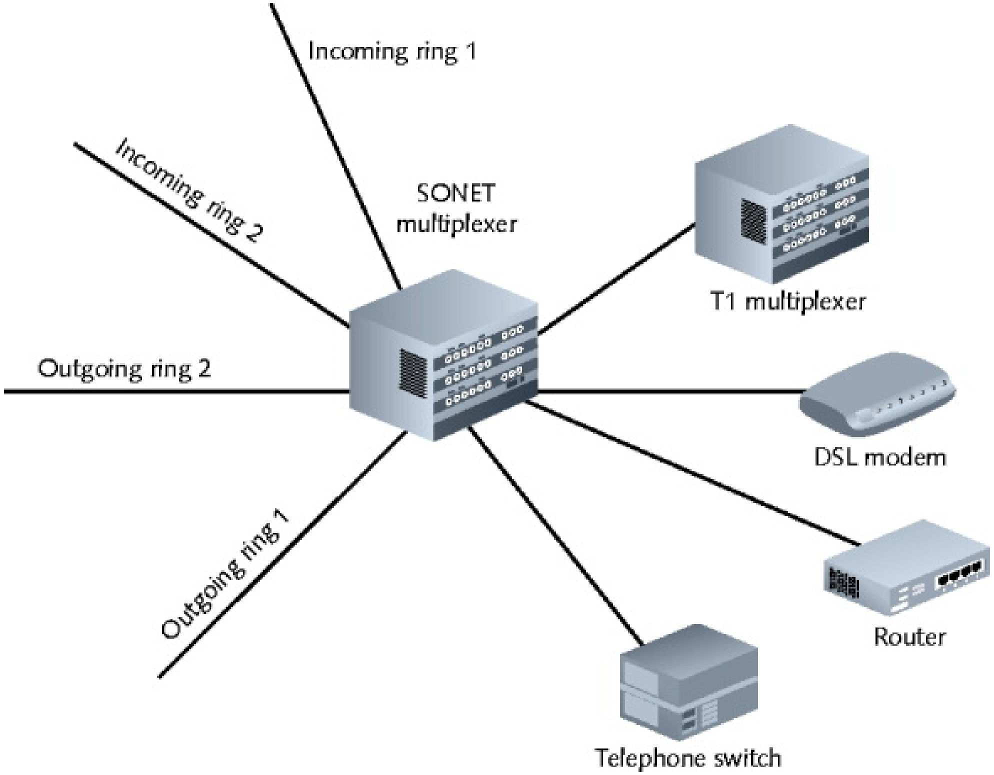
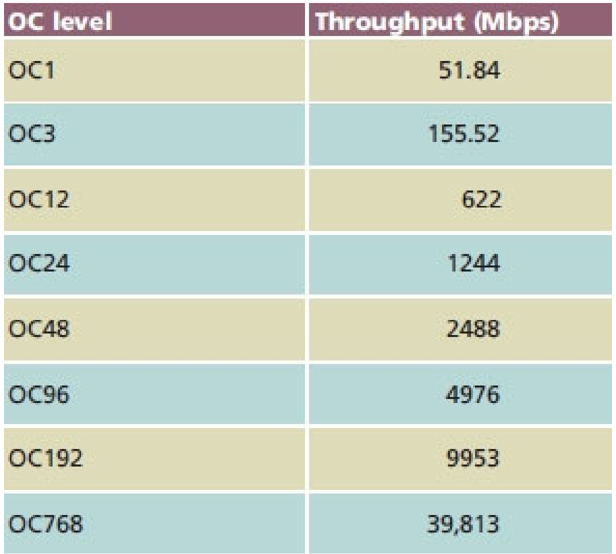


Figure: SONET connectivity

SONET (cont.)



OC level	Throughput (Mbps)
OC1	51.84
OC3	155.52
OC12	622
OC24	1244
OC48	2488
OC96	4976
OC192	9953
OC768	39,813

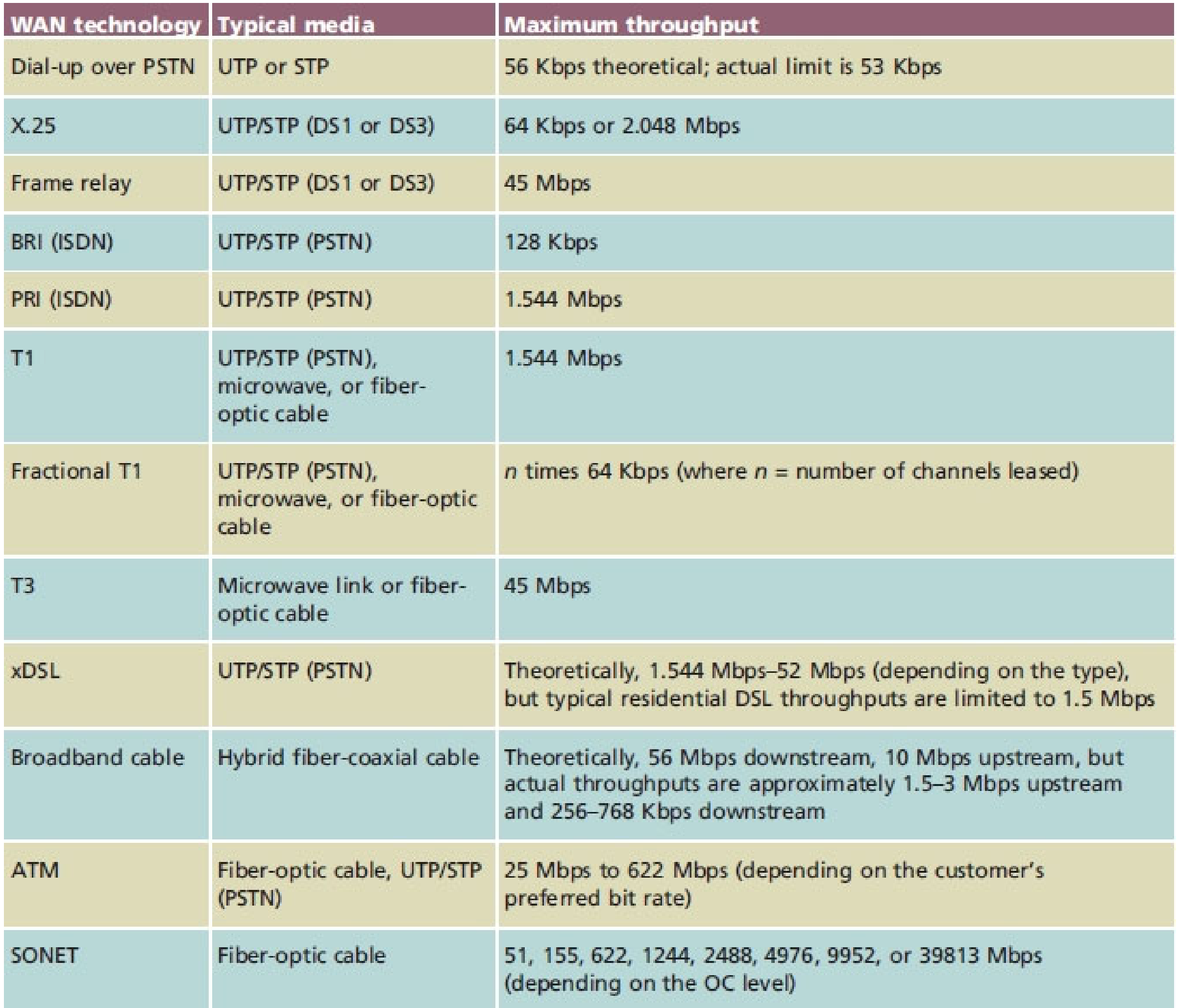
Table: SONET OC levels

- Data rate
  - Indicated by OC (Optical Carrier) level

SONET (cont.)

- Implementation
  - Large companies
  - Long-distance companies
    - Linking metropolitan areas and countries
  - ISPs
    - Guarantying fast, reliable Internet access
  - Telephone companies
    - Connecting Central Offices
- Cost
  - Expensive

WAN Technologies Comparison

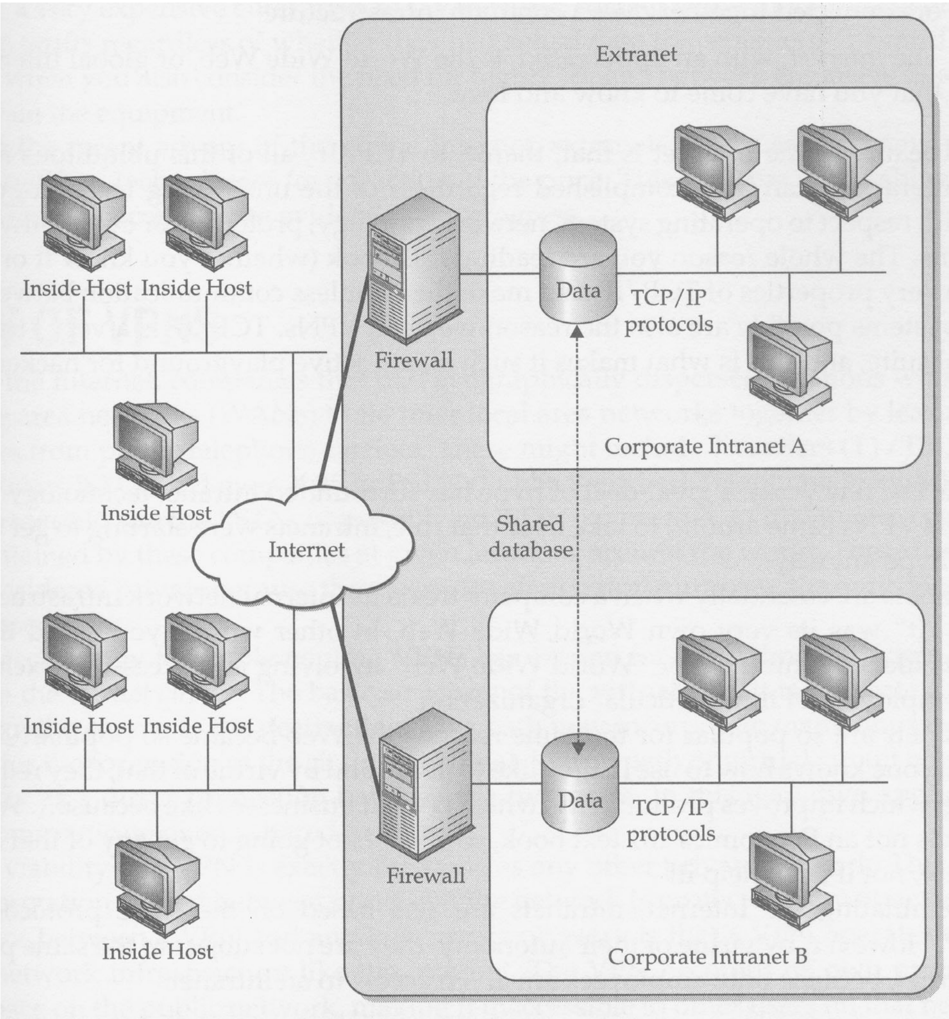


WAN technology	Typical media	Maximum throughput
Dial-up over PSTN	UTP or STP	56 Kbps theoretical; actual limit is 53 Kbps
X.25	UTP/STP (DS1 or DS3)	64 Kbps or 2.048 Mbps
Frame relay	UTP/STP (DS1 or DS3)	45 Mbps
BRI (ISDN)	UTP/STP (PSTN)	128 Kbps
PRI (ISDN)	UTP/STP (PSTN)	1.544 Mbps
T1	UTP/STP (PSTN), microwave, or fiber-optic cable	1.544 Mbps
Fractional T1	UTP/STP (PSTN), microwave, or fiber-optic cable	*n* times 64 Kbps (where *n* = number of channels leased)
T3	Microwave link or fiber-optic cable	45 Mbps
xDSL	UTP/STP (PSTN)	Theoretically, 1.544 Mbps–52 Mbps (depending on the type), but typical residential DSL throughputs are limited to 1.5 Mbps
Broadband cable	Hybrid fiber-coaxial cable	Theoretically, 56 Mbps downstream, 10 Mbps upstream, but actual throughputs are approximately 1.5–3 Mbps upstream and 256–768 Kbps downstream
ATM	Fiber-optic cable, UTP/STP (PSTN)	25 Mbps to 622 Mbps (depending on the customer's preferred bit rate)
SONET	Fiber-optic cable	51, 155, 622, 1244, 2488, 4976, 9952, or 39813 Mbps (depending on the OC level)

Table: Comparison of WAN technology throughputs

Internet? Intranet ? Extranet ?

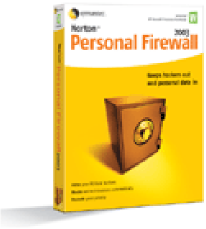
- Use Firewall and VPN technologies to build corporate networks



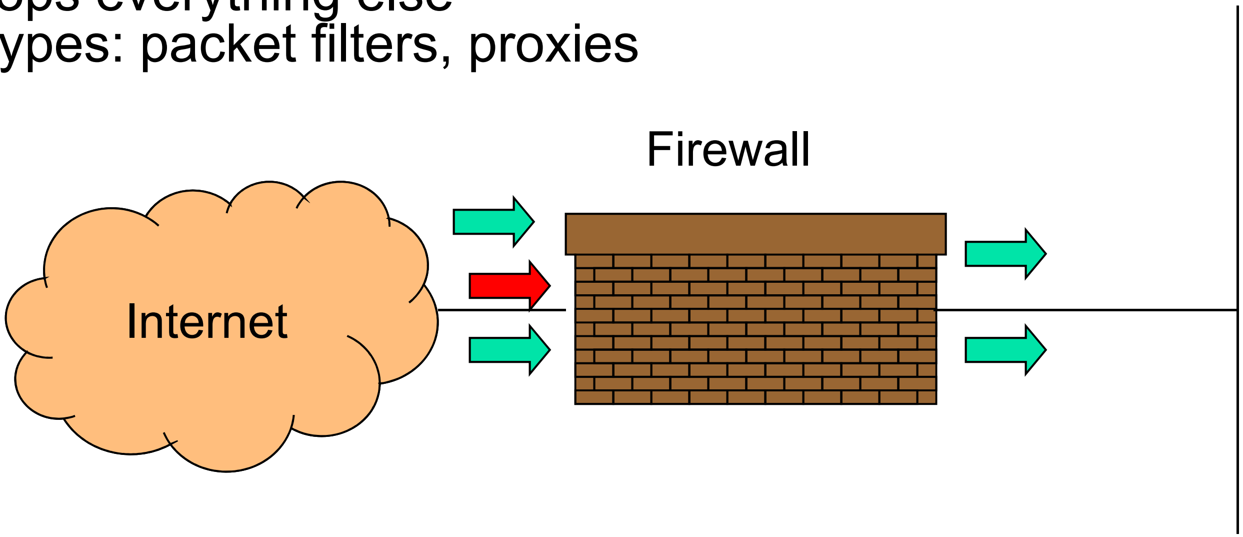
Firewall

- Lots of vulnerabilities on hosts in network
- Users don't keep systems up-to-date
  - Lots of patches
  - Zero-day exploits
- Solution
  - Limit access to the network
  - Put firewalls across the perimeter of the network
- Firewall inspects traffic through it
- Allows traffic specified in the policy
- Drops everything else
- 2 types: packet filters, proxies

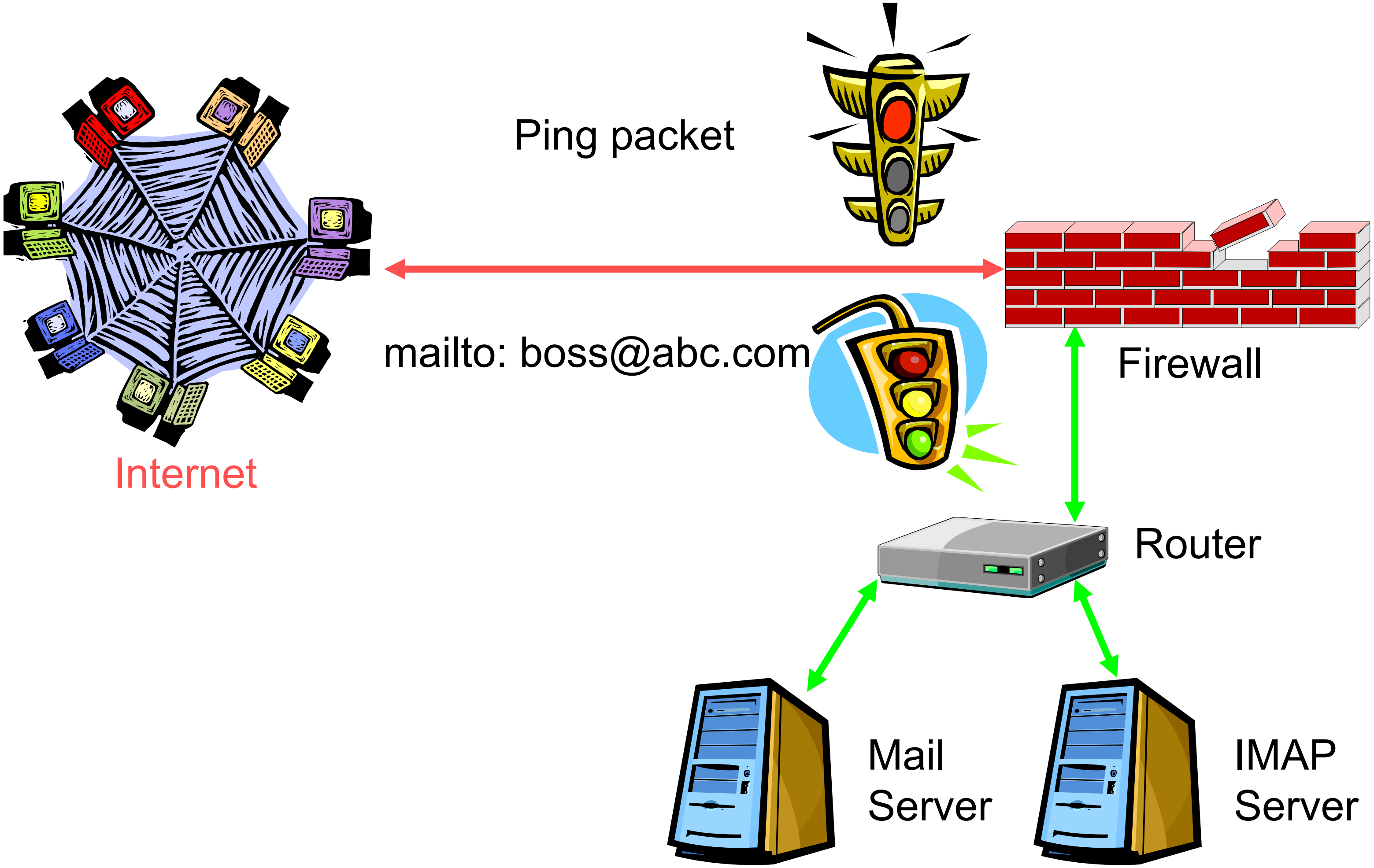
Hardware



Software

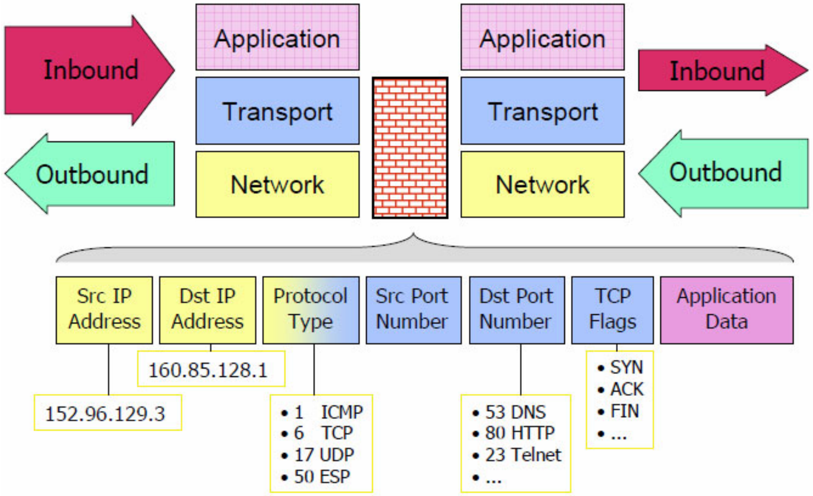


How Firewall work?



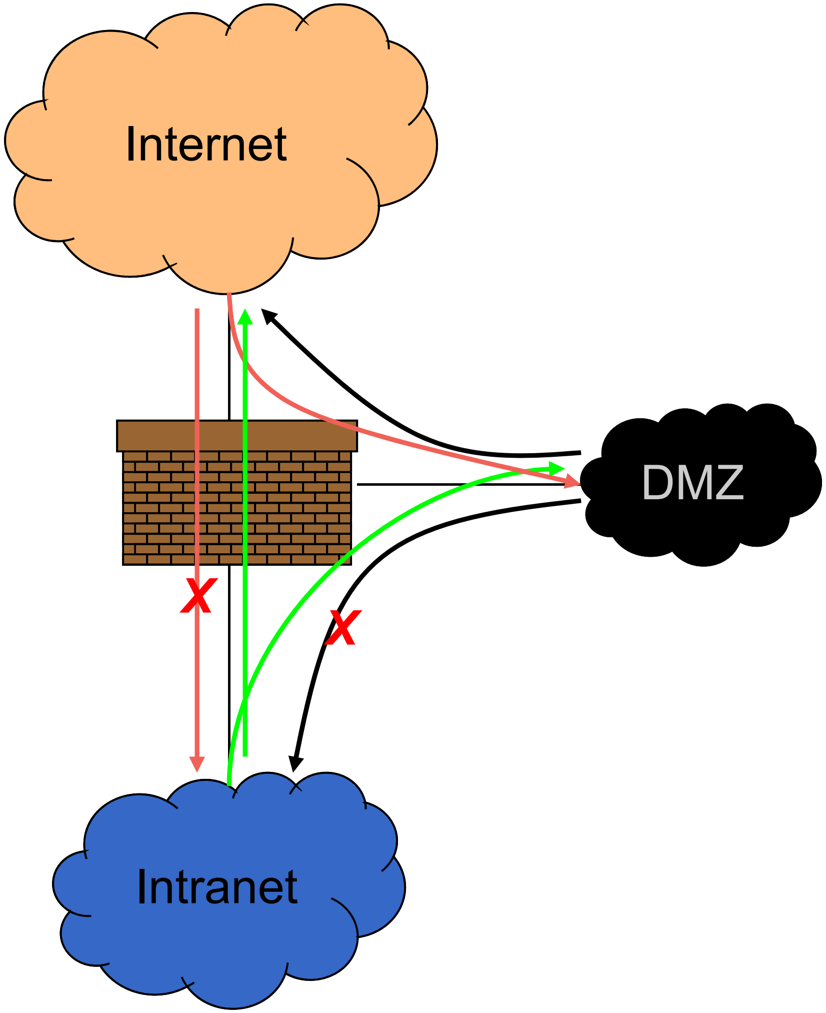
Packet Filtering

- Selectively passes packets from one network interface to another
- Usually done within a router between external and internal network
- What to filter based on?
  - Packet Header Fields
    1. IP source and destination addresses
    2. ICMP message types/protocol options
    3. Application port numbers, etc
  - Packet contents (payloads)
- Other possible actions:
  - Allow the packet to go through
  - Drop the packet (notify sender/drop silently)
  - Alter the packet (NAT)
  - Log information about the packet



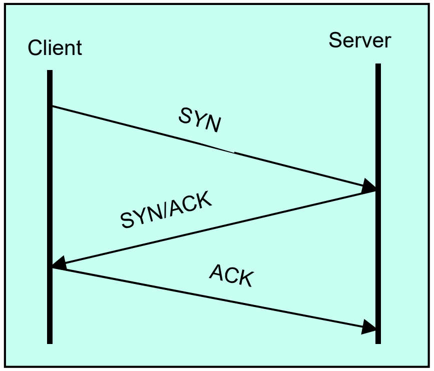
Typical Firewall Configuration

- Demilitarized zone (DMZ) as a perimeter network is a physical or logical subnetwork that contains and exposes an organization's external services to the Internet
- Internal hosts can access DMZ and Internet
- External hosts can access DMZ only, not Intranet
- DMZ hosts can access Internet only
- Advantages:
  - If a service gets compromised in DMZ it cannot affect internal hosts



Firewall Implementation

- Stateless packet filtering firewall
- Rule → (Condition, Action)
- Rules are processed in top-down order
  - If a condition satisfied
    - Action is taken
- Sample firewall rule
  - Allow SSH from external hosts to internal hosts



Two rules

Inbound and outbound

How to know a packet is for SSH?

Inbound: src-port>1023, dst-port=22

Outbound: src-port=22, dst-port>1023

Protocol=TCP

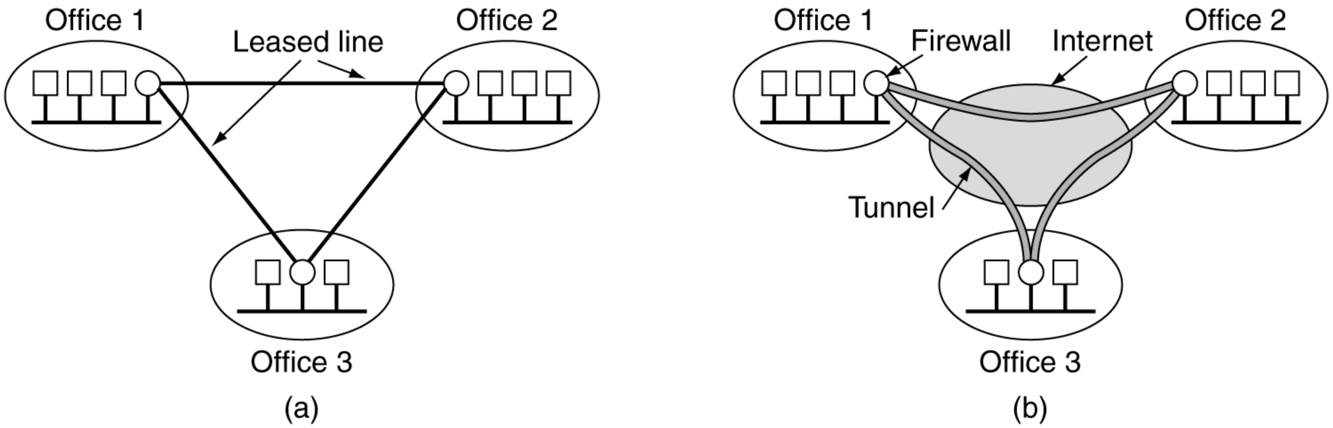
ACK Set?

Problems?

Rule	Dir	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Ack Set?	Action
SSH-1	In	Ext	> 1023	Int	22	TCP	Any	Allow
SSH-2	Out	Int	22	Ext	> 1023	TCP	Yes	Alow

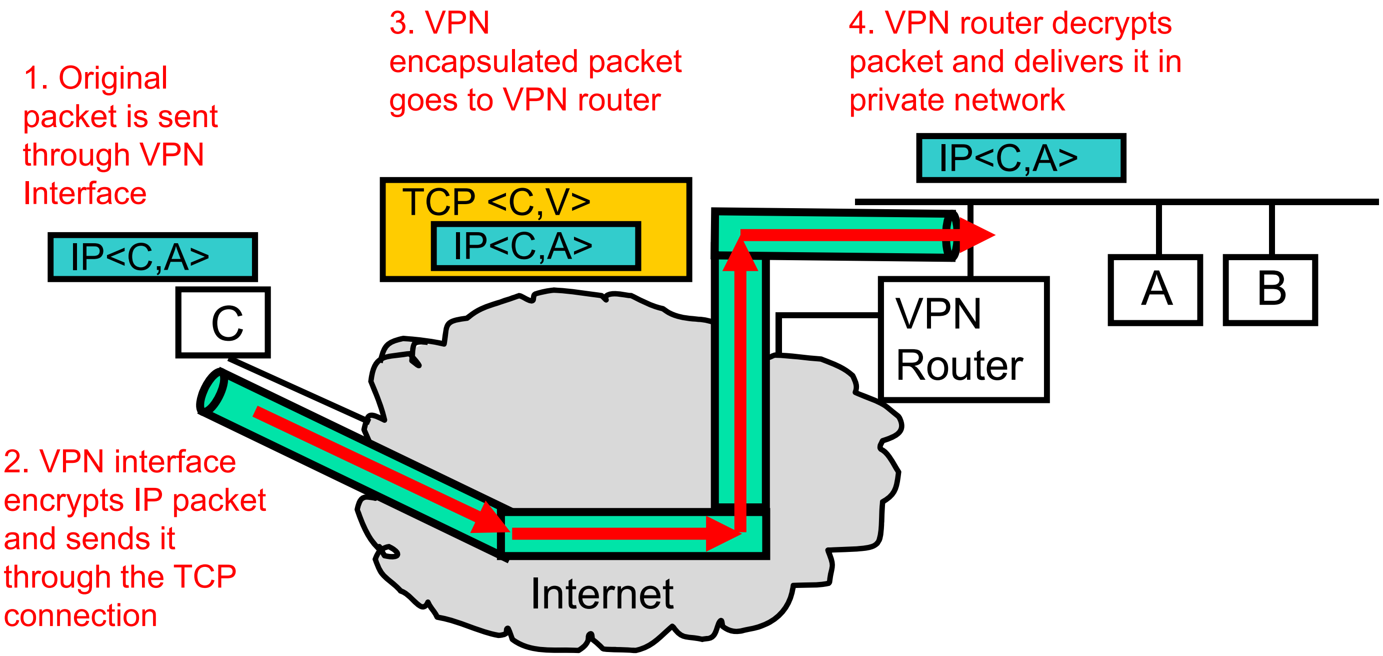
Virtual Private Network

- VPNs are used to connect remote computers to a corporate network using a secure channel
- IP packets are encrypted and then encapsulated in TCP or UDP packets
- Secure channel appears as an extra network interface to the remote machine
- VPN is part of a the corporate network from the viewpoint of remote machine



(a) Leased-line private network. (b) Virtual private network.

VPN (cont.)



1. Original packet is sent through VPN Interface

2. VPN interface encrypts IP packet and sends it through the TCP connection

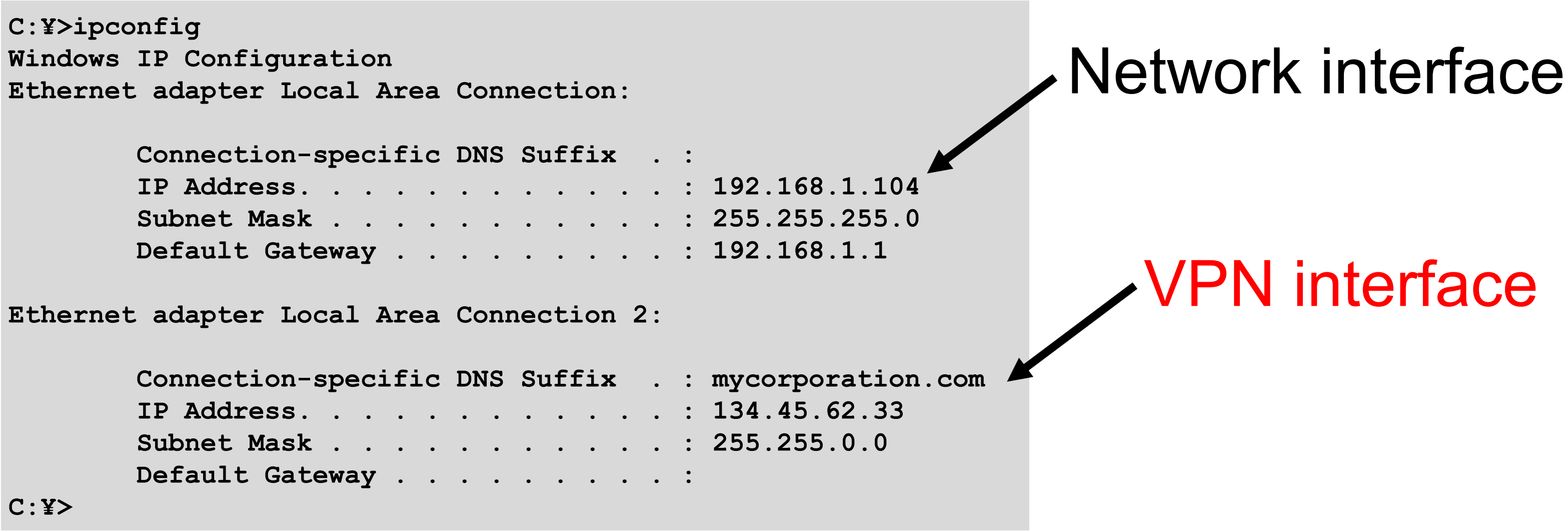
3. VPN encapsulated packet goes to VPN router

4. VPN router decrypts packet and delivers it in private network

Figure: VPN packet encapsulation

VPN (cont.)

- VPN layer in the remote host will forward the packets destined to the private network through the VPN channel
- Other packets are forwarded through the regular network interface
- Windows distributes its own VPN client. You can also get clients from manufacturers like CISCO



```
C:¥>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.104
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : mycorporation.com
        IP Address. . . . . . . . . . . . : 134.45.62.33
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :
C:¥>
```

Transport vs. Tunnel

- Transport
  - Implemented by the end point systems
  - Real address to real address
  - Cannot ‘go through’ other networks
- Tunnel
  - Encapsulation of the original IP packet in another packet
  - Can ‘go through’ other networks
  - End systems need not support this
  - Often PC to a box on the ‘inside’

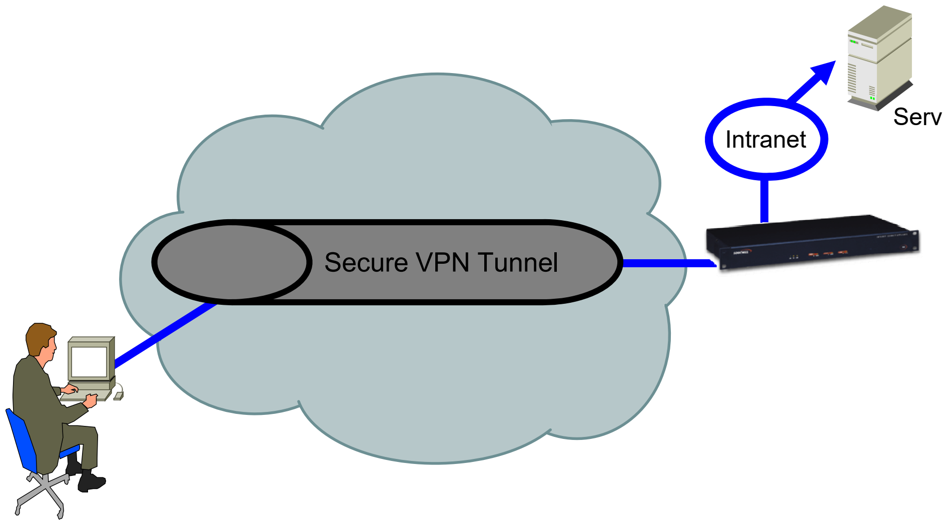
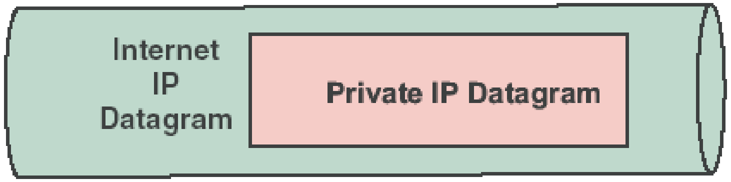


Figure: Tunnel establishes a secure connection between two private networks over a public medium like the Internet



Tunneling

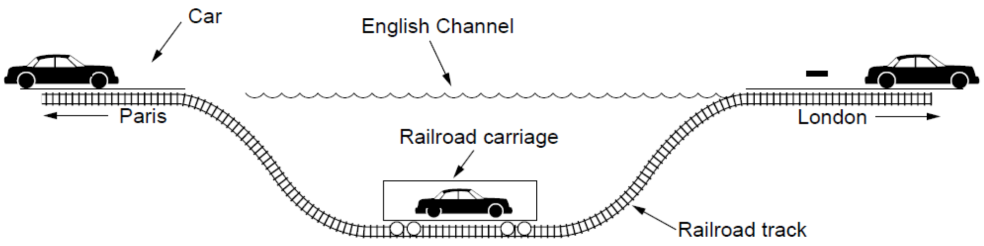


Figure: Tunneling a car from France to England

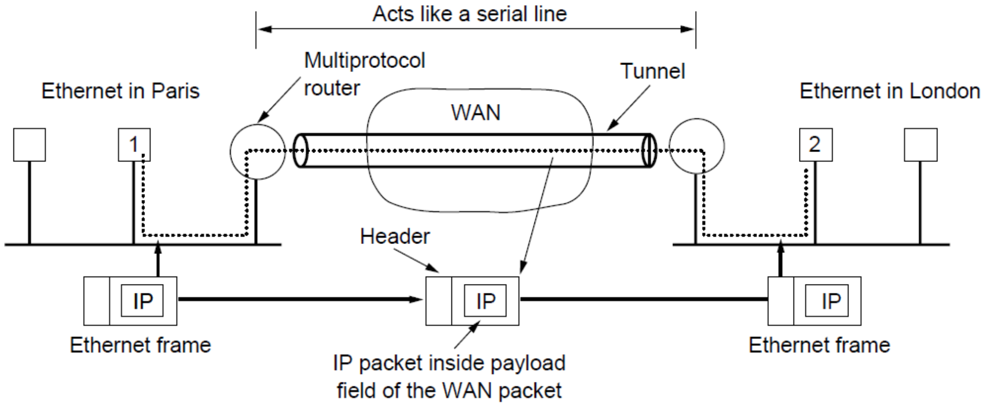


Figure: Tunneling a packet from Paris to London

Tunneling (cont.)

- 2 types of tunneling
  - Site-to-site: typically uses GRE
  - Remote-access: typically uses PPP

- Tunneling requires 3 protocols
  - Carrier – Default network protocol
  - Passenger – Original data
  - Encapsulation – GRE, IPSec, L2F, PPTP, L2TP

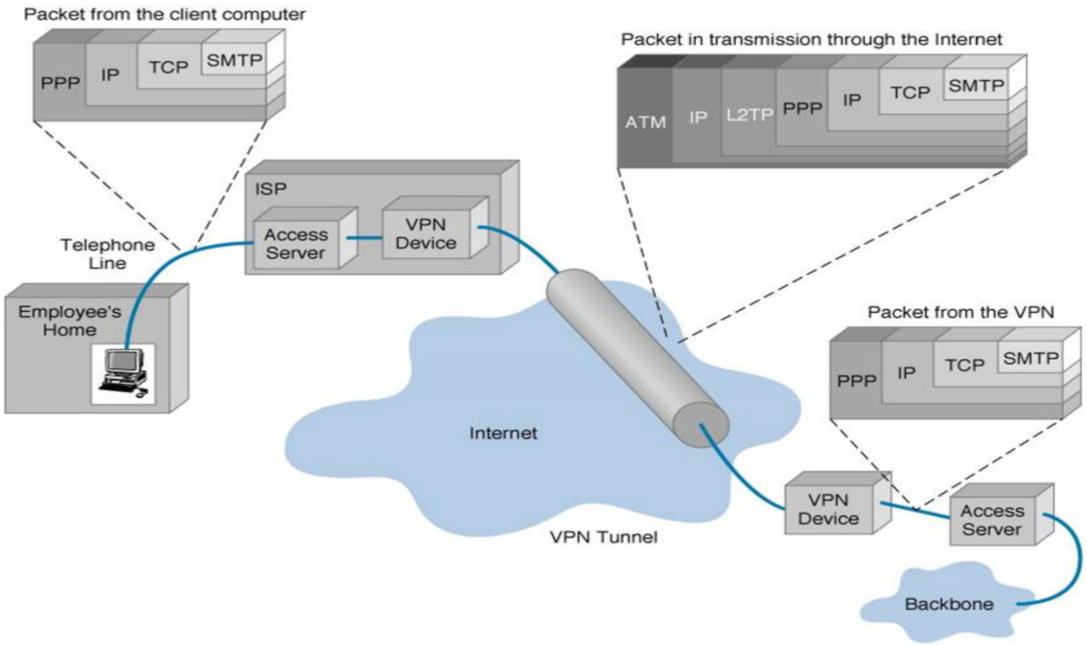


Figure: VPN Encapsulation

Network Address Translation (NAT)

- Router looks like a single device to the outside world (one IP address)
- Router looks like a DHCP server to the inside world (generates IP addresses)
  - Different networks can all share the same address space
- Each device inside the network has a unique subset of port numbers (so the router can address an incoming message correctly)
  - NAT translation table (outer port ⇔ inner host, inner port)
- Private IP addresses:
  - 10.0.0.0 – 10.255.255.255 (16,777,216 hosts)
  - 172.16.0.0 – 172.31.255.255 (1,048,576 hosts)
  - 192.168.0.0 – 192.168.255.255 (65,536 hosts)
- NAT uses source and destination ports of TCP and UDP to sort packets. Thus, NAT mixes up network layer with transport layer!!!

How NAT Works

- Message comes in from WAN
  - Based on port number, re-address it for LAN (internal address and port)
  - Forward out appropriate interface to LAN
  - Host responds
- Message goes out to LAN
  - Replace return address with WAN address and router port
- NAT Translation table contains necessary information to switch between LAN and WAN addresses

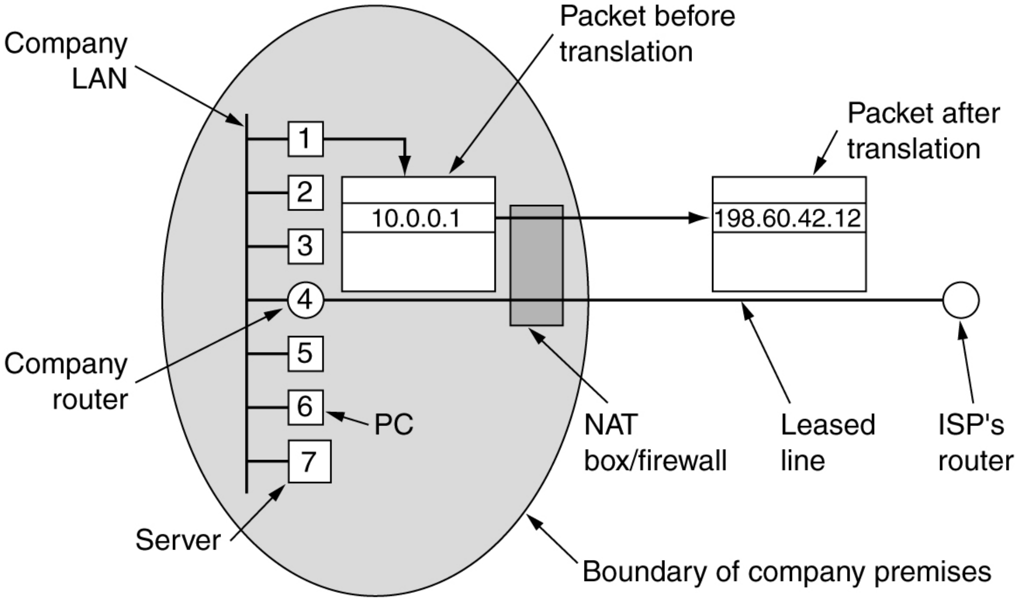
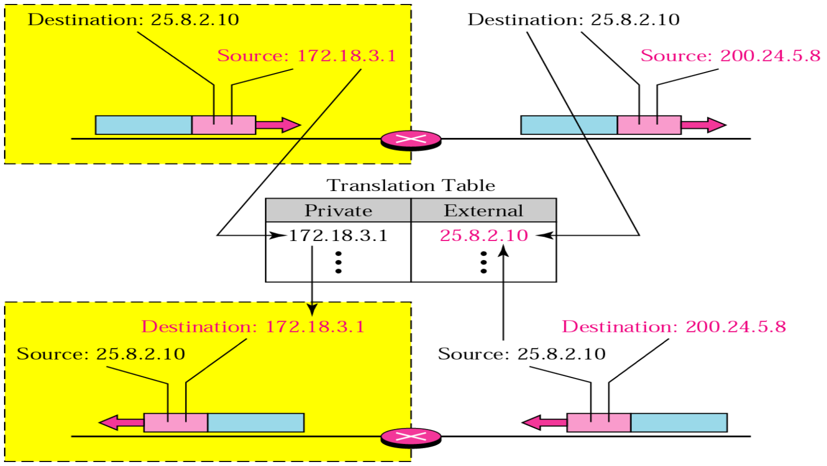


Figure: Placement and operation of a NAT box

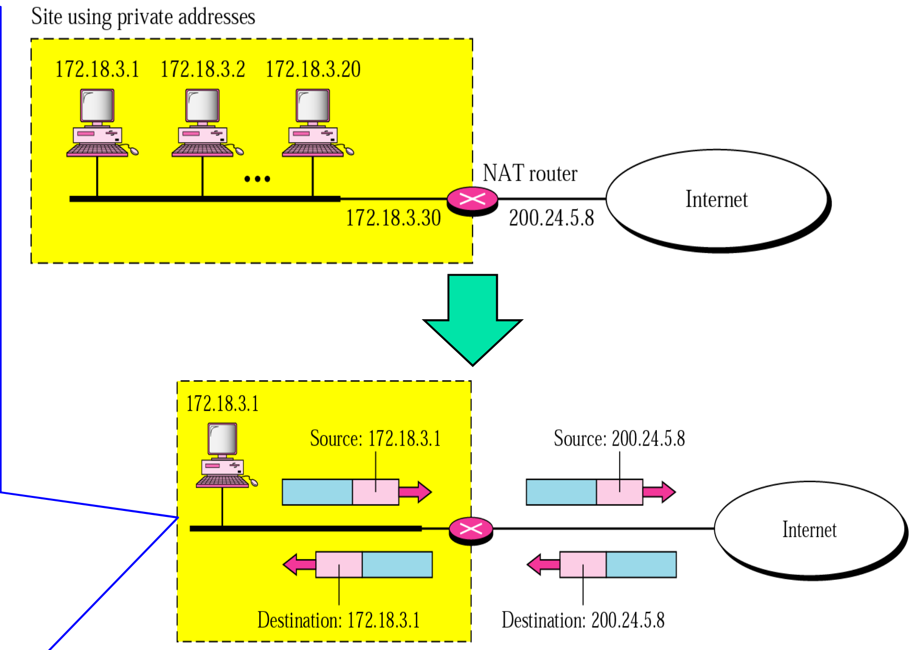
NAT Example

- Private address: 172.18.0.0 to 172.18.255.255
- NAT Router address: 200.24.5.8

Address translation



Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP



Announcement

- Next is Chapter 10 Traffic and Communication Engineering
- 09:00 ~ 10:40 on 14 November (Monday)