SCHOOL OF INNOVATIVE TECHNOLOGIES & ENGINEERING

Module Information Pack

Version 4.1

B.Sc (Hons) Computer Science with Network Security

BCNS/26A/FT

Networks

BCNS1207C

Academic Year 2026 – Semester 2

Programme Director:	Dr. Sandhya Armoogum
Programme Coordinator:	Mr. Ajit Gopee
Module Coordinator:	Mr. Rishi H. Heerasing
Module Convenor:	Mr. Rishi H. Heerasing
Office:	Room G2.14 Level 2 SITE BLOCK
Phone:	234 7624 ext. 34
E-mail:	rheerasing@utm.ac.mu
Academic Tutoring:	None
Lecture Day and Time:	Mondays: 11:00 – 14:00 BPML 2.08
Credits & Level:	6 credits, Level 1
Pre-requisites (If applicable):	None
Co-requisites (If applicable):	None
Method of Delivery & Frequency:	12 weeks; 1 x 3 Hrs sessions of lectures and tutorials.
Method & Criteria of Assessment:	70% Unseen Exam & 30% Coursework

Module Aims:

- To investigate the fundamentals of data communication and the problems that affects communication in relation to computer networks.
- To illustrate the concepts and applications of communications technologies and networks in the context of the OSI and TCP/IP reference models.
- To introduce the need for network security services such as confidentiality and authentication.
- To investigate the various communications standards, protocols, architectures, and transmission techniques currently available.
- To introduce the basic terminology, hardware and software technologies and standards in computer networks.
- To illustrate the concepts and provide practical insight by examining specific networking protocols and topologies.

Learning Objectives and Outcomes:

- Understand the technical literature, fundamental concepts & issues involved in data communications and computer networks.
- Understand the requirements for effective and reliable data transmission.
- Understand the layered structure of computer networks and distinguish the different protocols and type of services provided at each layer.
- Understand the techniques and algorithms that have been devised to effect proper communication across networks.
- Understand the different network security services and mechanisms used to enforce these services.
- Understand the concepts behind traditional and emerging data-link access standards.
- Understand the types and functions of network interconnect devices.

TENTATIVE LECTURE SCHEDULE

(F2F on ODD weeks and ONLINE on EVEN weeks)

Week	Dates	Topics Covered
1	12/10/26	Introduction to networks.
2	19/10/26	ISO-OSI Model; TCP/IP Suite. Application Layer protocols such as: HTTP, FTP, SMTP, POP/IMAP, DNS.
3	26/10/26	Transport Layer: Services and Protocols; TCP vs. UDP; Segment Structure, Reliable Data Transfer, Flow Control, Connection
4	02/11/26	Network Layer: Services and Path selection; IPv4; ICMP
5	09/11/26	Network Layer (Cont.): Fragmentation; Routing protocols; IPv6; Mobility.
6	16/11/26	Network Layer (Cont.): IP addressing and Calculation
7	23/11/26	Data Link Layer: Services; Multiple Access protocols; LAN addressing; ARP and RARP. Ethernet, Intermediate Systems.
8	30/11/26	Wireless Technologies
9	07/12/26	Network Security Services.
10	14/12/26	Network Design
New Year Break		
11	**11/01/27***	***Open-Book Class Test (30% of module weight)***
12	18/11/27*	Class Test Post Mortem + Revision

Week 4 and 5 are public holidays, classes shall be replaced, if needed. after Week 12.
* Week 11 and 12 dates are tentative yet.

READING LIST

RECOMMENDED TEXTS (as per availability in the UTM Resource Centre)**:**

- **Kurose & Ross (2002) *Computer Networking: A Top-Down Approach featuring the Internet:* 2nd Ed., Addison-Wesley (D4.6KUR)** ж
- **Tanenbaum A. (2001) *Computer Networks:* 4th Ed., Prentice-Hall (D4.6TAN)** ж
- Stallings W. (2001) *Data and Computer Communications:* 6th Ed., Prentice-Hall (D4.6STA)
- Hallsall F. (2001) *Data Communications, Computer Networks, and Open Systems:* 4th Ed., Addison-Wesley (D4.6HAL)
- Lowe D. (2005) *Networking for Dummies:* 7th Ed., Wiley Publishing ж

ж *You can download a copy of these e-books at https://www.rishiheerasing.net/download/network.html*

OTHER READING MATERIALS (Texts / Journals / Articles / Websites)**:**

- Pearson Companion Website for *Computer Networking: A Top-Down Approach, 8th Edition* at https://gaia.cs.umass.edu/kurose_ross/index.php
- Student Website for *Data and Computer Communications, 10th Edition* at http://williamstallings.com/DataComm/DCC10e-Student/

LECTURE NOTES

Available at **Nefertum's Shrine** at https://www.rishiheerasing.net/modules/bcns1207/ln.html

The notes are in .pdf format so you will need Adobe Acrobat® Reader to view them. This reader can also be downloaded from the two above-mentioned sites in the Downloads Section.

1

Introduction to Networks

BCNS1207C

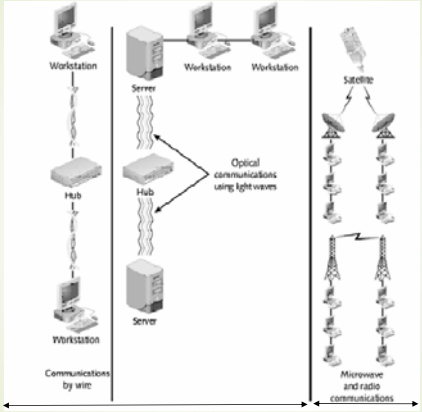
2

Network: Definition

- A set of devices (**nodes**) connected by **communication links** (wired or wireless).
- A **node** can be a computer, or any device capable of sending and/or receiving data generated by other nodes on the network.
- A network must be able to meet a certain number of criteria. The most important of those are: **Performance**, **Reliability, Security** and **Cost**.

3

Types of Communication Links



UTP, STP, Coaxial, USB cables — **Guided (wired)** — **Unguided (wireless / radiated)**

4

Physical Topology

- The **physical topology** refers to the way a network is laid out spatially.
- **Two** or more **nodes** connect to a **link.**
- **Two** or more **links** form a **topology**.
- The **topology** is the geometric representation of the relationship of all the links and nodes to one another.
- There are usually **four** basic topologies: **Mesh**, **Star, Bus** and **Ring**.

5

Mesh Topology

- In a **mesh topology**, every node has a **dedicated point-to-point** link to every other node.

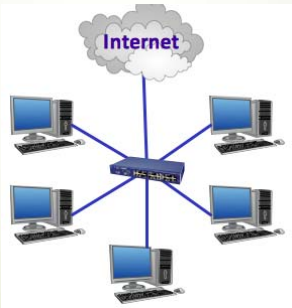
Full-Mesh:

Partial-Mesh:

6

Star Topology

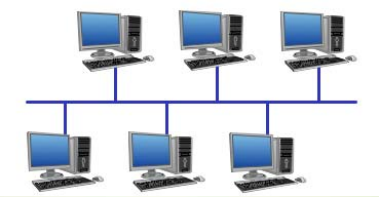
- In a **star topology**, each node has a **dedicated point-to-point** link only to a central controller, usually a **switch**.



7

Bus Topology

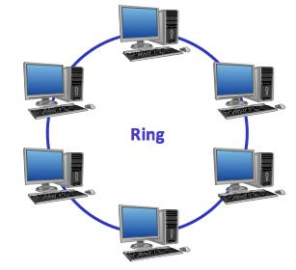
- In a **bus topology**, a **multipoint** link is used. One long cable acts as a **backbone** to link all the devices in a network.



8

Ring Topology

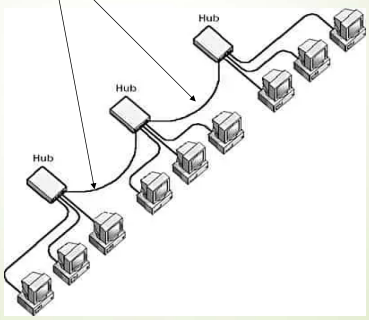
- In a **ring topology**, each node has a **dedicated point-to-point** link only with the **two** nodes on either side of it.



9

Hybrid: Star Bus Topology

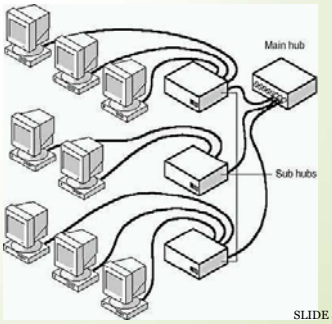
- In a **star bus topology**, **several star topology networks** are linked together with **linear bus trunks**.



10

Hybrid: Star Ring Topology

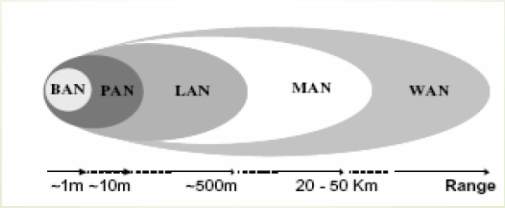
- In a **star ring topology**, **sub hubs** are linked together in a **star pattern** to a **main hub**, rather than to themselves with **linear bus trunks**.



11

Network Types Defined

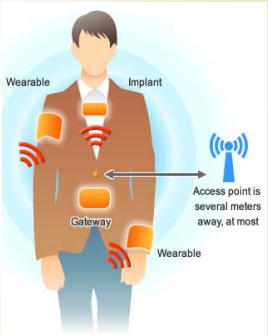
- Body Area Network
- Personal Area Network
- Local Area Network
- Metropolitan Area Networks
- Wide Area Networks



12

Body Area Network (BAN)

- Short range wireless network which consists of wearable or implanted electronic devices that transmit ID or sensor data to gateway device.
- It is also referred to as Wireless Body Area Network (WBAN) or Body Sensor Network (BSN) and spans less than 1 metre.



13

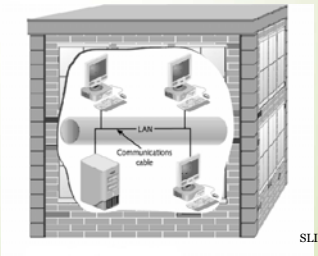
Personal Area Network (PAN)

- A Personal Area Network (PAN) is a computer network used for communication amongst computing devices (Smartphones, PDAs, Tablets) close to one person. The reach of a PAN is typically a few meters (<10 m).
- Personal area networks may be wired by computer buses such as USB and FireWire. However, Wireless Personal Area Network (WPAN) is made possible with network technologies such as IrDA, Bluetooth and Zigbee.

14

Local Area Network (LAN)

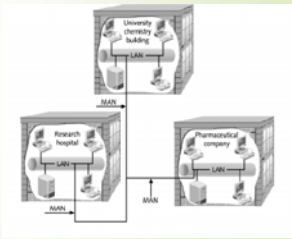
- Series of interconnected computers, printing devices, and other computer equipment that share hardware and software resources
- Service area usually limited to a given office area, floor, or building and is usually privately-owned.



15

Metropolitan Area Network

- Links **multiple LANs** in a large city or metropolitan region.
- May be wholly owned & operated by a private or public company such as a local telephone company.
- Many **telcos** provide services like **Switched Multi-Megabit Data Services** (SMDS).



16

Wide Area Network (WAN)

- Provides long-distance transmission of data, voice, image and video information over large geographic areas that may comprise a country, a continent, even the whole world.
- The best example of a WAN is the **Internet**.

17

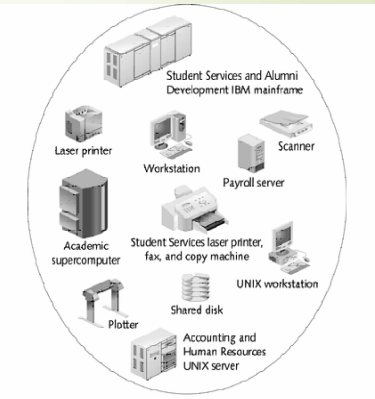
Identifying a Network Type

- Communications medium
  - Wire cable, fiber-optic cable, radio waves, microwaves, infrared radiation.
- Protocol
  - How networked data is formatted into discrete units
  - How each unit is transmitted and interpreted
- Topology
  - Physical layout of cable and logical path
- Network type
  - Private versus public

18

Network Classification

- **Enterprise** network
  - Combination of **LANs**, **MANs**, or **WANs** that provides users with an array of computer and network resources to complete different tasks.



Resources in an enterprise network

19

Events that Led up to LANs and WANs

- **1800s**
  - Oersted
  - Morse
  - Undersea cable
  - Pony Express
  - Bell
- **1900s**
  - Transcontinental and transatlantic calls
  - Voice digitization
  - Electronic digital computers
  - Transistors
  - Sputnik
  - Communications satellites
  - ASCII
  - Mass-produced minicomputers

20

LAN/WAN History: 1960s

- First WAN
- Hypertext
- Use of fiber optics for phone signals
- Beginning of ARPANET
- Packets and packet switching
- UNIX
- Telecommunications equipment
- First IMP prototype

21

LAN/WAN History: 1970s

- Ethernet
- ARPANET - 15 sites
- E-mail
- Terminal emulation
- International connections to ARPANET
- Telecommunications conversion from analogue to digital
- X.25
- First wireless gateway
- Internet Protocol
- LSI and VLSI chips
- ICCB later IAB

22

LAN/WAN History: 1980s

- BITNET
- IBM's PC
- Dial-up modem technology
- TCP and IP adopted as protocol suite for ARPANET
- First PC LAN
- Arrival of Internet
- Internetwork hosts
  - 5,000 in 1986
  - 100,000 in 1989
- "Cyberspace"
- T-carrier services
- NFSNET
- Desktop authoring and multimedia
- SNMP

23

LAN/WAN History: 1990s

- ARPANET retired
- SS7 technology
- NSFNET opened to commercial use
- First cyberbank
- Internet service providers
- Over 16 million Internet hosts

24

LAN/WAN History: 2000s

- IPv6 used for Internet2 backbone communications
- Video and radio capability
- Prices of 1-Gbps devices fall as competition increases

25

LAN/WAN History: 2010s

- Cloud Services commonplace
- Internet of Things (IoT)
- 10G, 25G, 40G and 100G Ethernet has been developed

26

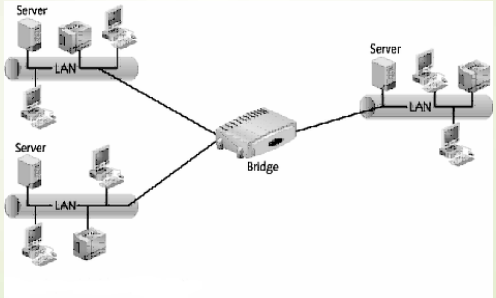
LAN/WAN Integration

- Becoming more advanced through networking devices like
  - Modems
  - Bridges
  - Routers
  - Gateways
  - Switches
  - Firewalls
  - Access Points

27

Bridges (almost obsolete replaced by switches)

- Connect different LANs or LAN segments using the **same access** method



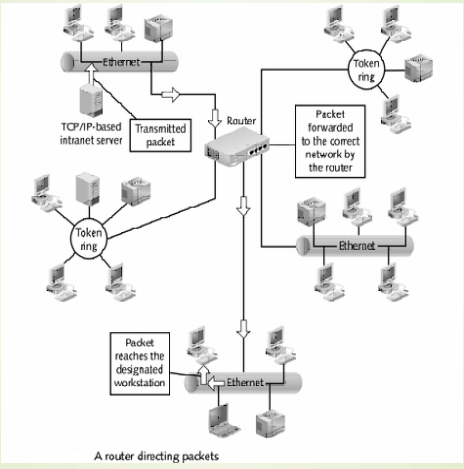
28

Routers

- Connect networks having the same or different access methods and media
- Route packets or datagrams to networks by using a decision-making process based on:
  - Routing table data
  - Discovery of most efficient routes
  - Pre-programmed information from network administrator

29

Routers

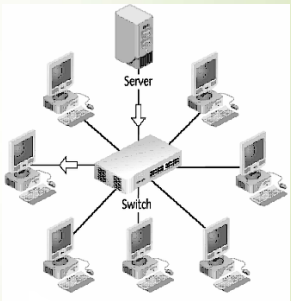


A router directing packets

30

Link-Layer or Layer 2 Switches

- Link network segments
- Forward and filter frames between segments
- Different types depending on speed, number of ports, manageability, mode of switching, etc.



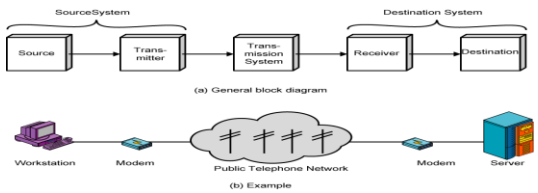
A switch in operation

Data Communications *vs* Networking

- Data Communication (DC) is concerned with the transmission of data over a communication medium/channel between two entities. Here we are more concerned about engineering issues e.g. properties of communication medium, physical characteristics of signals & interfaces, format, timing, etc.…

- Networking (Net) is concerned with the physical topology of two or more communicating entities and the logical topology of data transmission. Issues such as addressing, routing, reliability, etc become important.

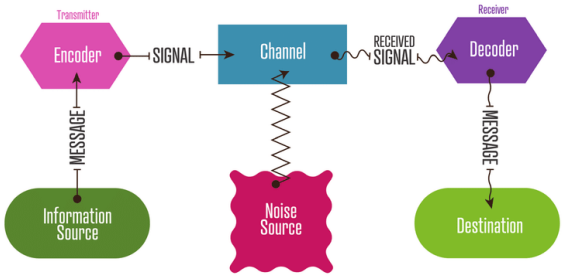
Simplified Communication Model



Major Communication tasks

- Transmission system utilization (DC+Net)
- Addressing (DC+Net)
- Interfacing (DC)
- Routing (Net)
- Signal generation (DC)
- Recovery (DC+Net)
- Synchronization (DC+Net)
- Message formatting (Net)
- Security (Net)
- Error detection and correction (DC+Net)
- Congestion control (Net)
- Flow control (DC+Net)

Simplified Communications Model by Shannon-Weaver



Layered Model

- Systems communicate over a shared communication medium according to an agreed upon convention (standard or protocol).
- Several sets of standards currently exist:
  - DoD: TCP/IP
  - ISO: OSI model
  - Commercial: SNA, IPX (Novell)
  - Proprietary
- In this module, we will basically follow the 7 layer approach defined by ISO: OSI.

DoD Model

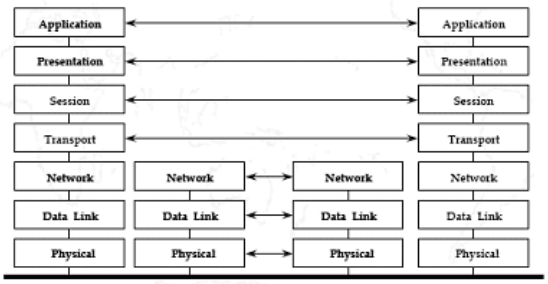
- DARPA (Defence Advanced Research Projects Agency)
- ARPANET => Internet
- TCP/IP Transmission Control Protocol/Internet Protocol consists of 4 layers
- TCP/IP developed concurrently with ISO model. TCP/IP does not contain protocols relating to all 7 ISO layers. Most of the functionalities of ISO are embedded in TCP/IP.

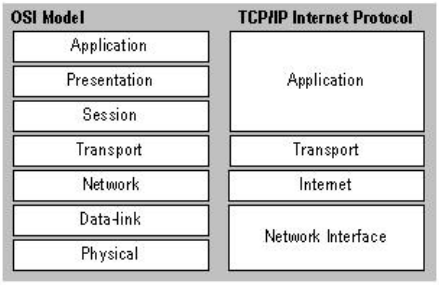
ISO/OSI Model

- Communication functions are partitioned into a vertical set of seven layers.
- each layer performs a related subset of functions required for communication.
- each layer provides services to next higher layer while depending on the previous lower layer to do more primitive functions.
- decomposes one problem into a number of more manageable sub-problems.
- communication is achieved by having corresponding (peer) entities in the same layer in two different systems communicate via a protocol.
- each protocol entity sends data down to the next lower layer so as to get data across to its peer entity.
- each entity communicates with entities in the layers above it and below it, across an interface.

ISO/OSI provides a common basis for coordination of standards and is based on a hierarchical model:

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer





TCP/IP vs. ISO-OSI

Application Layer

Goals:

- ❒ conceptual, implementation aspects of network application protocols
  - ❍ transport-layer service models
  - ❍ client-server paradigm
  - ❍ peer-to-peer paradigm
- ❒ learn about protocols by examining popular application-level protocols
  - ❍ HTTP
  - ❍ FTP
  - ❍ SMTP / POP3 / IMAP4
  - ❍ DNS

Application: communicating, distributed processes
- ❍ e.g. Email, Web, P2P file sharing, Instant Messaging
- ❍ running in end systems (hosts)
- ❍ exchange messages to implement application

Application-layer protocols:
- one "piece" of an application
- define messages exchanged by apps and actions taken
- use communication services provided by lower transport layer protocols (TCP, UDP)

Application-layer protocols define:

- ❒ Types of messages exchanged, e.g. request or response messages
- ❒ Syntax of message types: what fields in messages & how fields are delineated
- ❒ Semantics of the fields, i.e. meaning of information in fields
- ❒ Rules for when and how processes send & respond to messages

Public-domain protocols:
- ❍ defined in RFCs
- ❍ allows for interoperability
  eg, HTTP, SMTP

Proprietary protocols:
eg, Skype, Zoom, Messenger, etc…

Client-Server Paradigm

Client:
- ❒ initiates contact with server ("speaks first")
- ❒ typically requests service from server,
- ❒ Web client implemented in browser; email client implemented in mail reader

Server:
- ❒ provides requested service to client e.g., webserver sends requested webpage, mail server delivers email

Which type of service does an application need?

Data Loss and Timing
- ❒ some apps (e.g., audio) can tolerate some loss
- ❒ other apps (e.g., file transfer, telnet) require 100% reliable data transfer
- ❒ some apps (e.g., Internet telephony, interactive games) require low delay to be "effective"

Bandwidth
- ❒ some apps (e.g., multimedia) require minimum amount of bandwidth to be "effective"
- ❒ other apps ("elastic apps") make use of whatever bandwidth they get

application	data loss	throughput	time sensitive?
file transfer	no loss	elastic	no
e-mail	no loss	elastic	no
Web documents	no loss	elastic	no
real-time audio/video	loss-tolerant	audio: 5Kbps-1Mbps video:10Kbps-5Mbps	yes, 10's msec
streaming audio/video	loss-tolerant	same as above	yes, few secs
interactive games	loss-tolerant	Kbps+	yes, 10's msec
text messaging	no loss	elastic	yes and no

Transport protocol Services

TCP service:

- *connection-oriented:* setup required between client and server processes
- *reliable transport* between sending and receiving process
- *flow control:* sender won't overwhelm receiver
- *congestion control:* throttle sender when network overloaded
- *does not provide* timing or minimum bandwidth guarantees

UDP service:

- unreliable data transfer between sending and receiving process
- does not provide: connection setup, reliability, flow control, congestion control, timing, or bandwidth guarantee

Q: why bother? Why is there a UDP?

application	application layer protocol	transport protocol
file transfer/download	FTP [RFC 959]	TCP
e-mail	SMTP [RFC 5321]	TCP
Web documents	HTTP [RFC 7230, 9110]	TCP
Internet telephony	SIP [RFC 3261], RTP [RFC 3550], or proprietary HTTP	TCP or UDP
streaming audio/video	[RFC 7230], DASH	TCP
interactive games	WOW, FPS (proprietary)	UDP or TCP

HTTP: HyperText Transfer Protocol

- Web page consists of objects
- Object can be HTML file, JPEG image, Java applet, etc
- Web page consists of base HTML-file which includes several referenced objects
- Each object is addressable by a URL
- Example URL:
  https://www.rishiheerasing.net/bcns1207/syl.html
  <------ hostname --------> <------ path -------->

HTTP overview

HTTP: HyperText Transfer Protocol
- Web's application layer protocol
- client/server model
  - *client:* browser that requests, receives, "displays" web objects
  - *server:* sends objects in response to requests
- HTTP 1.0: RFC 1945 (est. 1996)
- HTTP 1.1: RFC 2068 (est. 1997)
- HTTP /2: RFC 7540 (est. 2015)
- HTTP /3: RFC 9114 (est. 2022)

HTTP Uses TCP:

- client initiates TCP connection (creates socket) to server, *port 80*
- server accepts TCP connection from client
- HTTP messages (application-layer protocol messages) exchanged between browser (HTTP client) and Web server (HTTP server)
- TCP connection closed

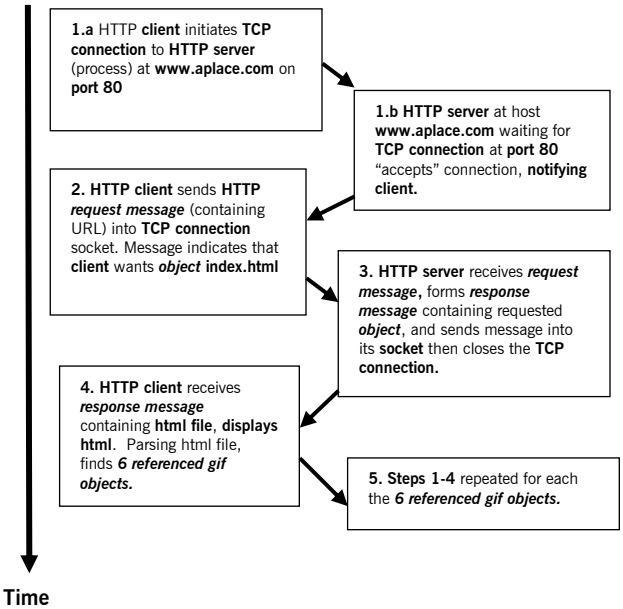
HTTP is "stateless" i.e. server maintains no information about past client requests

HTTP Connections

1. Non-persistent HTTP: (obsolete nowadays)
   - Only one object is sent over a single TCP connection.
   - HTTP/1.0 uses non-persistent HTTP.

Suppose a user enters the following URL: **http://www.aplace.com/index.htm**l and that this homepage contains some text and references to 6 gif images in total.

The following interactions will take place:



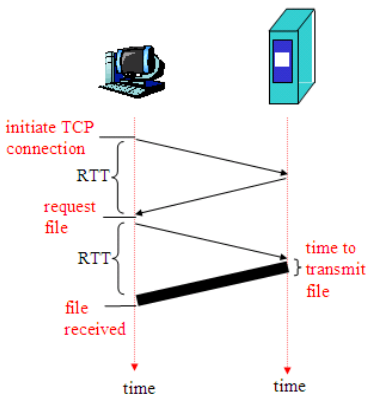
Response Time Modelling

Definition of Round-Trip Time (RTT) is the time to send a small packet to travel from client to server and back.

Response time:

- one RTT to initiate TCP connection
- one RTT for HTTP request and first few bytes of HTTP response to return
- file transmission time

Total = 2 x RTT+ transmit time



Non-persistent HTTP issues:

- requires 2 RTTs per object.
- OS must work and allocate host resources for each TCP connection.
- but browsers often open parallel TCP connections to fetch referenced objects.

2. Persistent HTTP: (HTTP/1.1 is still popular)
   - Multiple objects can be sent over a single TCP connection between client and server.
   - HTTP/1.1 uses persistent connections by default.

Persistent HTTP issues
- Server leaves connection open after sending response.
- Subsequent HTTP messages between same client/server are sent over same connection.

Persistent HTTP without pipelining
- client issues a new request only when previous response has been received.
- one RTT for each referenced object.

Persistent HTTP with pipelining
- default in HTTP/1.1
- client sends requests as soon as it encounters a referenced object.
- as little as one RTT for all the referenced objects.

HTTP/2

Key goal: decreased delay in multi-object HTTP requests

HTTP1.1: introduced multiple, pipelined GETs over single TCP connection
- server responds *in-order* (FCFS: first-come-first-served scheduling) to GET requests
- with FCFS, small object may have to wait for transmission (head-of-line (HOL) blocking) behind large object(s)
- loss recovery (retransmitting lost TCP segments) stalls object transmission

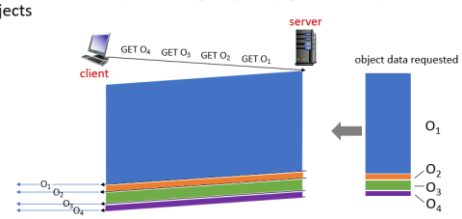
HTTP/2

Key goal: decreased delay in multi-object HTTP requests

HTTP/2: [RFC 7540, 2015] increased flexibility at *server* in sending objects to client:
- methods, status codes, most header fields unchanged from HTTP 1.1
- transmission order of requested objects based on client-specified object priority (not necessarily FCFS)
- *push* unrequested objects to client
- divide objects into frames, schedule frames to mitigate HOL blocking

HTTP/2: mitigating HOL blocking

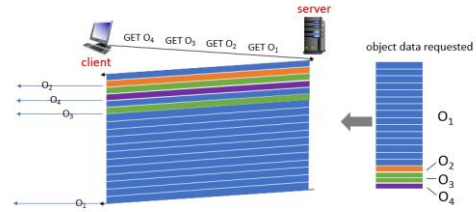
HTTP 1.1: client requests 1 large object (e.g., video file) and 3 smaller objects



objects delivered in order requested: O_2, O_3, O_4 wait behind O_1

HTTP/2: mitigating HOL blocking

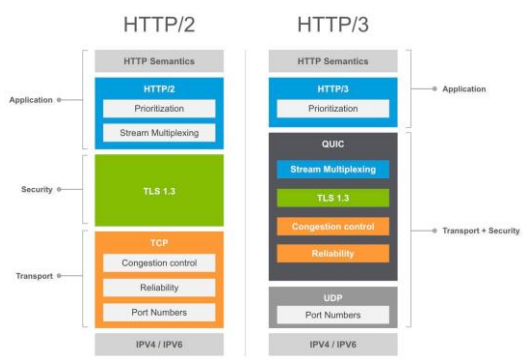
HTTP/2: objects divided into frames, frame transmission interleaved



O_2, O_3, O_4 delivered quickly, O_1 slightly delayed

HTTP/3

Since 2021, Google have standardised HTTP/3, which centres around a new protocol called QUIC (Quick UDP for Internet Connection)



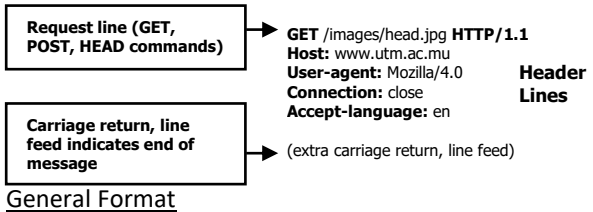
HTTP messages

- There are 2 types of HTTP messages: Request and Response.

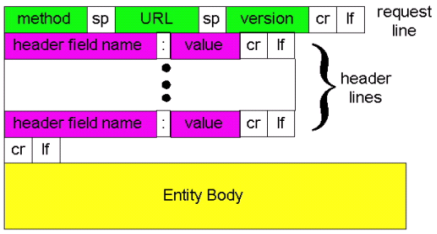
HTTP Request message

- ASCII (Human readable format)

e.g.



General Format



Uploading Form Input

POST method:

- Web page often includes form input.
- Input is uploaded to server in entity body.

GET method:

- Uses URL method
- Input is uploaded in URL field of request line: e.g. www.xxx.com/indexsearch?engineering

Method Types

HTTP/1.0:

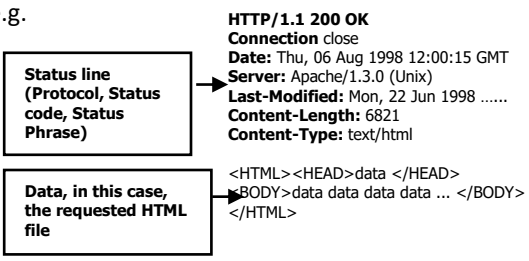
- GET, POST
- HEAD: asks server to leave requested object out of response.

HTTP/1.1:

- GET, POST, HEAD
- PUT: uploads file in entity body to path specified in URL field.
- DELETE: deletes file specified in URL field.

HTTP Response message

e.g.



HTTP Response Status Code

- Found on the first line of the client-server response message.

Some sample webserver status codes:

200 OK: request succeeded, requested object later in this message
301 Moved Permanently: requested object moved, new location later in same message
400 Bad Request: request message not understood by server
404 Not Found: requested document not found on this server
505 HTTP Version not supported: self-explanatory.

Cookies: Keeping "State"

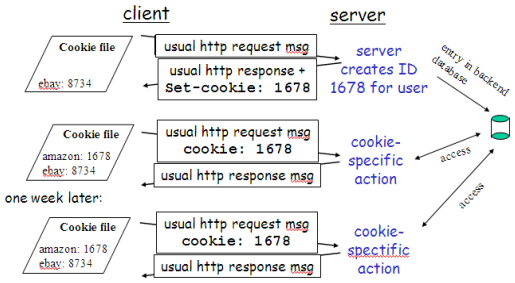
Many major websites use cookies nowadays.

Four components:

1) cookie header line in the HTTP response message
2) cookie header line in HTTP request message
3) cookie file kept on user's host and managed by user's browser
4) Database at Web site

e.g.

Susan always accesses the Internet from the same PC.
She visits an Ecommerce site for first time e.g. Amazon.
When initial HTTP request arrives at site, site generates a unique ID and creates an entry in database for ID.



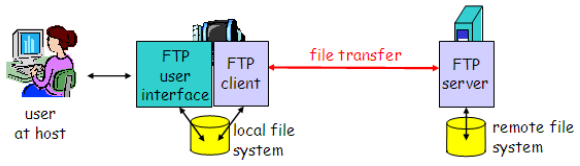
When and where cookies can be used:

authorization, shopping carts, recommendations
user session state (Web e-mail e.g. Hotmail)

Cookies and Privacy:

cookies permit sites to learn a lot about you
you may supply name and e-mail to sites
search engines use redirection & cookies to learn yet more
advertising companies obtain info across sites

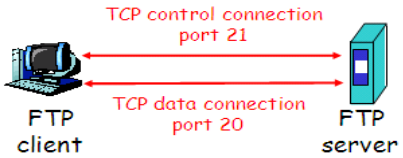
FTP: File Transfer Protocol



- transfer file to/from remote host
- client/server model
  client: side that initiates transfer (either to/from remote)
  server: remote host
- ftp: RFC 959
- ftp server: port 21

Separate Control and Data Connections

- FTP client contacts FTP server at port 21, specifying TCP as transport protocol.
- Client obtains authorization over control connection.
- Client browses remote directory by sending commands over control connection.
- When *server* receives a command for a file transfer, the server opens a *TCP data connection* to client.
- *After transferring one file, server closes connection*.
- *Server* opens a second *TCP data connection* to transfer another file.
- Control connection: "*out of band*"
- *FTP* server maintains *"state"*: current directory, earlier authentication.



Sample commands: sent as ASCII text over control channel

- USER username, PASS password, LIST return list of file in current directory
- RETR filename retrieves (gets) file, STOR filename stores (puts) file onto remote host.

Sample status codes and phrase: (as in HTTP)

- 331 Username OK, password required, 125 data connection already open; transfer starting, 425 Cannot open data connection, 452 Error writing file.

Electronic Mail

Three major components:

- user agents
- mail servers
- simple mail transfer protocol: SMTP

User Agent

- a.k.a. "email reader"
- composing, editing, reading and sending email messages
  e.g. Microsoft Outlook, Mozilla Thunderbird, Mailbird
- outgoing, incoming messages stored on server.

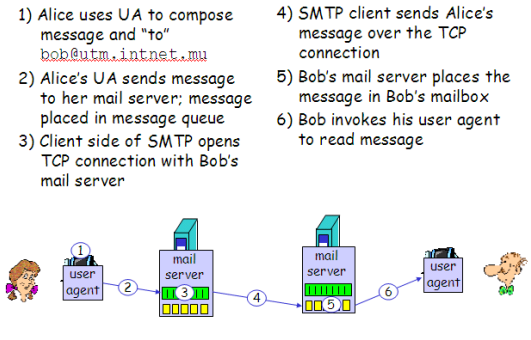
Mail Servers

- mailbox contains incoming messages for user
- message queue of outgoing mail messages
- SMTP protocol between mail servers to send email messages
  - client: sending mail server
  - server: receiving mail server

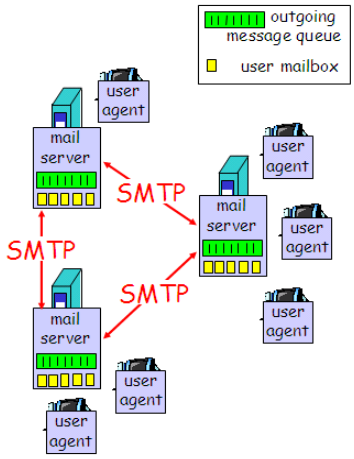
SMTP [RFC 2821]

- uses TCP to reliably transfer email message from client to server, port 25
- direct transfer: sending server to receiving server
- Three phases of transfer:
  handshaking (greeting)
  transfer of messages
  closure
- command/response interaction
  commands: ASCII text
  response: status code and phrase
- messages must be in 7-bit ASCII

Example: Alice sends a message to Bob



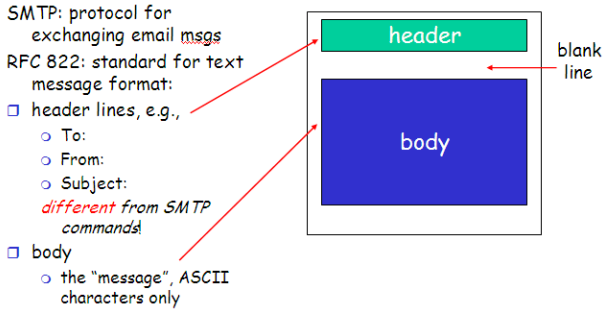
Typical SMTP Interaction



Summary

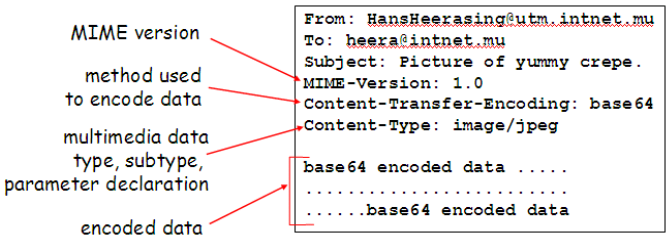
- SMTP uses persistent connections.
- SMTP requires message (header & body) to be in 7-bit ASCII.
- SMTP server uses CRLF.CRLF to determine end of message
- HTTP: pull SMTP: push
- Both have ASCII command/response interaction, status codes.
- HTTP: each object encapsulated in its own response message.
- SMTP: multiple objects sent in multipart messages.

Mail Message Format



Message format: Multipurpose Internet Mail Extensions

- MIME: Multipurpose Internet Mail Extension, RFC 2045, 2056
- Additional lines in message header declare MIME content Type and Version.



MIME Types:
Content-type: type/subtype, parameters
Text: example subtypes: plain, html
Image: example subtypes: jpeg, gif
Audio: example subtypes: basic (8-bit μ-law encoded), 32kbps PCM (32 kbps coding)
Video: example subtypes: mpeg, qt (QuickTime)
Application: example subtypes: msword, octet-stream

Mail Access Protocols
Mail access protocol: retrieval from server

1. POP: Post Office Protocol [RFC 1939] authorization (agent <-->server) and download.
2. IMAP: Internet Mail Access Protocol [RFC 1730] more features and more complex manipulation of stored messages on server.
3. HTTP: Hotmail, Gmail, etc. (Not technically email when accessed within a browser instead of an email client as HTTP is not a dedicated protocol for email communication.)

Properties of POP3

- Previous example uses "download and delete" mode.
- Bob cannot re-read e-mail if he changes client
- "Download-and-keep": copies of messages on different clients
- POP3 is stateless across sessions

IMAP Protocols

- Keep all messages in one place: the server.
- Allows user to organize messages in folders.
- IMAP keeps user state across sessions:
  names of folders and mappings between message IDs and folder name.

DNS- Domain Name System

People – Many Identifiers: Social Security #, National ID #...

What about internet hosts, routers, etc…?

- IP address (32/128 bit) – used for addressing datagrams.
- Domain Name, e.g. wtlab.utm.ac.mu used by us.

What is responsible for mapping IP Address to Domain Names? DNS

DNS

- Distributed Database - implemented in hierarchy of many *name servers.*
- Application-Layer Protocol – Host, routers, name servers to communicate to *resolve* names (Address/Name Translation) *Note: Complexity at Network's "edge"*

Why not have a centralized DNS?

- Single point of failure
- Traffic volume
- Distant centralized database
- Maintenance
- No one server has all name-to-IP address mappings.

LOCAL NAME SERVERS

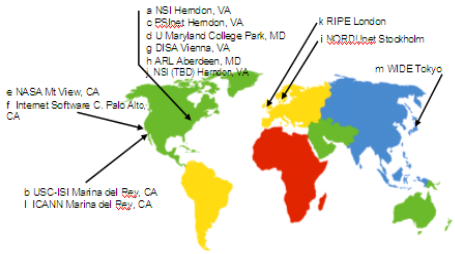
- Each ISP, company has a local default name server e.g. MyT primary DNS server is at IP 202.123.2.6, MyT secondary DNS server is at IP 202.123.2.11 Google primary DNS server is at IP 8.8.8.8 and secondary at IP 8.8.4.4.
- Client DNS query first goes to local name server.

AUTHORITATIVE NAME SERVERS

- For a host: stores that host's IP address, name.
- Can perform name/address translation for that host's name.

ROOT NAME SERVERS

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server



13 root name servers worldwide

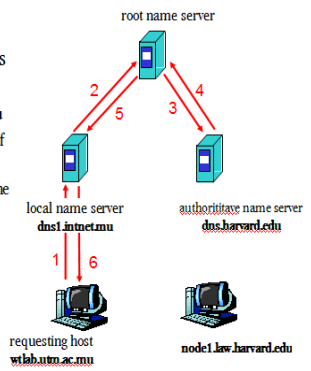
List of Root Servers

Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Simple DNS example

Host **wtlab.utm.ac.mu** wants IP address of **node1.law.harvard.edu**

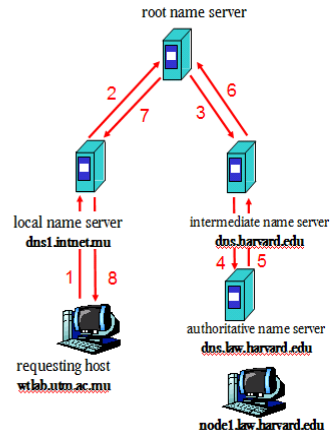
1. contacts its local DNS server, **dns1.intnet.mu**
2. **dns1.intnet.mu** contacts root name server, if necessary.
3. root name server contacts authoritative name server, **dns.harvard.edu**, if necessary



DNS example

Root name server:

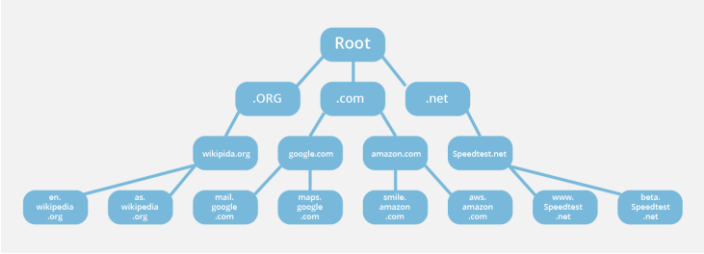
- may not know authoritative name server
- may know *intermediate name server:* who to contact to find authoritative name server



DNS: Caching and updating records.

- Once (any) name server learns mapping, it caches mapping
- Cache entries timeout and gets refreshed after some time (24-48 Hours)

Sample DNS Hierarchy



Transport Layer

- Transport Layer Services and Protocols
- Multiplexing and De-multiplexing
- Connectionless Transport: UDP
- Connection-Oriented Transfer: TCP
    a. Segment Structure
    b. Reliable Data Transfer
    c. Flow Control
    d. Connection Management

Transport Layer Services and Protocols

Transport Layer Services provide ***logical communication*** between application processes running on different host.

Transport layer Protocols run on **end-systems**:

Sending side: breaks ***Application Layer messages*** into ***segments***, passes them to ***Network Layer***

Receiving side: reassembles ***segments*** into ***messages***, passes them to ***Application Layer.***

Transport layer Protocols available to applications:

Internet: ***TCP*** and ***UDP***

Transport Layer v/s Network Layer

Network Layer provides ***logical communication*** between hosts.

Transport Layer provides ***logical communication*** between processes relies on, enhances, **network layer** services.

Household Analogy: e.g., *12 kids in Ann's house sending letters to 12 kids in Bill's house:*

- hosts = houses
- processes = kids
- application messages = letters in envelopes
- Transport Layer protocol = Ann and Bill (identified & unique processes.)
- Network Layer protocol = postal service

Internet Transport-Layer Services

TCP

- ***reliable, in-order delivery***
- ***congestion control (not covered)***
- ***flow control, error control***
- ***connection setup management***

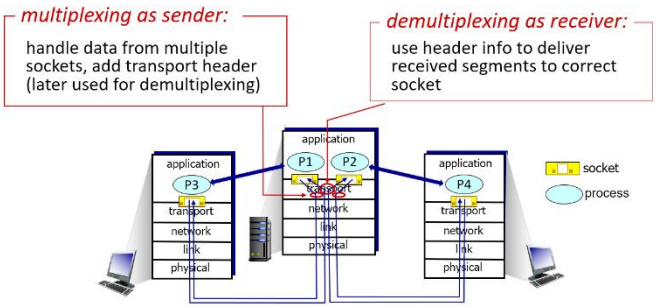
UDP

- ***no-frills (best-effort service)***
- ***unreliable, unordered delivery***
- ***minimal error control***

SERVICES NOT AVAILABLE TO BOTH:

- ***Delay guarantees***
- ***Bandwidth guarantees***

Multiplexing and Demultiplexing

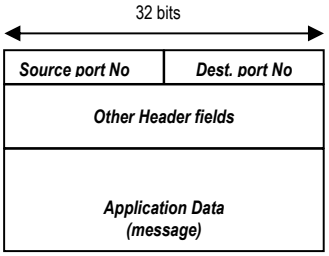


How demultiplexing works?

Host receives ***IP datagrams*** (will learn later)

1. each datagram has source ***IP address***, destination ***IP address. (will learn later)***
2. each datagram carries ***1 Transport Layer segment***
3. each segment has ***source and destination port numbers***. (***recall: well-known port numbers for specific application protocols***)

Host uses **IP addresses & Port Numbers** to direct segment to appropriate socket.

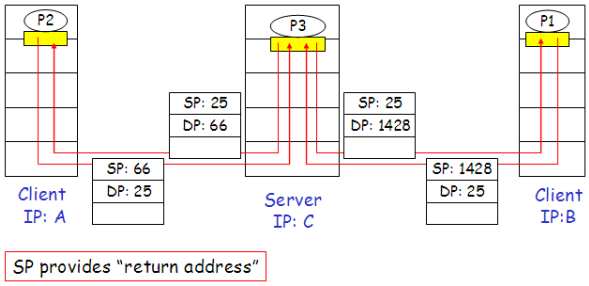


Generic *TCP* or *UDP* segment

Connectionless demultiplexing: UDP

UDP socket identified by two-parameters: (***destination IP address***, ***destination port number***)

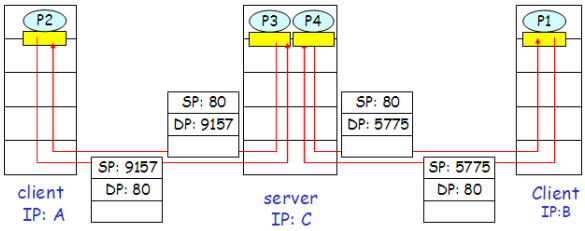
- When host receives ***UDP segment***:
  checks ***destination port number*** in segment.
  directs UDP segment to socket with that ***port number.***
- ***IP datagrams*** with different source ***IP addresses*** and/or ***source port numbers*** directed to same socket.



Connection-Oriented demultiplexing: TCP

TCP socket identified by four parameters: (***source IP address***, ***source Port number***, ***dest IP address***, ***dest port number***)

- Receiving host uses all four values to direct segment to appropriate socket.
- Server host may support many simultaneous **TCP** sockets:
  - each socket identified by its own 4 parameters.
- Web servers have different sockets for each connecting client
  - *Non-persistent HTTP* will have different socket for each request.



<u>Connectionless Transport: UDP [RFC 768]</u>

- "no frills" Internet Transport Protocol
- "best effort" service, UDP segments may be:
  - lost
  - delivered out of order to applications
- *connectionless-oriented:*
  - no handshaking between parties
  - each UDP segment handled independently of others

Why is there a UDP?

- no connection establishment (which add delay)
- simple: no connection state at sender, receiver
- small segment header
- no congestion control: UDP can blast away as fast as desired

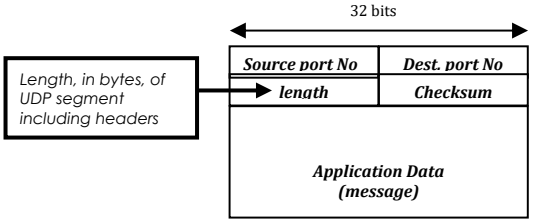
Where do we use UDP?

- often used for ***streaming multimedia*** applications
  - **loss tolerant**
  - **rate-sensitive**

- other UDP uses
  - **DNS (*Domain Name Service*)**
  - **SNMP (*Simple Network Management Protocol*)**

- How to achieve "reliable" transfer over UDP?

  - **add reliability at application layer.**
  - **Application-specific error recovery!**



UDP Segment Format

UDP Checksum

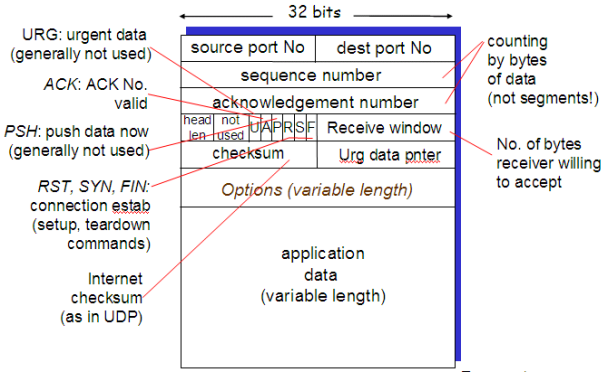
- ***Goal:*** detect "errors" (flipped bits) in transmitted segment
- ***Sender:***
  - treat segment contents as **sequence of 16-bit integers.**
  - **checksum**: addition (1's complement sum) of segment contents
  - sender puts ***checksum value*** into ***UDP checksum field***
- ***Receiver:***
  - compute ***checksum*** of received segment
  - check if computed ***checksum*** equals *checksum field value*:
    NO - error detected
    YES - no error detected. *But maybe errors nonetheless?* More later ….

Connection-Oriented Transport: TCP [RFC 793]

Transmission Control Protocol

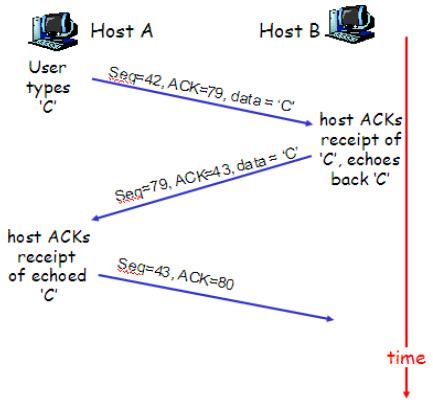
- **point-to-point:**
  - one sender, one receiver
- **reliable, in-order *byte steam:***
  - no "message boundaries"
- **pipelined:**
  - TCP congestion and flow control set window size
- **send & receive buffers**
- **full duplex data:**
  - bi-directional data flow in same connection
  - MSS: maximum segment size
- **connection-oriented:**
  - handshaking (exchange of control messages) initialise sender, receiver states before data exchange
- **flow controlled:**
  - sender will not overwhelm receiver

TCP Segment Structure



TCP Sequence Nos. and ACK Nos.

Simple Telnet Scenario:



- **Sequence Nos.:**
  - byte stream "number" of first byte in segment's data.
- **ACK Nos.:**
  - Sequence No. of next byte expected from other side
  - cumulative ACK

TCP Round Trip Time (RTT) and Timeout

Question: *How to set TCP timeout value?*

- longer than RTT
  - but RTT varies
- too short: premature timeout
  - unnecessary retransmissions
- too long: slow reaction to segment loss

Reliable Data Transfer

TCP creates *reliable data transfer* service on top of IP's unreliable service.

- *Pipelined* segments.
- *Cumulative Acks*

TCP uses single *retransmission timer.*

Retransmissions are triggered by:

- T*imeout events*
- *Duplicate ACKS*

Initially consider simplified TCP sender:

- ignore duplicate ACKS
- ignore flow control, congestion control

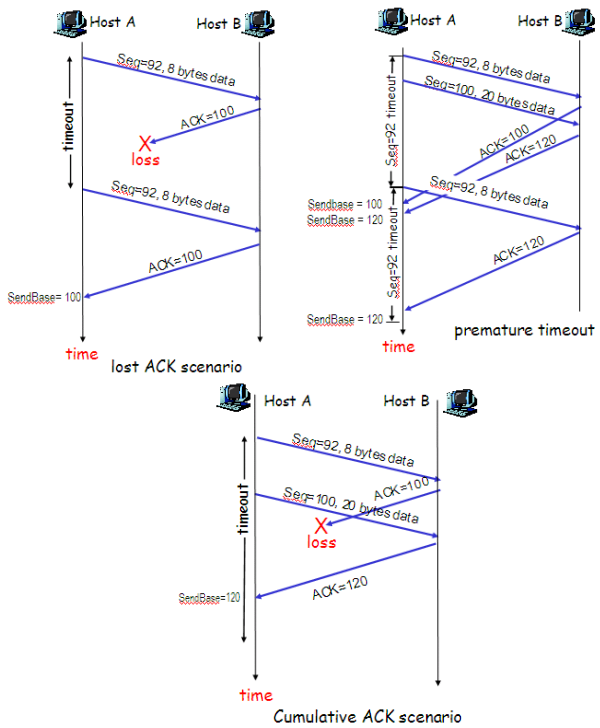
TCP Sender Events

- Data received from Applications:
  - Create segment with sequence nos.
  - Sequence no. is byte-stream number of first data byte in segment.
  - start timer if not already running (think of timer as for oldest unACKed segment)
  - expiration interval: TimeOutInterval

- Timeout:
  - retransmit segment that caused timeout
  - restart timer

- ACK received:
  - If acknowledges previously unACKed segments
  - update what is known to be ACKed
  - start timer if there are any outstanding segments

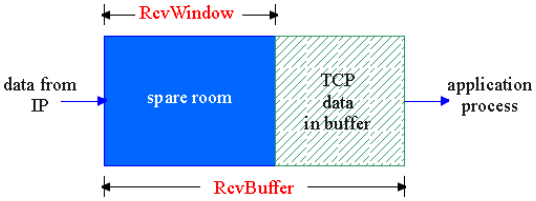
3 TCP Transmission Scenarios



TCP Flow Control

Reason: Sender won't overflow receiver's buffer by transmitting too much, too fast.

- receive side of TCP connection has a receive buffer:



Application process may be slow at reading from buffer
Speed-matching service: matching the send rate to the receiving application's drain rate.

How it works?

(Suppose TCP receiver discards out-of-order segments)

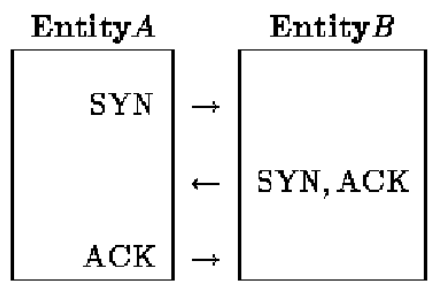
- **spare room in buffer**
  = RcvWindow
  = RcvBuffer-[LastByteRcvd - LastByteRead]
- Reciever advertises spare room by including value of RcvWindow in segments
- Sender limits unACKed data to RcvWindow
- guarantees receive buffer doesn't overflow

TCP Connection Management

- TCP sender, receiver establish "connection" before exchanging data segments
- initialize TCP variables:
  - seq. #s
  - buffers, flow control info (e.g. RcvWindow)

Opening a connection (Three-Way Handshake)

- Step 1: client host sends TCP SYN segment to server
  - specifies initial seq #
  - no data
- Step 2: server host receives SYN, replies with SYNACK segment
  - server allocates buffers
  - specifies server initial seq. #
- Step 3: client receives SYNACK, replies with ACK segment, which may contain data

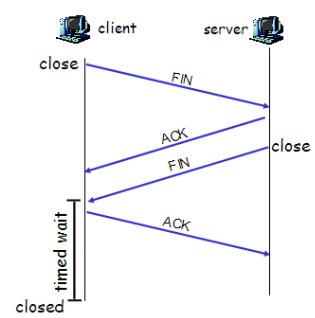


Closing a connection:

client closes socket:
`clientSocket.close();`

Step 1: client end system sends TCP FIN control segment to server

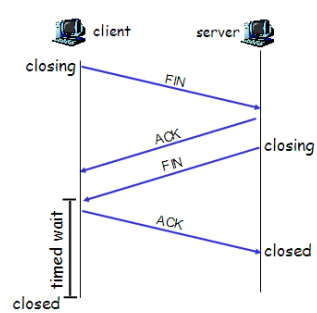
Step 2: server receives FIN, replies with ACK. Closes connection, sends FIN.



Step 3: client receives FIN, replies with ACK.
- Enters "timed wait" - will respond with ACK to received FINs

Step 4: server, receives ACK. Connection closed.

Note: with small modification, can handle simultaneous FINs.



Network Layer

- Network Layer Services
- IPv4
- Internet Routing Protocols: Reliable Transfer

Network Layer Services
Network Layer Functions

- transport packet from sending to receiving hosts
- network layer protocols in *every* host, router

Three important functions:

- *path determination:* route taken from source to destinations. (*Routing algorithms)*
- *forwarding:* move packets from router's input to appropriate router output.
- *call setup:* some network architectures require router call setup along path before data flows.

Network Service Model
Which *service model* for transporting packets from sender to receiver?

- guaranteed bandwidth?
- preservation of inter-packet timing (no jitter)?
- loss-free delivery?
- in-order delivery?
- congestion feedback to sender?

The most important abstraction provided by network layer: **Virtual Circuits** or **Datagrams? Big fight!!!**

Virtual Circuit: The Telephone Model
Source-to-Destination path behaves much like a telephone circuit:

- performance-wise
- network actions along source-to-destination path

How it works?

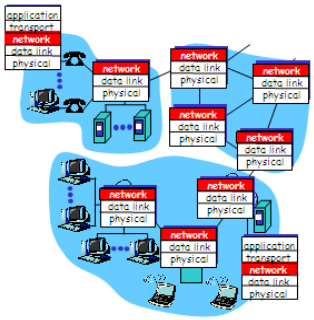
- call setup, teardown for each call *before* data can flow
- each packet carries VC Identifier (not destination host ID)
- *every* router on source-destination path keeps *state* for each passing connection

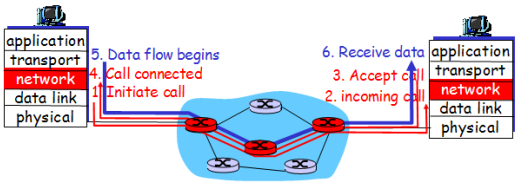
Note: Transport-layer connections only involved in the two end systems.

- link, router resources (bandwidth, buffers) may be *allocated* to VC to get circuit-like performance.

Signaling Protocols

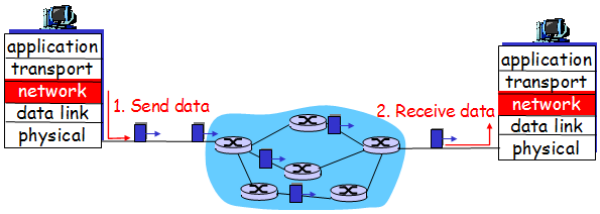
- used to setup, maintain, and teardown Virtual Circuit
- used in ATM, frame-relay, X.25 (*last two obsolete now*)





Datagram Network: The Internet Model

- no call setup at network layer
- routers: no state about end-to-end connections
  - no network-level concept of "connection"
- packets forwarded using destination host address
  - packets between same source-destination pair may take different paths



Network Layer Service Model Comparison Chart

Network Architecture	Service Model	Guarantees ? Bandwidth	Loss	Order	Timing	Congestion feedback
Internet	best effort	none	no	no	no	no (inferred via loss)
ATM	CBR	constant rate	yes	yes	yes	no congestion
ATM	VBR	guaranteed rate	yes	yes	yes	no congestion
ATM	ABR	guaranteed minimum	no	yes	no	yes
ATM	UBR	none	no	yes	no	no

Datagram v/s VC Network: Why?

Internet:

- data exchange among computers
  "elastic" service, no strict timing requirements.
- "smart" end systems (computers)
  can adapt, perform control, error recovery.
  simple inside network, **complexity** at "edge"
- many link types
  different characteristics, thus a uniform service is difficult to achieved.

ATM:

- evolved from telephony
- human conversation:
  - strict timing, reliability requirements
  - need for guaranteed service
- "dumb" end systems
  - telephones
  - **complexity** inside network

Hierarchal Routing

Our routing study has so far been idealized. But this is not true in practice!!! ***Why?***

1. All routers are not identical
2. Network is not 'flat'.

Assume that there are roughly about **200 million** nodes, we obviously cannot store all those destinations in routing tables because routing exchange will saturate links.

Solution: **Administrative Autonomy**

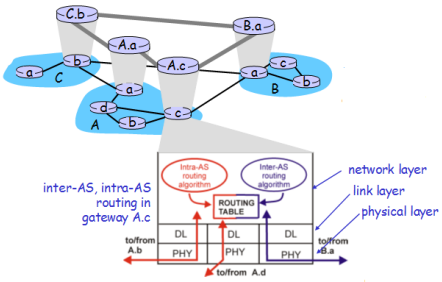
- **internet** = network of networks
- each **network administrator** may want to control routing in its own network

Aggregate routers into regions, "A**utonomous Systems**"
Routers in same **AS** run same routing protocol

- "***intra-AS***" routing protocol
- routers in different AS can run different ***intra-AS*** routing protocol

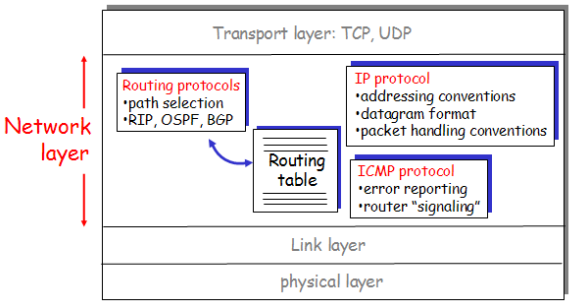
Gateway/Border Routers

- special routers in AS
- run ***intra-AS*** routing protocol with all other routers in AS
- *also* responsible for routing to destinations ***outside AS***
  i.e. run ***inter-AS*** routing protocol with ***other gateway routers***

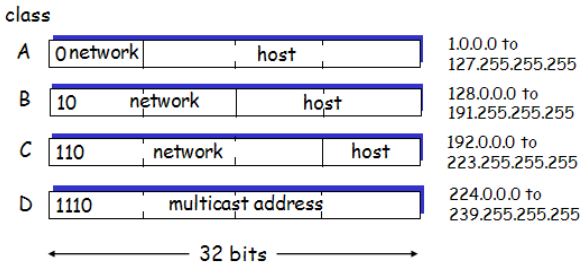


The Internet Protocol (IP) revisited

Network Layer Functions (overview)



IP Addressing "Class-full" (revisited)



Classless Inter Domain Routing (CIDR)

IP has been extremely successful with its exponential growth, but it is running out of address space.
In principle, over 2 billion addresses exist, but in practice millions of them are wasted by classes.
For most organizations, class A with 16 million addresses is too big and class C with 256 addresses is too small.
A class B network with 65,536 is just right.
Studies have shown that more than half of all class has fewer than 50 hosts.
Another problem is table explosion. Routers do not have to know about all the hosts, but they know about other networks.
Having ½ a million class C networks, every router would require a table with ½ a million entries.
The routing table problem can be solved by going to a deeper hierarchy (like telephone), but it requires more than 32-bit for IP addresses.
Most solutions solve 1 problem but create new ones.
One solution currently being implemented is **Classless Inter Domain Routing.**
The basic idea behind CIDR is to allocate the remaining class C networks (almost 2 million) in variable-sized blocks.

- If a site needs 2000 addresses, it is given 2048 addresses (8 contiguous class C networks), and not a full class B address.

In addition to using contiguous blocks, the allocation rules were also changed. The world was partitioned into 4 zones.

- Europe: 194.0.0.0 to 195.255.255.255
- North America: 198.0.0.0 to 199.255.255.255
- Central and South America: 200.0.0.0 to 201.255.255.255
- Asia and Pacific: 202.0.0.0 to 203.255.255.255

Each region was given 32 million addresses, with another 320 million class C addresses from 204.255.255.255 to 223.255.255.255 reserved for future use. Within each block allocate sub-block to ISP. ISP then allocates to customers. Restrict block sizes to powers of 2.
All routers must understand CIDR addressing
Let's see this at work…

How does Host get IP address?

- Hard-coded by system admin in a file
  - Wintel: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config file
- **DHCP**: Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play" (more later)

How does an ISP get block of addresses?

- ***ICANN***: **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers
  - allocates addresses
  - manages DNS
  - assigns domain names, resolves disputes

Getting a datagram from Source to Destination

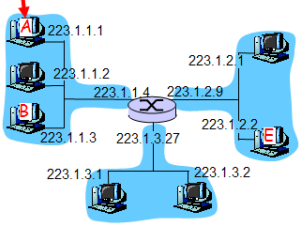
IP datagram:

misc fields	source IP addr	dest IP addr	data

- datagram remains unchanged, as it travels source to destination
- addr fields of interest here

forwarding table in A

Dest. Net.	next router	Nhops
223.1.1		1
223.1.2	223.1.1.4	2
223.1.3	223.1.1.4	2



Case 1

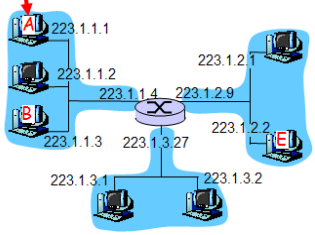
misc fields	223.1.1.1	223.1.1.3	data

Starting at A, send IP datagram addressed to B:

- look up net. address of B in forwarding table
- find B is on same net. as A
- link layer will send datagram directly to B inside link-layer frame
  - B and A are directly connected

forwarding table in A

Dest. Net.	next router	Nhops
223.1.1		1
223.1.2	223.1.1.4	2
223.1.3	223.1.1.4	2



Case 2

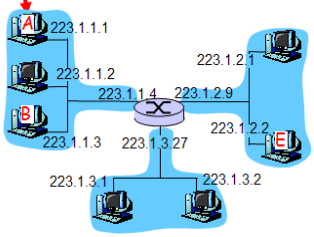
misc fields	223.1.1.1	223.1.2.3	data

Starting at A, dest. E:

- look up network address of E in forwarding table
- E on *different* network
  - A, E not directly attached
- routing table: next hop router to E is 223.1.1.4
- link layer sends datagram to router 223.1.1.4 inside link-layer frame
- datagram arrives at 223.1.1.4
- continued…..

forwarding table in A

Dest. Net.	next router	Nhops
223.1.1		1
223.1.2	223.1.1.4	2
223.1.3	223.1.1.4	2



Case 3

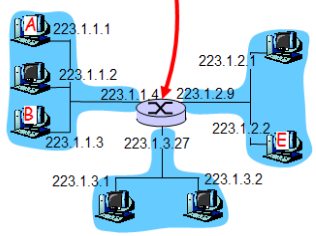
misc fields	223.1.1.1	223.1.2.3	data

Arriving at 223.1.4, destined for 223.1.2.2

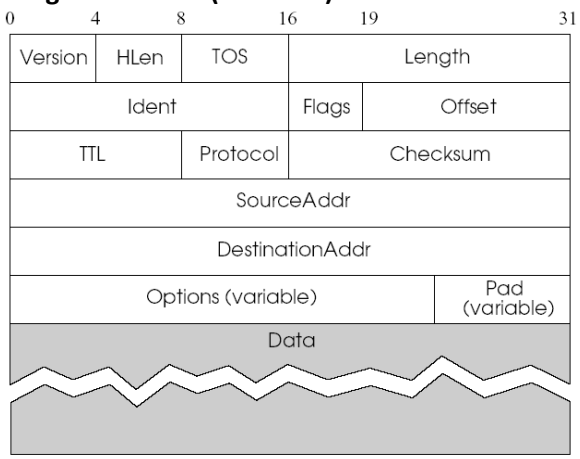
- look up network address of E in router's forwarding table
- E on *same* network as router's interface 223.1.2.9
  - router, E directly attached
- link layer sends datagram to 223.1.2.2 inside link-layer frame via interface 223.1.2.9
- datagram arrives at 223.1.2.2!!! (hooray!)

forwarding table in router

Dest. Net	router	Nhops	interface
223.1.1	-	1	223.1.1.4
223.1.2	-	1	223.1.2.9
223.1.3	-	1	223.1.3.27



IP Datagram Format (revisited)



Network Layer (Cont.)

- IP fragmentation and Reassembly
- ICMP
- DHCP
- Inside the Router
- IPv6
- Mobility

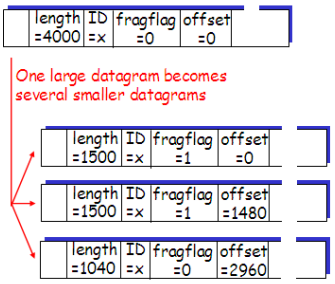
IP Fragmentation and Reassembly

Each network has some MTU (Max Transmission Unit) Size

Strategy

- Fragment when necessary (MTU < Datagram)
- IP packet needs to _t in payload part of frame
- Try to avoid fragmentation at source host
- Re-fragmentation is possible at routers etc.
- Fragments are self-contained datagrams
- All fragments contain same value in **ident field**
- Each fragment is re-encapsulated in frame
- Delay reassembly until destination host
- Do not recover from lost fragments
- IP header bits used to identify, order related fragments

Example
- 4000 byte datagram
- MTU = 1500 bytes



Internet Control Message Protocol (ICMP)

- used by hosts, routers, gateways to communication network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

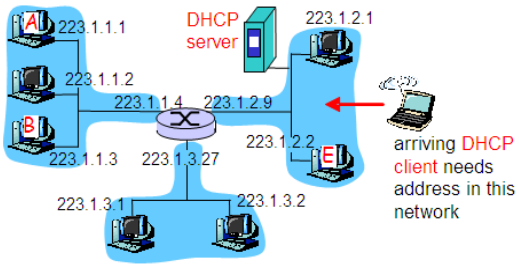
Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

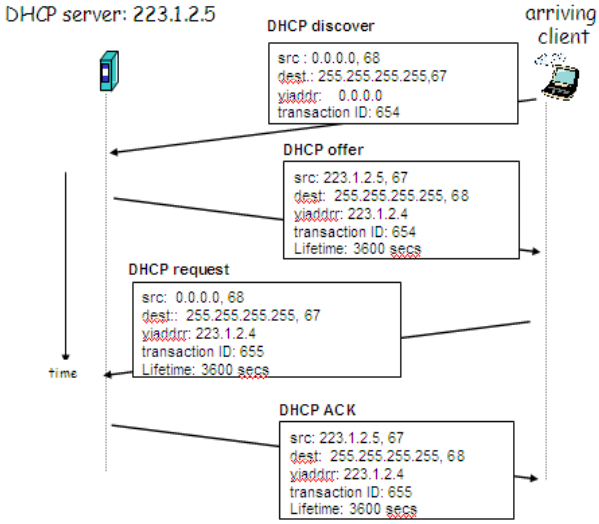
Dynamic Host Control Protocol (DHCP)

Goal: allow host to *dynamically* obtain its IP address from network server when it joins network
- Can renew its lease on address in use
- Allows reuse of addresses (only hold address while connected an "on"
- Support for mobile users who want to join network (more shortly)

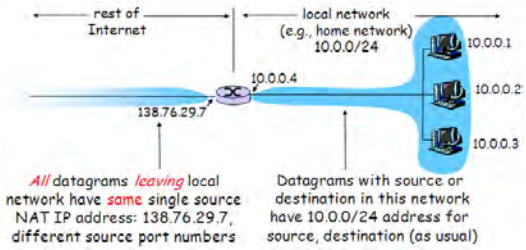
DHCP overview:
- host broadcasts "DHCP discover" msg
- DHCP server responds with "DHCP offer" msg
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

DHCP Client-Server Scenario





Network Address Translation (NAT)

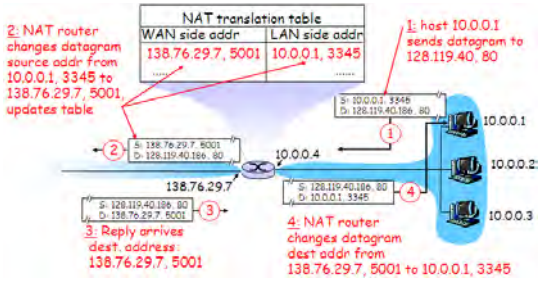


Motivation: local network uses just one IP address as far as outside word is concerned:

- no need to be allocated range of addresse from ISP: - just one IP address is used for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly visible by outside world (a security plus).

Implementation: NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #) . . . remote clients/servers will respond using (NAT IP address, new port #) as destination address.
- *remember in translation table* every (source IP add, port#) to (NAT IP add, new port#) translation pair
- *incoming datagrams: replace* (NAT IP address, new port #) in destination fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table



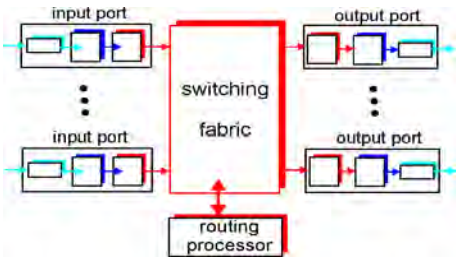
Conclusion:

16-bit port-number field: 65,536 simultaneous connections with a single LAN-side address!
NAT controversial as routers should only process up to L3.
NAT possibility must be envisaged by app developers as IP address shortage instead solved by IPv6

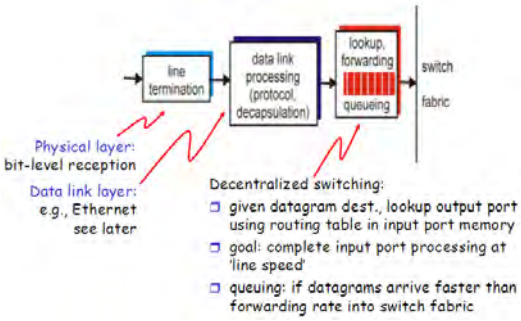
Inside the Router?

Two key router functions:

run routing algorithms/protocol (RIP, OSPF, BGP)
routing datagrams from incoming to outgoing link.

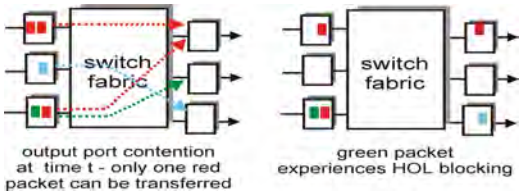


Input port functions



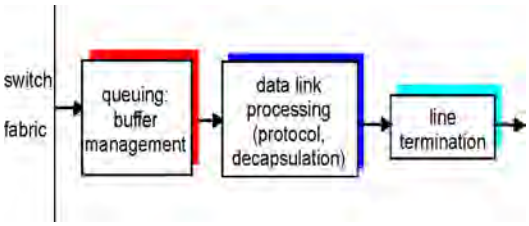
Input port queuing

- Fabric slower that input ports combined -> queuing may occur at input queues
- Head-of-the-Line (HOL) blocking: queued datagram at front of queue prevents others in queue from moving forward
- queuing delay and loss due to input buffer overflow!

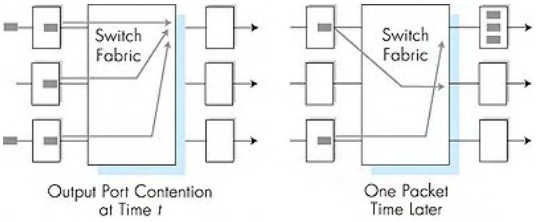


Output ports

- *Buffering* required when datagrams arrive from fabric faster than the transmission rate
- *Scheduling discipline* chooses among queued datagrams for transmission



- buffering when arrival rate via switch exceeds output line speed
- *queueing (delay) and loss due to output port buffer overflow!*



Ipv6

- CIDR may last for a few years, but everyone realizes that the days of IP in its current form (IPv4) are numbered. (by 2008, all addresses will run out)
- Besides growing number of mobile stations, it may not be long before every TV set is an Internet node, producing billion machines.
- IETF has started working on a new version of IP, which would never run out of addresses, and solving a variety of other problems.

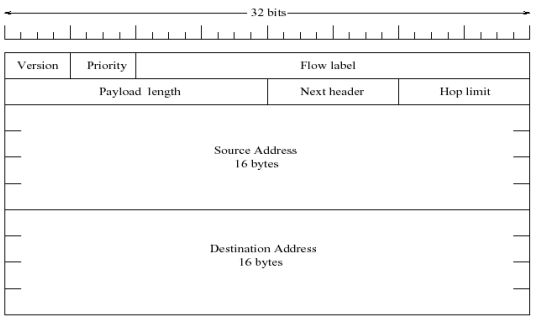
Its major goals were to:

- Supports billions of hosts, even with inefficient address space allocation.
- Reduce the size of the routing tables.
- Simplify IP to allow routers to process packets faster.
- Provide better security than current IP.
- Pay more attention to type of service, particularly for real-time data.
- Aid multicasting by allowing scopes to be specified.
  - Make it possible for a host to roam without changing its address.
  - Allow the protocol to evolve in the future.
  - Permit the old and new protocols to coexist for years.

Major Features

- 128-bit addresses (3.4 X 10^{38} addresses)
- Auto configuration
- Real-time service
- Authentication and security
- End-to-end fragmentation
- Protocol extensions

IPv6 Header Format



- Fixed 40-byte "base" header
- **Extension headers** (fixed order, mostly fixed length)
  - fragmentation
  - source routing
  - authentication and security
  - other options
- The **Version field** is always 6 for IPv6 and 4 for Ipv4.
- The **Priority field** is used to distinguish between packets whose sources can be flow controlled and those that can't
- The **Flow label** is still experimental, but will be used to allow set up of particular properties between peers.
- The **Payload length** field tells how many bytes follow the fixed 40-byte header
- The **Next header** field tells which of the (currently) six **extension headers** follows this one. If this header is last IP header the next header would be layer 4 i.e. (TCP/UDP)
- The **Hop limit** field is used to keep packets from living forever. In IPv4 this was Time To Live.
- The **Source** and **Destination fields** are fixed-length 16-byte (128 bit) addresses.

Other Changes from Ipv4

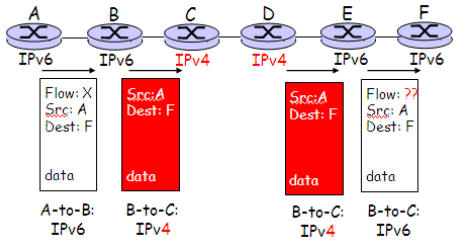
- *Checksum*: removed entirely to reduce processing time at each hop.
- *Options:* allowed, but outside of header, indicated by "Next Header" field.
- *ICMPv6:* new version of ICMP
  - extra message types, e.g. "Packet Too Big"

Transition from IPv4 to IPv6

- Not all routers can be upgraded simultaneously: i.e no "flag days" so how will the network operate with mixed IPv4 and IPv6 routers?

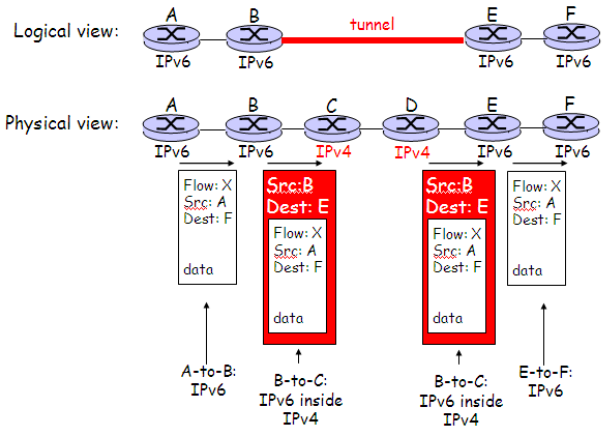
Two proposed approaches:

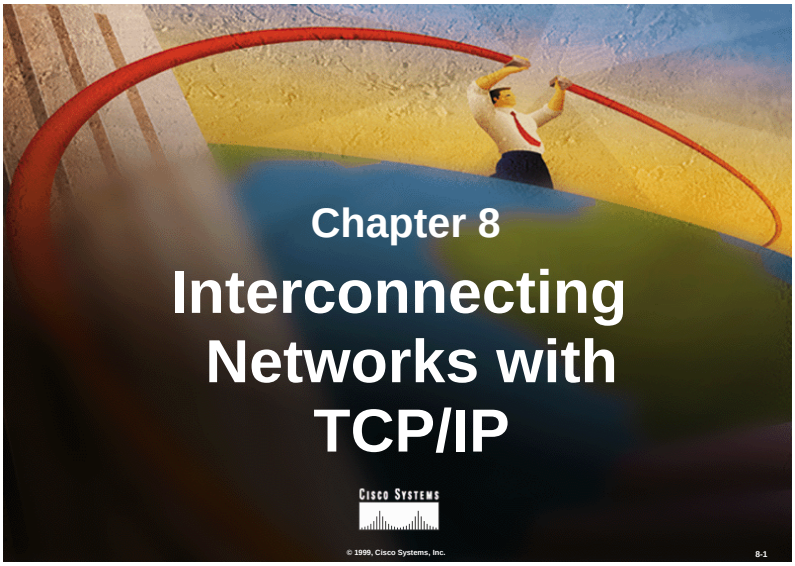
Dual Stack Approach



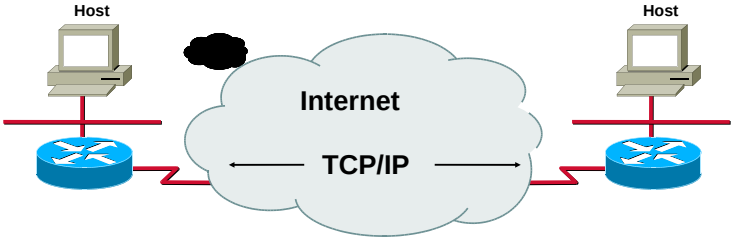
Note: flow header info lost

Tunnelling Approach





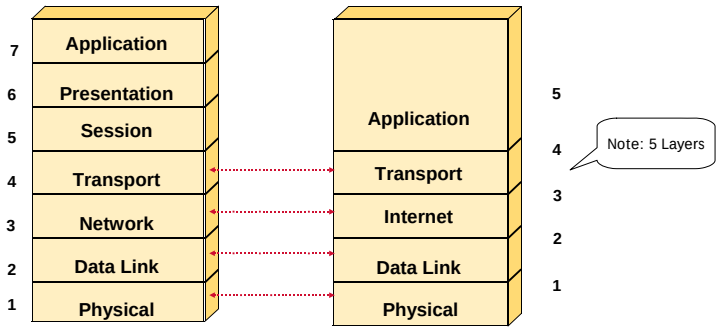
Introduction to TCP/IP



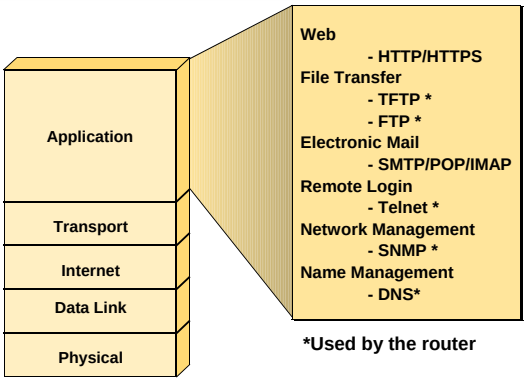
Early protocol suite

Universal

TCP/IP Protocol Stack

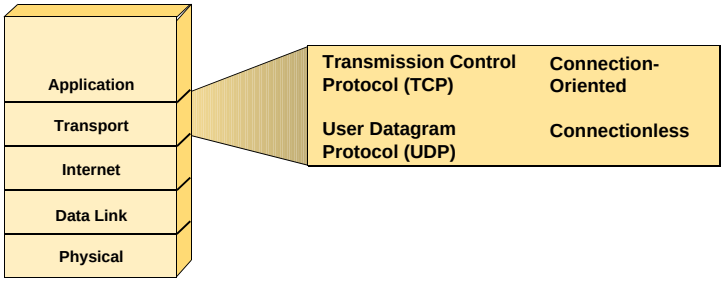


Application Layer Overview

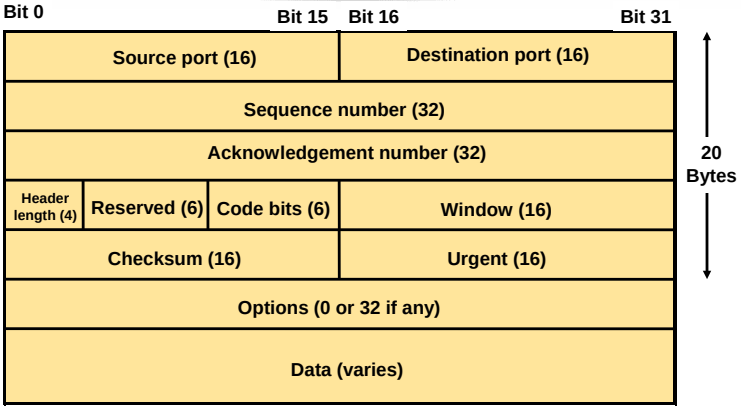


*Used by the router

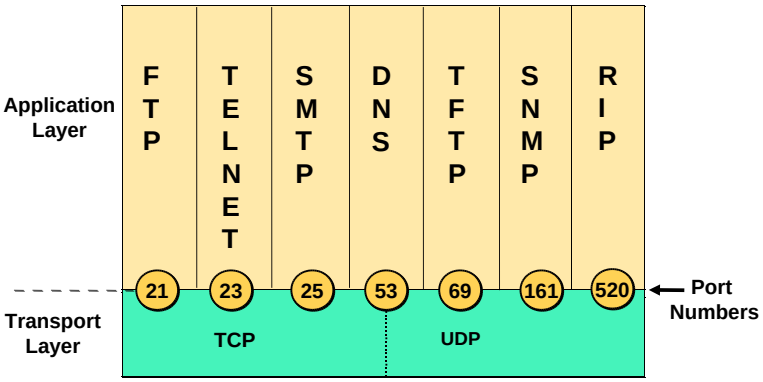
Transport Layer Overview



TCP Segment Format

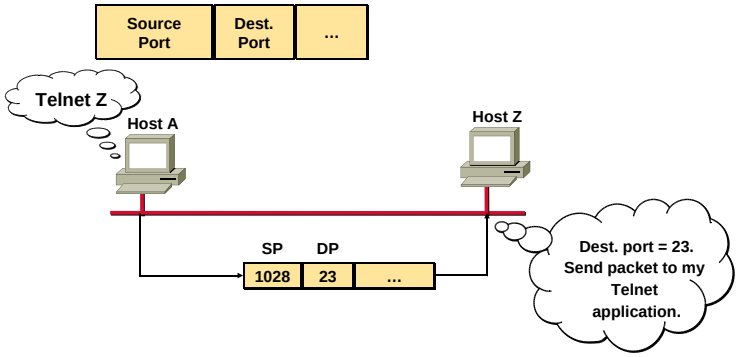


Port Numbers



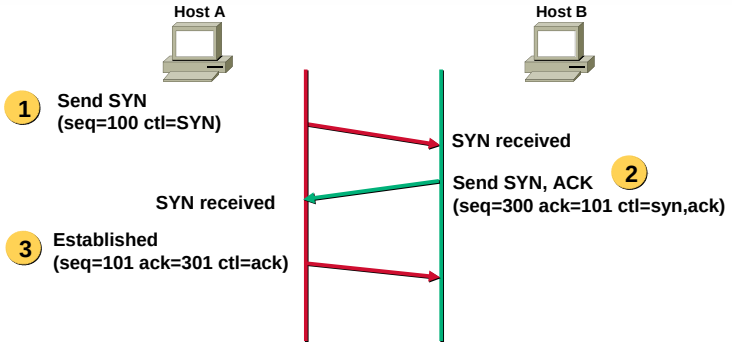
© 1999, Cisco Systems, Inc.

TCP Port Numbers



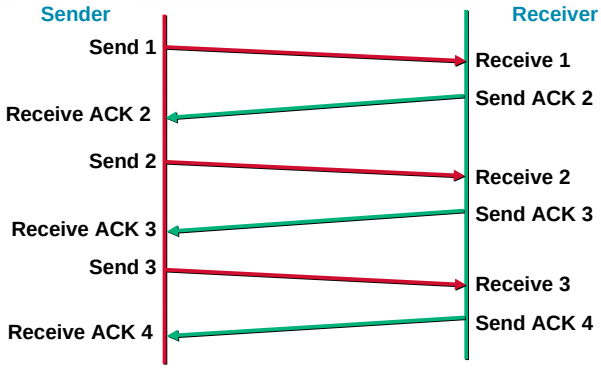
© 1999, Cisco Systems, Inc.

TCP Three Way Handshake/ Open Connection



© 1999, Cisco Systems, Inc.

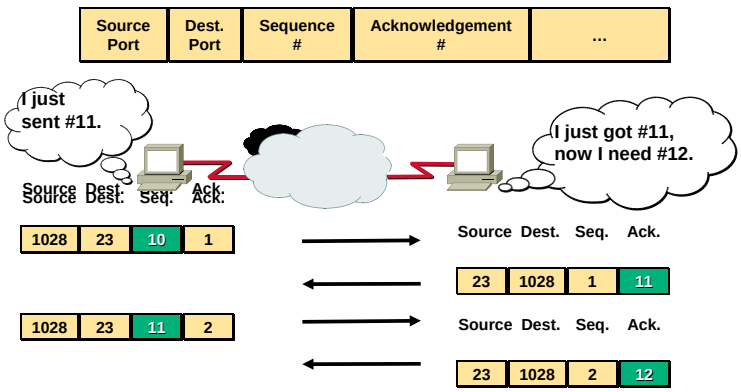
TCP Simple Acknowledgment



Window size = 1

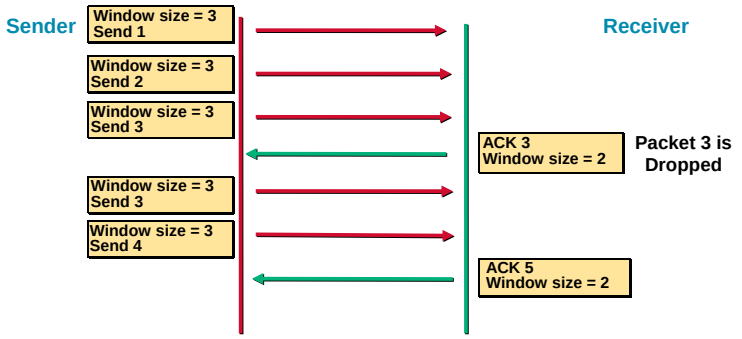
© 1999, Cisco Systems, Inc.

TCP Sequence and Acknowledgment Numbers



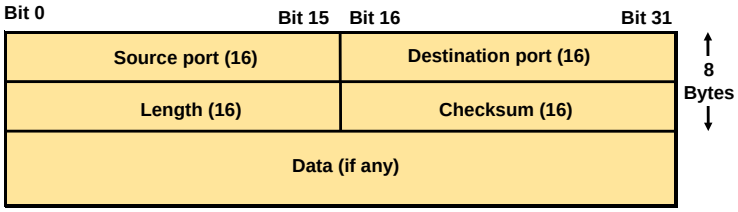
© 1999, Cisco Systems, Inc.

TCP Windowing



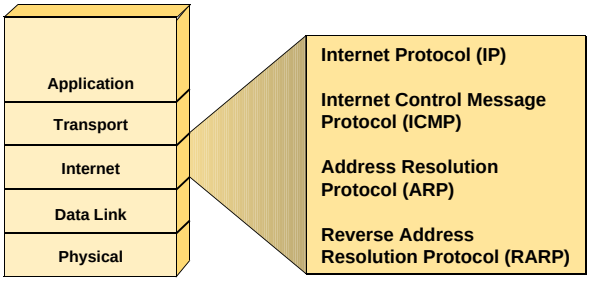
© 1999, Cisco Systems, Inc.

UDP Segment Format



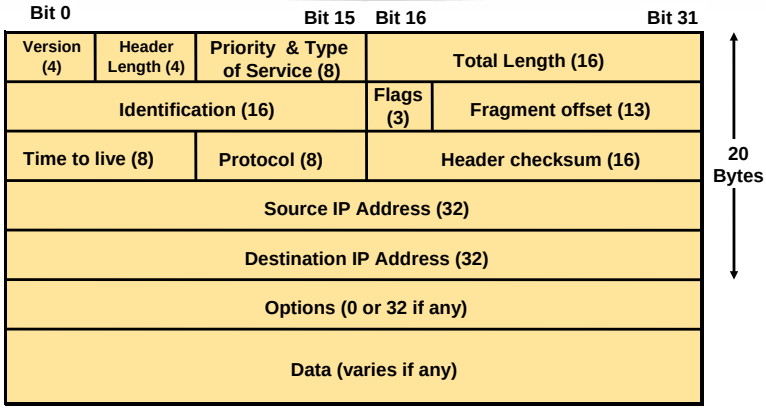
No sequence or acknowledgment fields

Internet Layer Overview

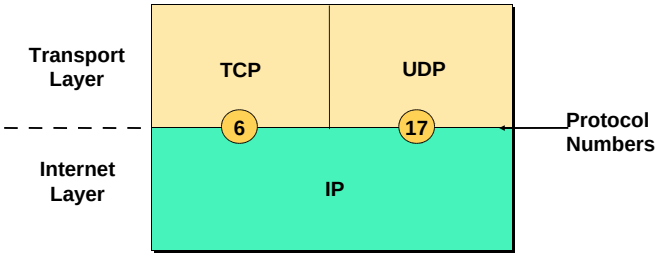


OSI network layer corresponds to the TCP/IP internet layer

IP Datagram

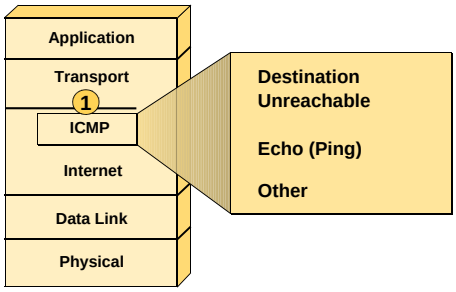


Protocol Field

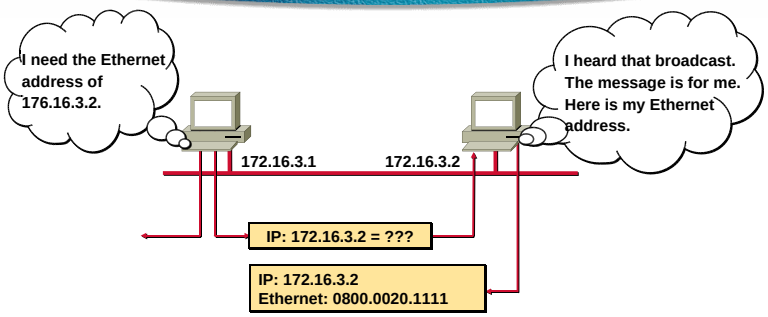


Determines destination upper-layer protocol

Internet Control Message Protocol



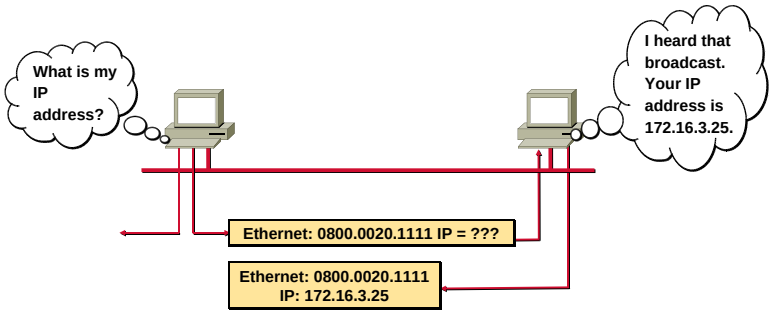
Address Resolution Protocol



Map IP → Ethernet

Local ARP

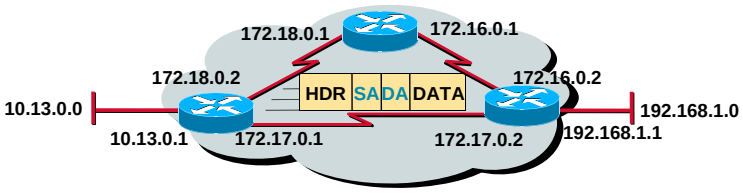
Reverse ARP



Map Ethernet → IP

© 1999, Cisco Systems, Inc.

Introduction to TCP/IP Addresses



- Unique addressing allows communication between end stations
- Path choice is based on location

© 1999, Cisco Systems, Inc.

IP Addressing

32 bits

Dotted Decimal	Network		Host	
Maximum	255	255	255	255
	1 8	9 16	17 24	25 32
Binary	11111111	11111111	11111111	11111111
	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
Example Decimal	172	16	122	204
Example Binary	10101100	00010000	01111010	11001100

© 1999, Cisco Systems, Inc.

IP Address Classes

	8 bits	8 bits	8 bits	8 bits
Class A:	Network	Host	Host	Host
Class B:	Network	Network	Host	Host
Class C:	Network	Network	Network	Host
Class D:	Multicast			
Class E:	Research			

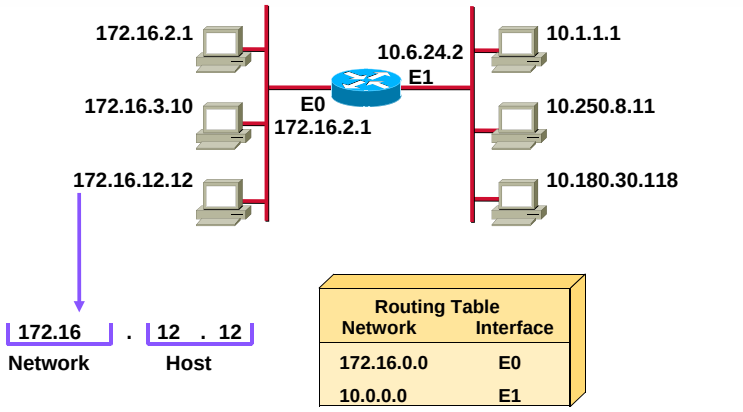
© 1999, Cisco Systems, Inc.

IP Address Classes

Bits:	1 8	9 16	17 24	25 32
Class A:	0NNNNNNN	Host	Host	Host
	Range (1-126)			
Bits:	1 8	9 16	17 24	25 32
Class B:	10NNNNNN	Network	Host	Host
	Range (128-191)			
Bits:	1 8	9 16	17 24	25 32
Class C:	110NNNNN	Network	Network	Host
	Range (192-223)			
Bits:	1 8	9 16	17 24	25 32
Class D:	1110MMMM	Multicast Group	Multicast Group	Multicast Group
	Range (224-239)			

© 1999, Cisco Systems, Inc.

Host Addresses



© 1999, Cisco Systems, Inc.

Determining Available Host Addresses

Network		Host	
172	16	0	0
10101100	00010000	00000000	00000000
		00000000	00000001
		00000000	00000011
		⋮	⋮
		11111111	11111101
		11111111	11111110
		11111111	11111111

16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

N
1
2
3
⋮
65534
65535
65536
- 2
65534

$2^N-2 = 2^{16}-2 = 65534$

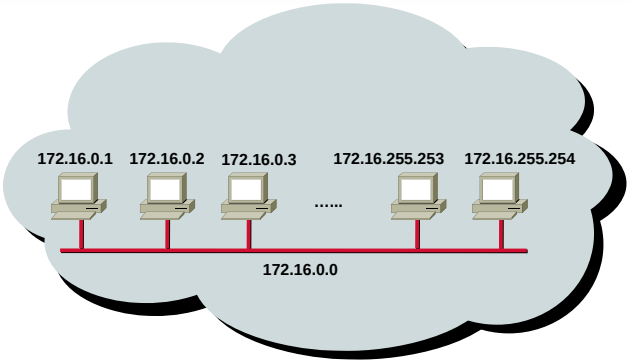
© 1999, Cisco Systems, Inc.

IP Address Classes Exercise Answers

Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
256.241.201.10			

© 1999, Cisco Systems, Inc.

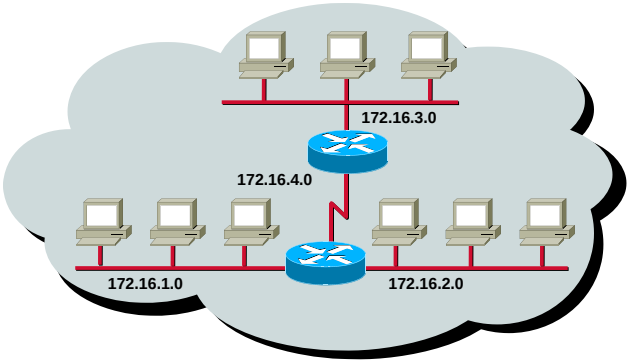
Addressing without Subnets



Network 172.16.0.0

© 1999, Cisco Systems, Inc.

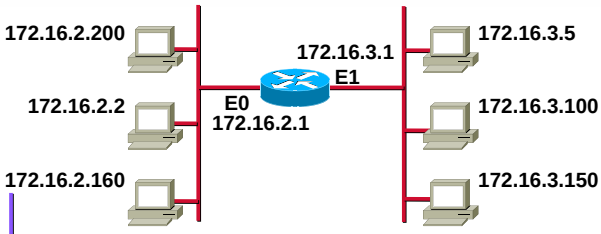
Addressing with Subnets



Network 172.16.0.0

© 1999, Cisco Systems, Inc.

Subnet Addressing

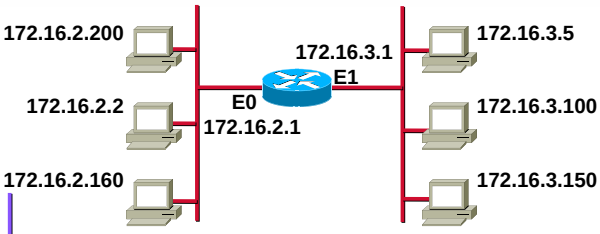


172.16 . 2 . 160
Network Host

New Routing Table Network	Interface
172.16.0.0	E0
172.16.0.0	E1

© 1999, Cisco Systems, Inc.

Subnet Addressing



172.16 . 2 . 160
Network Subnet Host

New Routing Table Network	Interface
172.16.2.0	E0
172.16.3.0	E1

© 1999, Cisco Systems, Inc.

Subnet Mask

	Network		Host	
IP Address	172	16	0	0
Default Subnet Mask	255 11111111	255 11111111	0 00000000	0 00000000

Also written as "/16" where 16 represents the number of 1s in the mask.

	Network		Subnet	Host
8-bit Subnet Mask	255	255	255	0

Also written as "/24" where 24 represents the number of 1s in the mask.

© 1999, Cisco Systems, Inc.

Decimal Equivalents of Bit Patterns

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

© 1999, Cisco Systems, Inc.

Subnet Mask without Subnets

	Network		Host	
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
Network Number	172	16	0	0

Subnets not in use—the default

© 1999, Cisco Systems, Inc.

Subnet Mask with Subnets

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.0	11111111	11111111	11111111	00000000
	10101100	00010000	00000010	00000000
Network Number	172	16	2	0

128 192 224 240 248 252 254 255

Network number extended by eight bits

© 1999, Cisco Systems, Inc.

Subnet Mask with Subnets (cont.)

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
Network Number	172	16	2	128

128 192 224 240 248 252 254 255 128 192 224 240 248 252 254 255

Network number extended by ten bits

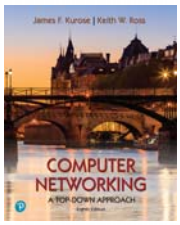
© 1999, Cisco Systems, Inc.

Subnet Mask Exercise Answers

Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0		
10.6.24.20	255.255.240.0		
10.30.36.12	255.255.255.0		

© 1999, Cisco Systems, Inc.

Computer Networking: A Top-Down Approach
8th Edition
Jim Kurose, Keith Ross
Pearson, 2020



Link Layer and LANs

Slideset 2

Link Layer and LANs

Our goals:

- understand principles behind data link layer services:
  - error detection, correction *(see separate Slide Set x)*
  - sharing a broadcast channel: multiple access
  - link layer addressing
  - Local area networks: Ethernet and VLANs
- datacentre networks
- instantiation and implementation of various link layer technologies

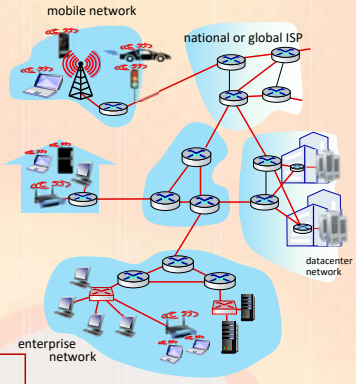
Outline

- **Introduction**
- Multiple Access protocols
- LANs
  - addressing and ARP
  - Ethernet
  - Switches
  - VLANs
- Link Virtualization: MPLS
- Data Centre networking

Link layer: introduction

terminology:

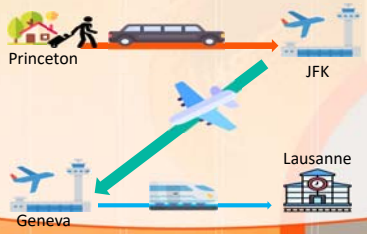
- hosts, routers: nodes
- communication channels that connect adjacent nodes along communication path: links
  - wired , wireless
  - LANs
- layer-2 packet: *frame*, encapsulates datagram



link layer has responsibility of transferring datagram from one node to physically adjacent node over a link

Link layer: context

- Datagram transferred by different link protocols over different links:
  - e.g., Ethernet on first link, frame relay on intermediate links, 802.11 on last link
- Each link protocol provides different services
  - e.g., may or may not provide reliable data transfer over link

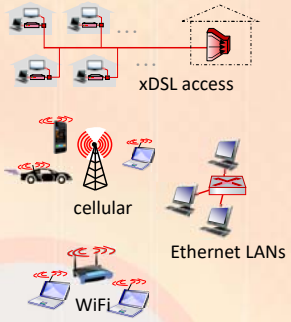


transportation analogy

- trip from Princeton to Lausanne
  - limo: Princeton to JFK
  - plane: JFK to Geneva
  - train: Geneva to Lausanne
- tourist = datagram
- transport segment = communication link
- transportation mode = link layer protocol
- travel agent = routing algorithm

Link Layer Services

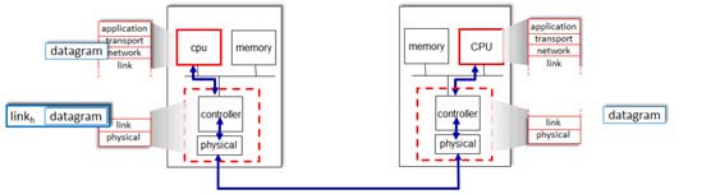
- **Framing, link access:**
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - '**MAC addresses**' used in frame headers to identify source and destination (different from IP address!)
- **Reliable delivery between adjacent nodes**
  - seldom used on low bit error link (fibre, twisted pair)
  - wireless links: high error rates



Link Layer Services

- **Flow Control:**
  - pacing between adjacent sending and receiving nodes
- **Error Detection and Correction:** ***(See Slideset 5)***
  - errors caused by signal attenuation, noise.
  - receiver detects presence of errors: signals sender for retransmission or drops frame.
  - receiver identifies ***and corrects*** bit error(s) without resorting to retransmission
- **Half-duplex / Full-duplex**
  - with half duplex, nodes at both ends of link can transmit, but not at same time

Interfaces Communicating



sending side:
- encapsulates datagram in frame
- adds error checking bits, reliable data transfer, flow control, etc.

receiving side:
- looks for errors, reliable data transfer, flow control, etc.
- extracts datagram, passes to upper layer at receiving side

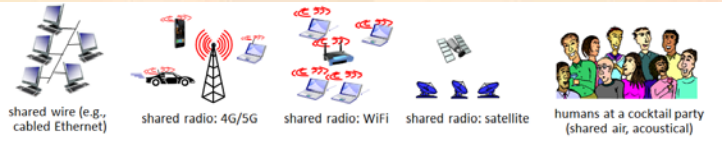
Outline

- Introduction
- **<u>Multiple Access protocols</u>**
- LANs
  - addressing and ARP
  - Ethernet
  - Switches
  - VLANs
- Link Virtualization: MPLS
- Data Centre networking

Multiple Access Links and Protocols

Two types of "links":

- point-to-point
  - PPP for dial-up access
  - point-to-point link between Ethernet switch and host
- broadcast (shared wire or medium)
  - traditional Ethernet
  - 802.11x wireless LAN. 4G/5G cellular, satellite



Multiple Access protocols

- single shared broadcast channel
- *interference:* two or more simultaneous transmissions by nodes:
  - Collision if node receives two or more signal at the same time
  - only one node can send successfully at a time

<u>Multiple Access protocol</u>

- distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
- communication about channel sharing must use channel itself!
  - No out of band channel for coordination

Ideal Multiple Access Protocol

<u>Broadcast channel of rate R bps</u>

1. When one node wants to transmit, it can send at rate R.
2. When M nodes want to transmit, each can send at average rate R/M
3. Fully decentralized:
   - no special node to coordinate transmissions
   - no synchronization of clocks, slots
4. Simple

MAC Protocols: a taxonomy

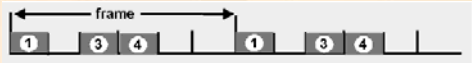
Three broad classes:

- Channel Partitioning
  - divide channel into smaller "pieces" (time slots, frequency, code) – TDMA, FDMA, CDMA
  - allocate piece to node for exclusive use
- Random Access
  - channel not divided, allow collisions
  - "recover" from collisions
- "Taking turns"
  - Nodes take turns, but nodes with more data to send cab take longer turns

Channel Partitioning MAC protocols: TDMA

TDMA: time division multiple access

- access to channel in "rounds"
- each station gets fixed length slot (length = packet trans time) in each round
- unused slots go idle
- example: 6-station LAN, slots 1,3,4 have packets, slots 2,5,6 idle

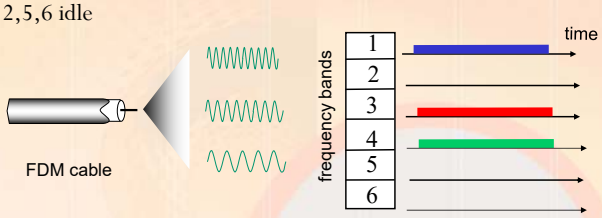


- TDM (Time Division Multiplexing): channel divided into N time slots, one per user; inefficient with low duty cycle users and at light load.
- *Road Traffic analogy: Traffic Lights*

Channel Partitioning MAC protocols: FDMA

FDMA: Frequency division multiple access

- Channel spectrum divided into frequency bands
- each station assigned a fixed frequency band.
- unused transmission time in frequency bands go idle
- example: 6-stations LAN :Stations 1,3,4 have packets to send; bands 2,5,6 idle



Road Traffic analogy: Lanes

Channel Partitioning (CDMA)

CDMA (Code Division Multiple Access)

- unique "code" assigned to each user; i.e., code set partitioning
- used mostly in wireless broadcast channels (cellular, satellite, etc)
- all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
- *encoded signal* = (original data) X (chipping sequence)
- *decoding:* inner-product of encoded signal and chipping sequence
- allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")

Road Traffic analogy: vehicles from same user have ,say, unique colour

Random Access Protocols

- When node has packet to send
  - transmit at full channel data rate R.
  - no *a priori* coordination among nodes
- When two or more transmitting nodes: *collision*
- Random Access MAC protocol specifies:
  - how to detect collisions
  - how to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - CSMA, CSMA/CD, CSMA/CA

CSMA (Carrier Sense Multiple Access)

CSMA: Listen before transmit:

- If channel sensed idle: transmit entire frame
- If channel sensed busy, defer transmission
- Human analogy: don't interrupt others!
- Collisions *can* still occur though because of the propagation delay means two nodes may not hear each other's transmission

CSMA/CD (Collision Detection)

CSMA/CD: carrier sensing, deferral as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage

- collision detection:
  - easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - difficult in wireless LANs: receiver shut off while transmitting
- human analogy: the polite conversationalist

"Taking Turns" MAC protocols

channel partitioning MAC protocols:

- share channel efficiently and fairly at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

Random access MAC protocols

- efficient at low load: single node can fully utilize channel
- high load: collision overhead

"taking turns" protocols

look for best of both worlds!

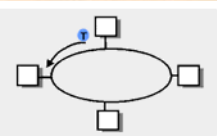
"Taking Turns" MAC protocols

Polling:

- master node "invites" slave nodes to transmit in turn
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)

Token passing:

- control **token** passed from one node to next sequentially.
- token message
- concerns:
  - token overhead
  - latency
  - single point of failure (token)



Summary of MAC protocols

- **Static Channel Partitioning**, by time, frequency or code
  - Time Division, Code Division, Frequency Division
- **Dynamic Random partitioning**,
  - CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet, CSMA/CA used in 802.11x
- **Taking Turns**
  - polling from a central site, token passing
  - Bluetooth, FDDI, Token Ring (802.5)

Outline

- Introduction
- Multiple Access protocols
- **LANs**
  - **addressing and ARP**
  - Ethernet
  - Switches
  - VLANs
- Link Virtualization: MPLS
- Data Centre networking

LANs: Addressing and ARP

32-bit IPv4 or 128-bit IPv6 address (Logical Address):

- *network-layer* address for interface
- used for layer 3 (network layer) routing
  - e.g. IPv4: 128.119.40.136
  - e,g. IPv6: 2001:0000:130F:0000:0000:09C0:876A:130B (hexadecimal notation)

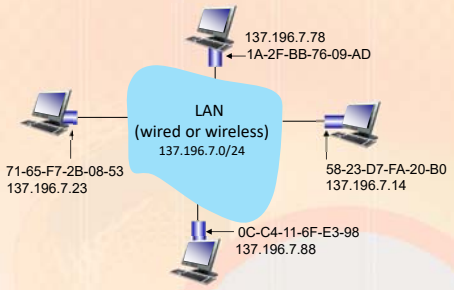
LAN (or MAC or Physical or Ethernet or Hardware) address:

- used to get datagram from one interface to another physically-connected interface (same network)
- 48-bit MAC address (for most LANs) burned in the adapter ROM and hence cannot be changed but can be also software settable.
  - E.g. 1A-2F-BB-76-09-AD (hexadecimal notation)

LANs: Addressing and ARP

Slide Set 2

Each adapter on LAN has unique 48-bit MAC address



LAN Address

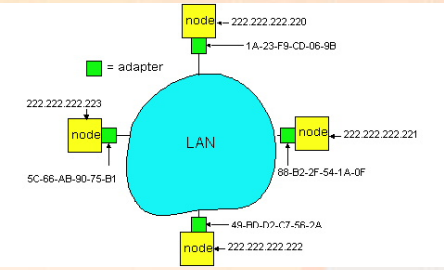
Slide Set 2

- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:
  - (a) MAC address: like Social Security Number
  - (b) IP address: like postal address
- MAC flat address => portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - depends on IP network to which node is attached

ARP: Address Resolution Protocol

Slide Set 2

***Question**: How to determine MAC address of B knowing B's IP address?*



- Each IP node (*host/router*) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes

< IP address; MAC address; TTL>

- TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

ARP protocol

Slide Set 2

- A wants to send datagram to B, and A knows B's IP address.
- Suppose B's MAC address is not in A's ARP table.
- A broadcasts ARP query packet, containing B's IP address
  - all machines on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (*unicast*)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  - *soft state*: information that times out (goes away) unless refreshed
- ARP is "plug-and-play":
  - nodes create their ARP tables without intervention from net administrator

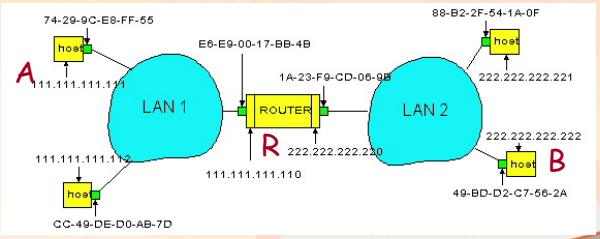
Routing to another LAN

Slide Set 2

send datagram from A to B via R;

Assume A know's B IP address

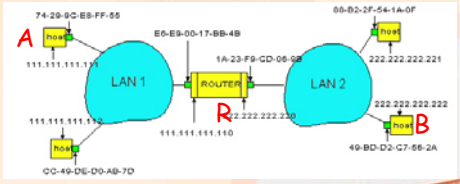
- Two ARP tables in router R, one for each IP network (LAN)
- In routing table at source Host, find router 111.111.111.110
- In ARP table at source, find MAC address **E6-E9-00-17-BB-4B**, etc



Routing to another LAN

Slide Set 2

- A creates datagram with source A, destination B
- A uses ARP to get R's MAC address for 111.111.111.110
- A creates link-layer frame with R's MAC address as dest, frame contains A-to-B IP datagram
- A's data link layer sends frame
- R's data link layer receives frame
- R removes IP datagram from Ethernet frame, sees its destined to B
- R uses ARP to get B's physical layer address
- R creates frame containing A-to-B IP datagram sends to B



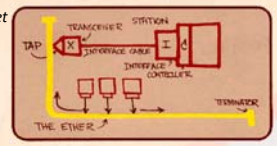
Outline

- Introduction
- Multiple Access protocols
- **LANs**
  - addressing and ARP
  - **Ethernet**
  - Switches
  - VLANs
- Link Virtualization: MPLS
- Data Centre networking

Ethernet

"dominant" wired LAN technology:
- first widely used LAN technology
- simpler, cheap
- kept up with speed race: 10 Mbps – 400 Gbps
- single chip, multiple speeds (e.g., Broadcom BCM5761)

Metcalfe's Ethernet sketch



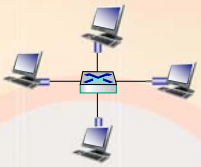
2022 ACM A.M. Turing Award Laureate

https://www.uspto.gov/learning-and-resources/journeys-innovation/audio-stories/defying-doubters

Ethernet physical topology

- bus: popular through mid 90s (*obsolete now*)
  - all nodes in same collision domain (can collide with each other)
- switched: prevails today
  - active link-layer 2 *switch* in center
  - each "spoke" runs a (separate) Ethernet protocol (nodes do not collide with each other)

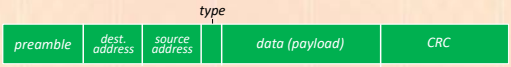
bus: coaxial cable



Switched
Twisted pair cable

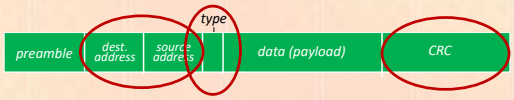
Ethernet Frame Structure

sending interface encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame



preamble:
- used to synchronize receiver, sender clock rates
- 7 bytes of 10101010 followed by one byte of 10101011

Ethernet Frame Structure (more)



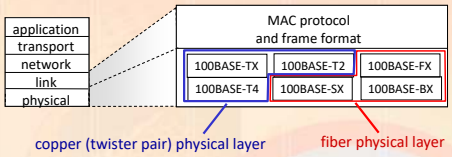
- addresses: 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g., ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- type: indicates higher layer protocol
  - mostly IP (0800 hex) but others possible, e.g., Novell IPX, AppleTalk
  - used to demultiplex up at receiver
- CRC: 32-bit cyclic redundancy check at receiver
  - error detected: frame is dropped

Ethernet: Unreliable, Connectionless

- connectionless: no handshaking between sending and receiving NICs
- unreliable: receiving NIC doesn't send ACKs or NAKs to sending NIC
  - data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: unslotted CSMA/CD with binary backoff

IEEE 802.3 - Ethernet Link & Physical layers

- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 2 Mbps, ... 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps, 80 Gbps
    - different physical layer media: fiber, cable



Outline

- Introduction
- Multiple Access protocols
- **LANs**
  - addressing and ARP
  - Ethernet
  - **Switches**
  - VLANs
- Link Virtualization: MPLS
- Data Centre networking

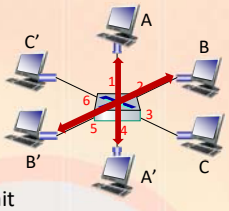
Ethernet Switch

- Switch is a link-layer device: takes an *active* role
  - store, forward Ethernet (or other type of) frames
  - examine incoming frame's MAC address, *selectively* forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent: hosts *unaware* of presence of switches
- plug-and-play, self-learning
  - switches do not need to be configured
- Classified as:
  - Non-Manageable: cheap, basic features
  - Manageable: more expensive, support VLAN, STP, PoE, modular, etc..
  - Port Speed: Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1000Mbps, etc…
  - Store-N-Forward or Cut-through Modes
  - Number of ports: 8,16, 32, 64, etc…
  - Port media type: Twisted Pair, Fiber optics, etc…

Ethernet Switch

Switch: multiple simultaneous transmissions

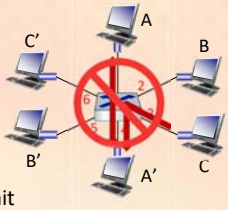
- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions



switch with six interfaces (1,2,3,4,5,6)

Switch: Multiple Simultaneous transmission

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain
- switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions
  - but A-to-A' and C to A' can *not* happen simultaneously



switch with six interfaces (1,2,3,4,5,6)

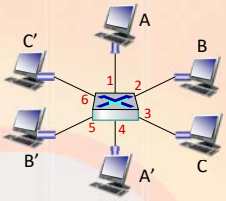
Switch Forwarding Table

All switches, once powered up maintain a Forwarding Table in temporary memory (RAM). The Forwarding table is also knows as MAC table or CAM table

Q: how does switch know A' reachable via interface 4, B' reachable via interface 5?

A: each switch has a Forwarding table, each entry contains:

- (MAC address of host, interface to reach host, time stamp)
- looks like a routing table!



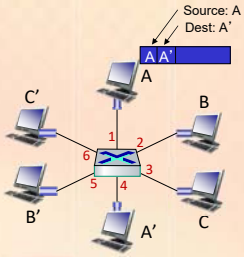
Q: how are entries created, maintained in switch table?

- something like a routing protocol?

Switch: Transparent, Self-learning

Slide Set 2

- switch *learns* which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender: incoming LAN segment
  - records sender/location pair in switch table



MAC addr	interface	TTL
A	*1*	*60*

Switch table (initially empty)

Switch: Frame buffering and forwarding

Slide Set 2

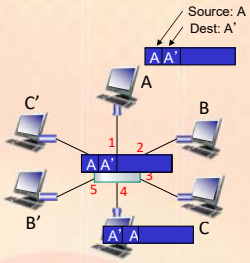
when a frame received at a switch port interface:

1. record incoming port interface, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination
   then {
   if destination on segment from which frame arrived
   then drop frame
   else forward frame on interface indicated by entry
   }
   else flood /* forward on all interfaces except arriving interface */

Self-Learning: Forwarding Example

Slide Set 2

- frame destination, A', location unknown: flood
- destination A location known: selectively send on just one link



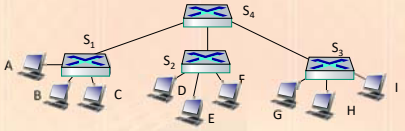
MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

Interconnecting Switches

Slide Set 2

self-learning switches can be connected together:

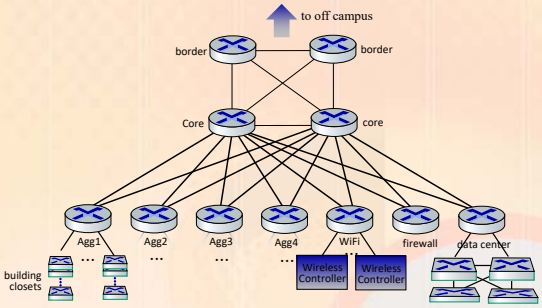


Q: sending from A to G - how does S_1 know to forward frame destined to G via S_4 and S_3?

- A: self learning! (works exactly the same as in single-switch case!)

UMass Campus Network

Slide Set 2



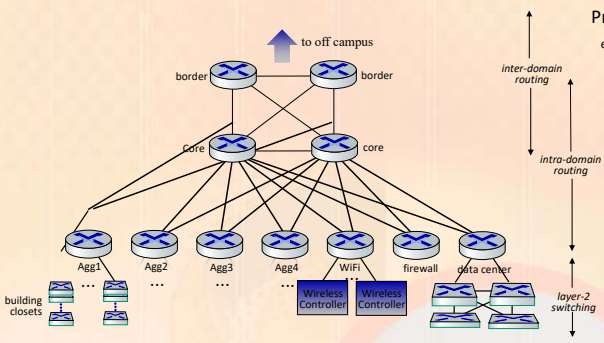
UMass network:

- 4 firewalls
- 10 routers
- 2000+ network switches
- 6000 wireless access points
- 30000 active wired network jacks
- 55000 active end-user wireless devices

… all built, operated, maintained by ~15 people

UMass Campus Network

Slide Set 2



Protocols	Link Speeds
eBGP	10G; 100G pending
iBGP IS-IS	40G & 100G
IS-IS	40G
Ethernet	10G & 1G

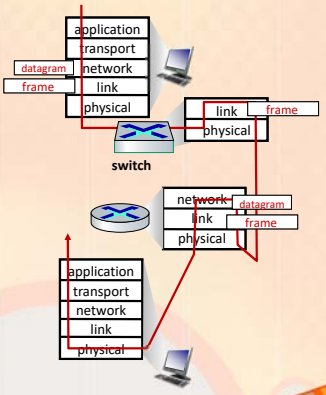
Switches vs. Routers

both are store-and-forward:

- *routers*: network-layer devices (examine network-layer headers)
- *switches:* link-layer devices (examine link-layer headers)

both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses

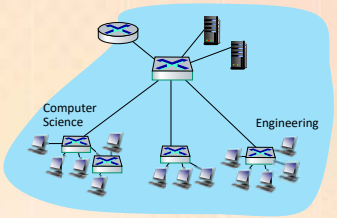


Outline

- Introduction
- Multiple Access protocols
- **LANs**
  - addressing and ARP
  - Ethernet
  - Switches
  - **VLANs**
- Link Virtualization: MPLS
- Data Centre networking

Virtual LANs (VLANs): Motivation

Q: what happens as LAN sizes scale, users change point of attachment?

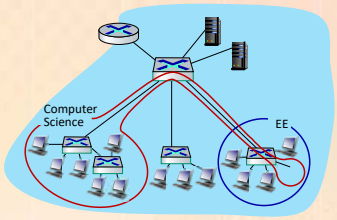


single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy issues

Virtual LANs (VLANs): Motivation

Q: what happens as LAN sizes scale, users change point of attachment?



single broadcast domain:

- *scaling:* all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy, efficiency issues

administrative issues:

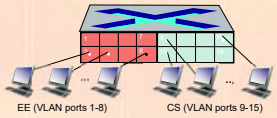
- CS user moves office to EE - *physically* attached to EE switch, but wants to remain *logically* attached to CS switch

Port-based VLANs

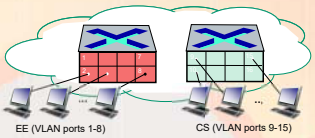
Virtual Local Area Network (VLAN)

switch(es) supporting VLAN capabilities can be configured to define multiple *virtual* LANS over single physical LAN infrastructure.

port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



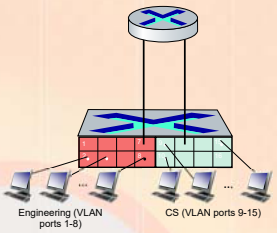
… operates as multiple virtual switches



Port-based VLANs

Port-based VLANs

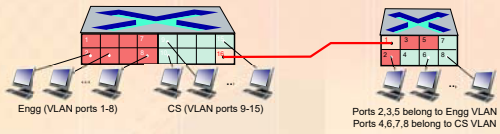
- traffic isolation: frames to/from ports 1-8 can *only* reach ports 1-8
  - can also define VLAN based on MAC addresses of endpoints, rather than switch port
- dynamic membership: ports can be dynamically assigned among VLANs
- forwarding between VLANS: done via routing (just as with separate switches)
  - in practice vendors sell combined switches plus routers



VLANs spanning multiple switches

Slide Set 2

VLANS spanning multiple switches



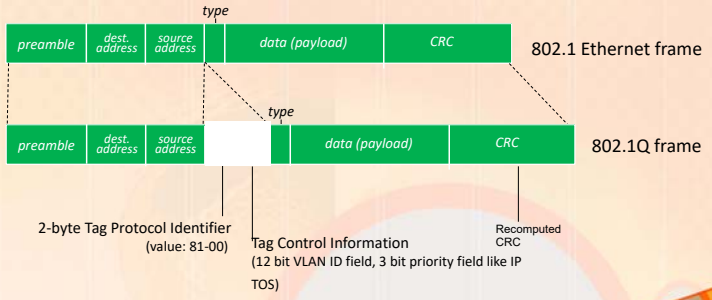
trunk port: carries frames between VLANS defined over multiple physical switches

- frames forwarded within VLAN between switches can't be vanilla 802.1 frames (must carry VLAN ID info)
- 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports

55

802.1Q VLAN frame format

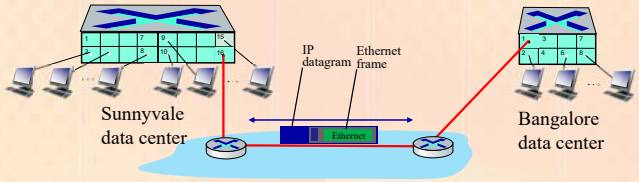
Slide Set 2



56

EVPN: Ethernet VPNs aka VXLANs

Slide Set 2



Layer-2 Ethernet switches *logically* connected to each other (e.g., using IP as an *underlay*)

- Ethernet frames carried *within* IP datagrams between sites
- "*tunneling* scheme to *overlay Layer 2 networks on top of Layer 3 networks* … runs over the existing networking infrastructure and provides a means to "stretch" a Layer 2 network." [RFC 7348]

57

Outline

Slide Set 2

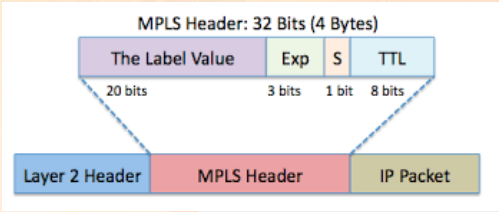
- Introduction
- Multiple Access protocols
- LANs
  - addressing and ARP
  - Ethernet
  - Switches
  - VLANs
- **Link Virtualization: MPLS**
- Data Centre networking

58

MultiProtocol Label Switching (MPLS)

Slide Set 2

- goal: high-speed IP forwarding among network of MPLS-capable routers, using fixed length label (instead of shortest prefix matching)
  - faster lookup using fixed length identifier
  - borrowing ideas from Virtual Circuit (VC) approach
  - but IP datagram still keeps IP address!



59

MPLS capable routers

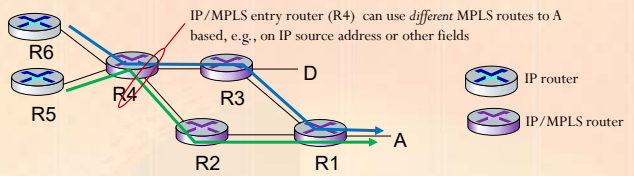
Slide Set 2

- a.k.a. label-switched router
- forward packets to outgoing interface based only on label value (*don't inspect IP address*)
  - MPLS forwarding table distinct from IP forwarding tables
- *flexibility:* MPLS forwarding decisions can *differ* from those of IP
  - use destination *and* source addresses to route flows to same destination differently (traffic engineering)
  - re-route flows quickly if link fails: pre-computed backup paths

60

MPLS versus IP paths

Slide Set 2

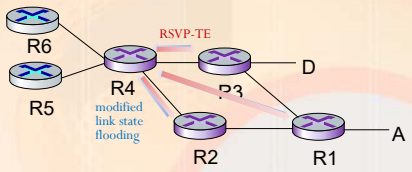


- IP routing: path to destination determined by destination address alone
- MPLS routing: path to destination can be based on source *and* destination address
  - flavor of generalized forwarding (MPLS 10 years earlier)
  - *fast reroute:* precompute backup routes in case of link failure

MPLS Signalling

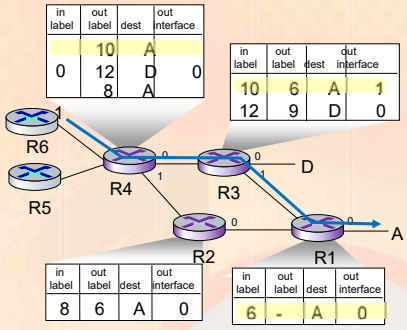
Slide Set 2

- modify OSPF, IS-IS link-state flooding protocols to carry info used by MPLS routing:
  - e.g., link bandwidth, amount of "reserved" link bandwidth
- entry MPLS router uses RSVP-TE signaling protocol to set up MPLS forwarding at downstream routers



MPLS forwarding tables

Slide Set 2



in label	out label	dest	out interface
	10	A	
0	12	D	0
	8	A	

in label	out label	dest	out interface
10	6	A	1
12	9	D	0

in label	out label	dest	out interface
8	6	A	0

in label	out label	dest	out interface
6	-	A	0

Outline

Slide Set 2

- Introduction
- Multiple Access protocols
- LANs
  - addressing and ARP
  - Ethernet
  - Switches
  - VLANs
- Link Virtualization: MPLS
- **Data Centre networking**

Datacentre Networks

Slide Set 2

10's to 100's of thousands of hosts, often closely coupled, in close proximity:

- e-business (e.g. Amazon)
- content-servers (e.g., YouTube, Akamai, Apple, Microsoft)
- search engines, data mining (e.g., Google)

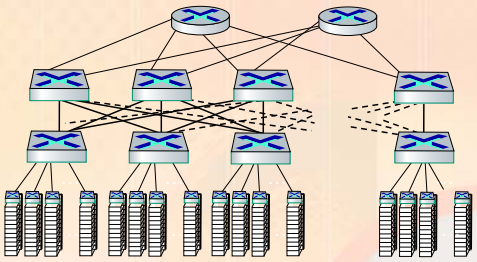
challenges:

- multiple applications, each serving massive numbers of clients
- reliability
- managing/balancing load, avoiding processing, networking, data bottlenecks

Inside a 40-ft Microsoft container, Chicago data center

Datacentre Networks: Network elements

Slide Set 2



Border routers
- connections outside datacenter

Tier-1 switches
- connecting to ~16 T-2s below

Tier-2 switches
- connecting to ~16 TORs below

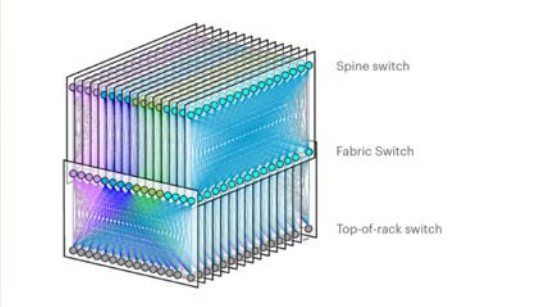
Top of Rack (TOR) switch
- one per rack
- 100G-400G Ethernet to blades

Server racks
- 20- 40 server blades: hosts

Datacentre Networks: Network Elements

Slide Set 2

Facebook F16 data center network topology:

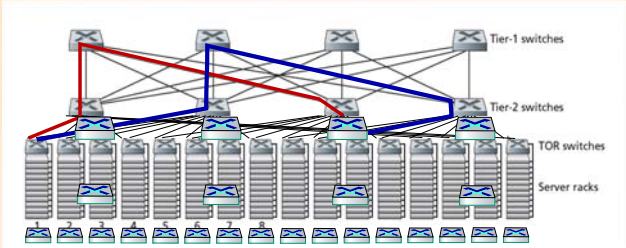


https://engineering.fb.com/data-center-engineering/f16-minipack/ (posted 3/2019)

Datacentre Networks: Multipath

Slide Set 2

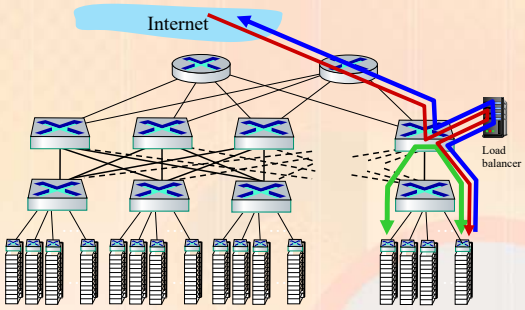
- rich interconnection among switches, racks:
  - increased throughput between racks (multiple routing paths possible)
  - increased reliability via redundancy



two disjoint paths highlighted between racks 1 and 11

Application-layer Routing

Slide Set 2



load balancer: application-layer routing

- receives external client requests
- directs workload within data center
- returns results to external client (hiding data center internals from client)

Datacentre Networks: Protocol Innovations

Slide Set 2

link layer:

RoCE: remote DMA (RDMA) over Converged Ethernet

transport layer:

ECN (explicit congestion notification) used in transport-layer congestion control (DCTCP, DCQCN)

experimentation with hop-by-hop (backpressure) congestion control

routing, management:

SDN widely used within/among organizations' datacenters

place related services, data as close as possible (e.g., in same rack or nearby rack) to minimize tier-2, tier-1 communication

Google Networking: Infrastructure and Selected Challenges (Slides: https://networkingchannel.eu/google-networking-infrastructure-and-selected-challenges/

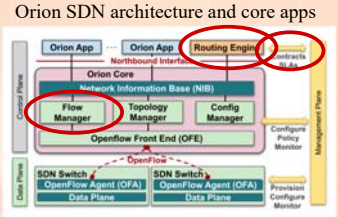
Datacentre Networks: Google SDN

Slide Set 2

ORION: Google's new SDN control plane for internal datacenter (Jupiter) + wide area (B4) network

- routing (intradomain, iBGP), traffic engineering: implemented in *applications* on top of ORION core
- edge-edge flow-based controls (e.g., CoFlow scheduling) to meet contract SLAs
- management: pub-sub distributed microservices in Orion core, OpenFlow for switch signaling/monitoring

Orion SDN architecture and core apps



Note:

- no routing protocols, congestion control (partially) also managed by SDN rather than by protocol
- are protocols dying?

Network Security

Slide Set 4

What is this Slideset about?

This chapter is to address

- security needs
- security services
- security mechanisms and protocols

for data stored in computers (computer security) and transmitted across computer networks (network security)

What security is about in general?

- Security is about protection of assets
- Prevention
  - take measures to prevent assets from being tampered or stolen
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been tampered
- Reaction
  - take measures to recover assets

Real-world examples

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard, …
- Detection
  - missing items, burglar alarms, CCTV, …
- Reaction
  - attack on burglar, call the police, replace/backup stolen asset, make an insurance claim, …

Internet shopping example

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, don't send card number via Internet use payment wallets instead.
- Detection
  - an unauthorized transaction appears on your credit card statement or wallet.
- Reaction
  - complain, dispute, ask for a new card, sue
  - Or, pay and forget

Information security: Past & Present

- Traditional Information Security
  - keep the cabinets locked
  - put them in a secure room
  - human guards
  - electronic surveillance systems
  - Physical and Administrative mechanisms
- Modern World
  - Data is found inside computers in digital format
  - Computers are interconnected
  - **Hence computer and network security both required**

Some Terminologies

- Computer Security
  - automated tools and mechanisms to protect data **in** a computer, even if the computers are connected to a network e.g.
    - against hackers (intrusion detection systems)
    - against malware
- Network Security
  - measures to prevent, detect, and correct security violations that involve the **transmission** of information in a network

Services, Mechanisms, Attacks

- 3 aspects of information security:
  - security attacks (and threats)
    - actions that compromise security of assets
  - security services
    - services counter to attacks
  - security mechanisms
    - used by services
    - E.g. Confidentiality is a service, Encryption is the mechanism.

Attacks

- Attacks on computer systems
  - break-in to destroy or tamper information
  - break-in to steal information
  - blocking to operate properly
  - malicious software (malware)
    - wide spectrum of problems (more later)

Attacks

- Network Security Attacks
  - **Passive** and **Active**
- Passive attacks
  - intercept messages by *sniffing* or *snooping*.
  - What can the attacker do?
    - use information personally ("fetish")
    - release the content ("gossip")
    - traffic analysis ("spying")
  - Hard to detect, try to prevent… How?

Attacks

- Active attacks involves interruption, withholding, modification, fabrication, deletion of messages.
  - Masquerade/Spoofing (attack on authentication)
    - pretend to be someone else to perform an illegitimate action
  - Insertion/Fabrication (attack on integrity and/or authentication)
    - create a bogus message usually via spoofing
  - Replay (attack on authentication and/or integrity and/or availability)
    - passively capture data and send later

Attacks

- Active attacks
  - Deny (attack on non-repudiation)
    - Refuse to acknowledge sending/receiving a message
  - Modification (attack on integrity)
    - change the content of a message
  - Denial-Of-Service (attack on availability)
    - prevention the normal use of servers, end users, or network itself

Security Services

- to detect and/or deter attacks
- to enhance security
- replicate functions of physical documents
  - have signatures, dates, seals, watermark
  - protection from disclosure, tampering, or destruction
  - notarize
  - record

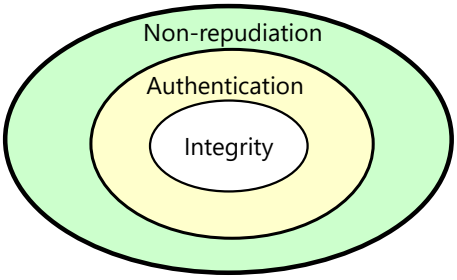
ISO 7498-2 Security Services

- Authentication
  - Assurance of the identity of the communicating entity
    - peer-entity authentication
      - mutual confidence in the identities of the parties involved in a connection
    - data-origin authentication
      - assurance about the source of the received data
- Confidentiality
  - protection of data from unauthorized disclosure

ISO 7498-2 Security Services

- Data Integrity
  - assurance that data received is exactly the same at the time sent by an authorized sender
  - i.e. no modification, insertion, or replay
- Non-Repudiation
  - protection against denial by one of the parties in a communication
  - Origin non-repudiation
    - proof that the message was sent by the specified party
  - Destination non-repudiation
    - proof that the message was received by the specified party

Relationships



Security Mechanisms

- Basically cryptographic techniques/technologies
  - that serve to secure services
  - to prevent/detect/recover attacks
- Encipherment (Encryption)
  - use of mathematical algorithms to transform data into a form that is not readily intelligible using ciphers
    - keys are involved

Security Mechanisms

- Message Digest
  - similar to encryption, but one-way (recovery not possible)
  - generally no keys are used
- Digital Signature & Message Authentication Code
  - Addition or Cryptographic transformation of a data unit to prove the source and the integrity of the data
- Authentication Exchange
  - ensure the identity of an entity by exchanging some information

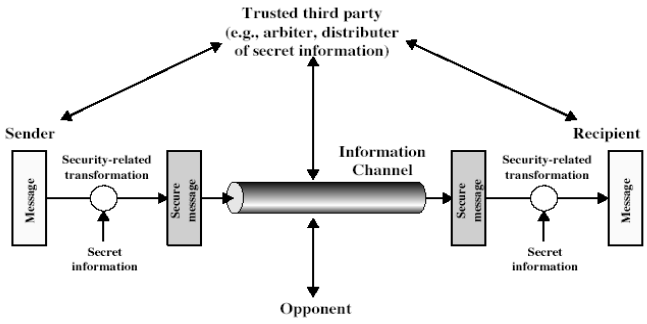
Security Mechanisms

- Notarization
  - use of a trusted third party to assure certain properties of a data exchange
- Time-stamping
  - inclusion of correct date and time within messages
- Non-cryptographic mechanisms
  - traffic padding (for traffic confidentiality)
  - Intrusion Detection Systems
  - Firewalls, Honeynet, Honeypot

Two Security references

- ITU-T X.800 Security Architecture for OSI
  - gives a systematic way of defining and providing security requirements
- RFC 2828
  - over 200 pages glossary on Internet Security

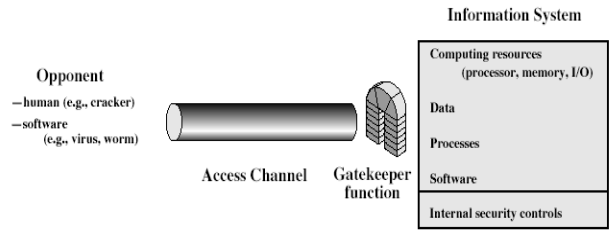
Model for Network Security



Model for Network Security

- This model requires the
  - design a suitable algorithm for the security transformation
  - generation the secret information (keys) used by the algorithm
  - Development of methods to distribute and share the secret information reliably
  - specify a protocol enabling the principals to use the transformation and secret information for a security service.

Model for Network Access Security



Model for Network Access Security

- This model requires the
  - Selection of appropriate gatekeeper functions to identify users and ensure only authorized users access designated information or resources
    - e.g. what you know, what you have, who you are
    - aka 3 Factor authentication
  - Internal control to monitor the activity and analyze information to detect intrusion.

More on Computer System Security

- Based on security policies
  - Set of rules that specify
    - How resources are managed to satisfy the security requirements
    - Which actions are permitted, which are not
  - Ultimate aim
    - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
  - Scope
    - Organizational or Individual
  - Implementation
    - Partially automated, but mostly humans are involved

Aspects of Computer Security

- Mostly related to Operating Systems
- Similar to those discussed for Network Security
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Dependability

Aspects of Computer Security

- Confidentiality
  - Prevent unauthorised disclosure of information
  - Synonyms: Privacy and Secrecy
    - any differences? Let's discuss
- Integrity
  - In general, "make sure that everything is as it is supposed to be"
  - Specifically, "no unauthorized modification or deletion"
- Availability
  - services should be accessible when needed and without delay

Aspects of Computer Security

- Accountability
  - audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party
  - How can we do that?
    - Users have to be **identified** and **authenticated** to have a basis for access control decisions and to find out responsible party in case of a violation.
    - The security system keeps an **audit log (audit trail)** of security relevant events to detect and investigate intrusions.
- Dependability
  - Can we trust the system as a whole?

Fundamental Tradeoff

- Between security and ease-of-use
- Security may require clumsy and inconvenient restrictions on users and processes

"If security is an add-on that people have to do something special to get, then most of the time they will not get it"

Martin Hellman,
co-inventor of Public Key Cryptography

Designing a successful product

- User-transparent
- Do not assume potential users to be security experts
  - but provide enough set of options for security experts
- a security feature in a product is a plus, but a security product is a challenge in the market
  - people intend to pay for secure products, but not to pay security products
- Homework: Prove or disprove the last bullet by making a search in the Internet.

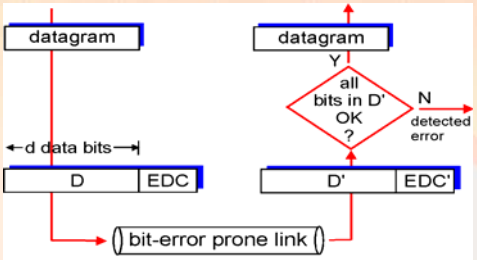
Error Control: Detection and Correction

Slide Set 5

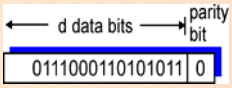
Error Detection

EDC = Error Detection and Correction bits (redundancy)
D = Data protected by error checking, may include header fields

- **Error detection not 100% reliable!**
  - **protocol may miss some errors, but rarely**
  - **larger EDC field yields better detection and correction**



Single Bit Parity Checking (Detect Only)



This is an example of odd parity: The parity bit is chosen (0) in such a way that the total number of 1s is odd (9)

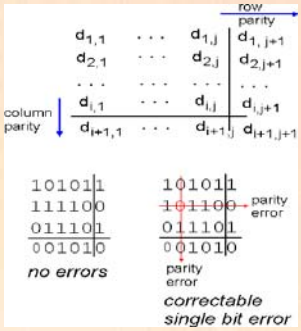
IMPORTANT
A single bit parity check will only be able to detect 1 or and odd number of bits in error.

Even Parity Scheme:
Parity bit chosen so that total number of 1s including the parity bit is **EVEN.**

Odd Parity Scheme:
Parity bit chosen so that total number of 1s including the parity bit is **ODD**.

It is highly efficient since a single parity bit is needed for any length of data bits (Message M).

2-D Bit Parity Checking (Detect & Correct)



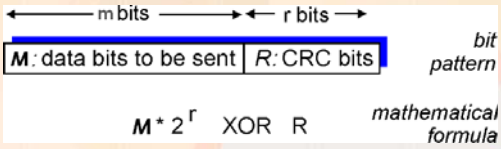
This is an example of even parity: The parity bits are chosen in such a way that the total number of 1s is either a column or row is even

In this technique, the data bits are rearranged in an nxm matrix. Ideally a square matrix for higher efficiency. The parity bit is chosen for each row and column in the matrix. An additional parity bits can be used for checking the parity bits themselves but this is optional.

IMPORTANT
A 2-D bit parity check will only be able to detect 1 or and odd number of bits in error in either a column or a row but can also correct single bit errors if they occur in different rows and columns.

Cyclic Redundancy Check (Detect Only)

- view Message bits, M, as a binary number
- choose r+1 bit pattern divisor (generator), G
- goal: choose r CRC bits, R, such that
  - <M,R> exactly divisible by G (modulo 2)
  - receiver knows G, divides <M,R> by G. If non-zero remainder occurs: error detected!



Example of CRC in an Ethernet frame

CRC appends **redundant** bits to the frame trailer called Frame Check Sequence (FCS)

The FCS bits are used at Receiver for error detection

In a given frame containing a total of n bits, we define:

k = the number of original data bits (Message M)

(n – k) = the number of added bits as the FCS field or Code Bits (CB)

So, the total frame length is k + (n – k) = n bits or Code Word (CW)

	M (k)	CB (n-k)
CW(n)	1 0 1 0 0 0 1 1 0 1	01110

CRC Generation

CRC generation at the sender is all about finding the FCS, given the data (M) and a divisor (G) that makes CW exactly divisible by G (i.e. with 0 remainder)

	M (k)	FCS or CB (n-k)
CW (n)	1 0 1 0 0 0 1 1 0 1	0 1 1 1 0

110101 G (n-k+1)

There are three equivalent ways to see how the CRC code is generated:

Modulo-2 Arithmetic Method

Polynomial Method (not covered)

Digital Logic Method (not covered)

What is F that makes T divide P exactly? i.e. with no remainder

Modulo-2 Arithmetic

- *In modulo 2 arithmetic addition and substruction are identical to EXCLUSUVE OR (XOR) operation.*
- *Multiplication and division are the same as in base-2 arithmetic without carries in addition or borrows in substraction.*

0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

Examples:

1011 XOR 0101 = 1110

1001 XOR 1101 = 0100

CRC Error Detection Process

Given k-bit data (M), the Sender generates an (n – k)-bit FCS field (CB) such that the *total* n-bit frame (CW) is exactly divisible by a predefined (n-k+1) bit divisor (G) (i.e. gives a zero remainder)

In general, the received frame (CW') may or may not be identical to the sent frame (CW).

Let the received frame be (CW')

Only in error-free transmissions that we have CW' = CW

Receiver divides (CW') by the same known divisor (G) and checks if there is any remainder, if division yields a remainder then the frame is erroneous

If the division yields zero remainder then the frame is error-free unless many erroneous bits in CW' resulted in a new exact division by G.

This is extremely unlikely but possible, causing an undetected error!

Example – Modulo-2 Arithmetic Method

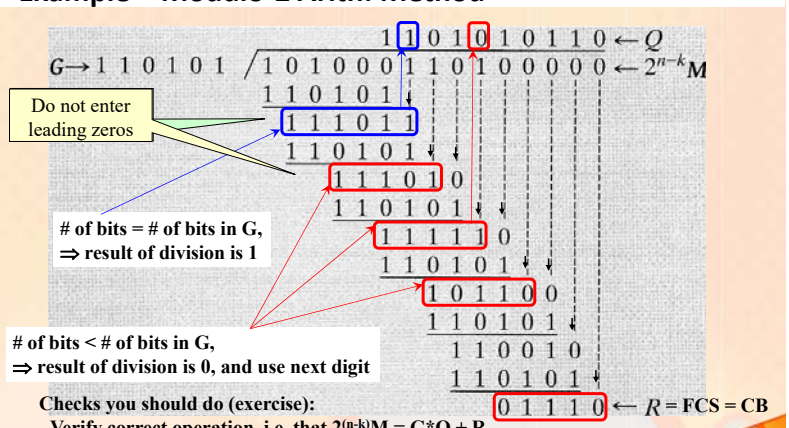
- Given
  - M = 1 0 1 0 0 0 1 1 0 1 At the Sender (source) side
  - G = 1 1 0 1 0 1 (i.e. $x^5+x^4+x^2+1$)
- Find the FCS field
- Solution:
  - First we note that:
    - The size of the data block M is k = 10 bits
    - The size of G is (n – k + 1) = 6 bits
      - Hence the FCS length is n – k = 5
      - Total size of the frame CW is n = 15 bits

Example – Modulo-2 Arithmetic Method

- Solution (continued):
  - Multiply $2^{(n-k)}$ x M
    - $2^{(5)}$ x 1 0 1 0 0 0 1 1 0 1 = 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0
    - This is a simple shift to the left by five positions and inserting (n-k) zeroes.
  - Divide $2^{(n-k)}$ x M / G (see next slide for details)
    - 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 ÷ 1 1 0 1 0 1 yields:
      - **Quotient Q = 1 1 0 1 0 1 0 1 1 0**
      - **Remainder R = 0 1 1 1 0**
  - So, FCS = R = 0 1 1 1 0: Append it to M to get the full frame CW to be transmitted
  - CW = 1 0 1 0 0 0 1 1 0 1 0 1 1 1 0

M FCS

Example – Modulo-2 Arith. Method



Checks you should do (exercise):

- Verify correct operation, i.e. that $2^{(n-k)}$M = G*Q + R

- Verify that the obtained CW(1010001101 01110) divides G (110101) exactly (i.e. with zero remainder)

Example – Modulo-2 Arith. Method

For G = 110011 & M = 11100011, find the CRC

```
                10110110
110011/1110001100000
       110011
         101111
         110011
          111000
          110011
            101100
            110011
             111110
             110011
CRC =          11010
```

CW to transmit is? Answer: 11100011 11010

Hamming Code (Detect & Correct)

Hamming Code is an error control technique where the redundant bits (CB) are spread at strategic position within the message bits (M).

- The position of these redundant bits are always at position 2^n (where n =0,1,2,3,...) i.e. position 1,2,4,8,...
- The number of redundant bits needed depends on the number of bits in the message (M).
- It is usually expressed as a function ***H(CW,M)*** e.g **H(11,7)** i.e. 7 message bits and 4 Code Bits (CB) yielding an 11-bit Codeword (CW)

Hamming Code: Code Bits Generation

At the SENDER:

Suppose M = 101000001 (9 bits)

The following equation should hold $2^{CB} \geq M+CB+1$

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	0	?	0	0	0	?	1	?	?

We reserve **4 boxes**: 1,2,4 and 8 for the code bits (CB), and insert the message bits (M) in the remaining boxes. There should be 9+4 = 13 boxes in all which represents the 13 bits in the codeword (CW).

- To obtain the values of the code bits (the 4 boxes with interrogation marks), we perform a **modulo-2 addition** of all the box positions containing a '1' bit.
- In modulo-2 addition, we count the number of '1's in each column respectively. If the number of '1's is even, the addition yield 0 else if the number of '1's is odd, the addition yields 1.

Hamming Code: Code Bits Generation

Modulo-2 addition yields:

```
13:  1101
11:  1011
3 :  0011
     0101   = Code Bits
```

These become the code bits and are substituted back in the interrogation mark boxes. The transmitted codeword therefore becomes:

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	0	0	0	0	0	1	1	0	1

Hamming Code: Error Checking

At the RECEIVER:

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	0	0	0	0	0	1	1	0	1

A modulo-2 addition is performed on the received codeword with all the box positions containing a '1':

```
13:  1101
11:  1011
 4:  0100
 3:  0011
 1:  0001
     0000   Since addition is 0, it implies that no errors have taken place.
```


Hamming Code: Error Correction

Assume that at the RECEIVER, bit number 11 is in error:

13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	0	0	0	0	0	0	0	1	1	0	1

A modulo-2 addition is performed on the received codeword with all the box positions containing a '1':

```
13:  1101
 4:  0100
 3:  0011
 1:  0001
     1011
```

Since addition is NOT 0, it implies that a error has taken place. The bit position in error is given by the result of the addition **i.e. 1011 = 11th bit.** So to correct, we simply invert the bit value.

Hamming Code

- It is always assumed that the code bits are not corrupted during transmission.
- Hamming code can only detect and correct **1 bit** in error in the message M.
- The efficiency of Hamming Code increases as the number of bits in the message becomes larger.

Summary

- Single parity bit checking can **only detect** one or an odd number of bits in error in the message M. It has the highest efficiency as it needs only one code bit irrespective of the length of the message M.
- 2-Dimensional parity bit checking can **detect and correct** one or more errors as long as one or an odd number of bits in error occur in different rows and/or columns.
- CRC can **only detect** any number of bits in error in the message M. The number of code bits needed is always one bit less than the divisor irrespective of the length of the message M.
- Hamming code can **detect and correct** a single bit in error in the message M. The number of code bits needed increases with the length of the message M.

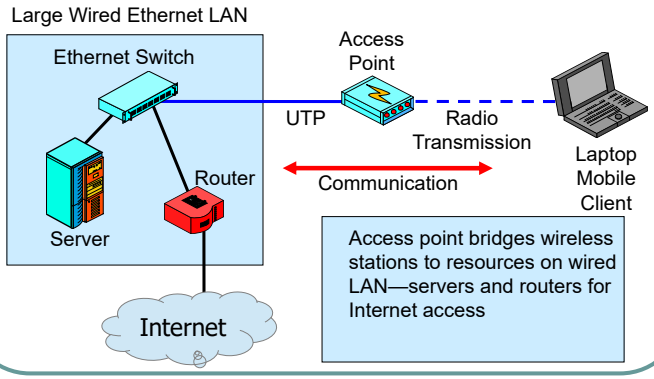
Wireless LANs

Slide Set 6

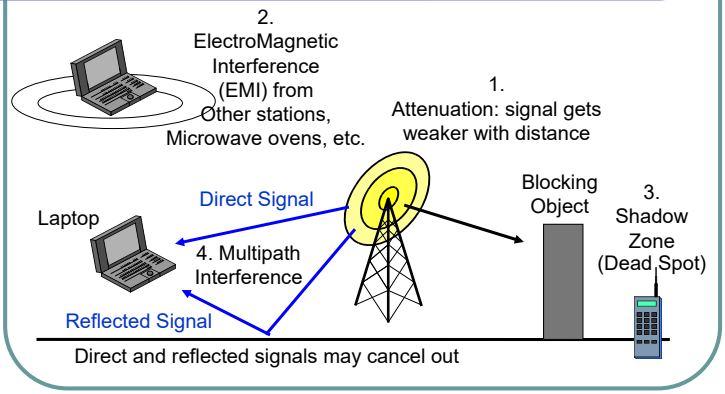
Wireless LANs

- The Big Thing in local area networking today
- Gives mobility to users within the corporate premises
- Not a competitor for the main wired Ethernet LAN today; extends the wired LAN's resources to mobile users

Wireless LAN (WLAN) Access Point



Wireless Propagation Problems

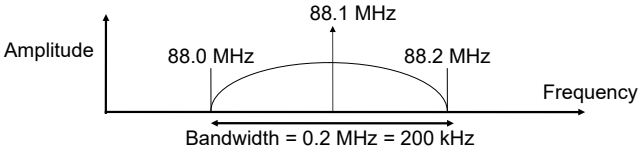


Wireless Propagation Problems

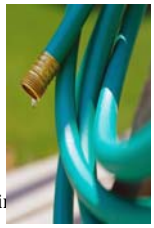
- Some problems are Frequency-Dependent
  - Higher-frequency signals attenuate faster
    - Absorbed more rapidly by moisture in the air
  - Higher-frequency signals blocked more by obstacles
    - At lower frequencies, signal refract (bend) around obstacles like an ocean wave hitting a buoy
    - At higher frequencies, signals do not refract; leave a complete shadow behind obstacles

Channel Bandwidth

- Channel Bandwidth
  - Eg. A FM radio channel centred at 88.1MHz has a bandwidth of 0.2 MHz (200 kHz) i.e. from 88.0 to 88.2 MHz.
  - Higher-speed signals need wider bandwidths (e.g. TV channels need at least 4 MHz)



Transmission Speed – Capacity Theorem

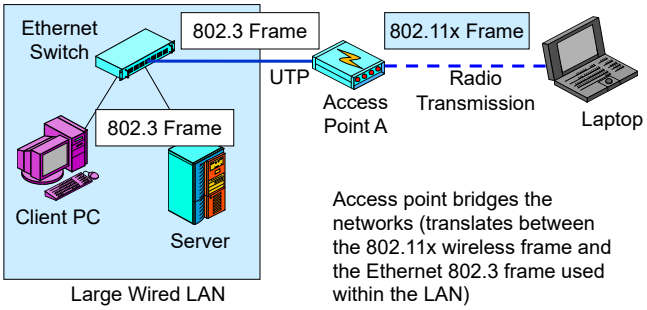


- Shannon Capacity Theorem
  - $C = B * \log_2 (1+S/N)$
    - C = capacity i.e. maximum possible transmission speed in the channel (bps)
    - B = Bandwidth (Hz) (Like thickness of a hose)
    - S/N = Signal-to-Noise power
  - Note that doubling the bandwidth (B) doubles the maxi transmission speed
  - More generally, increasing the bandwidth by X increases the maximum possible speed by X
  - Increasing S/N helps slightly but usually cannot be done to any significant extent

The Golden Zone

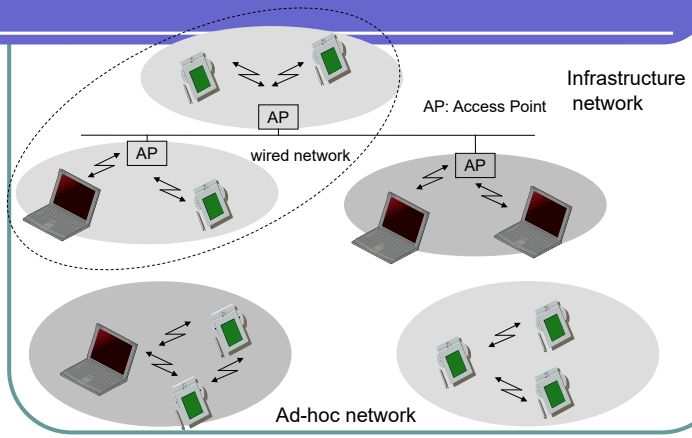
- The Golden Zone
  - Most organizational radio technologies operate in the "golden zone"
  - High megahertz to low gigahertz range
  - At higher frequencies, there is more available bandwidth
  - At lower frequencies, signals propagate better.
  - Frequencies should be high enough for there to be large total bandwidth
  - Frequencies should be low enough to allow fairly good propagation characteristics.

Typical 802.11x Wireless LAN Operation with Access Points

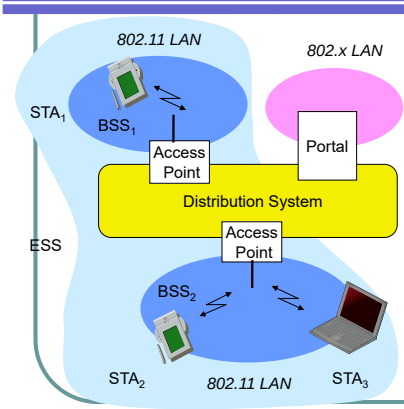


Access point bridges the networks (translates between the 802.11x wireless frame and the Ethernet 802.3 frame used within the LAN)

Infrastructure Mode vs. Ad-hoc Mode



Architecture of an infrastructure network



Station (STA)
- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)
- group of stations using the same radio frequency

Access Point (AP)
- station integrated into the wireless LAN and the distribution system

Portal
- bridge to other (wired) networks

Distribution System
- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

802.11x Wireless Access Point and Wireless LAN Adapters (PCMCIA, PCI & USB)

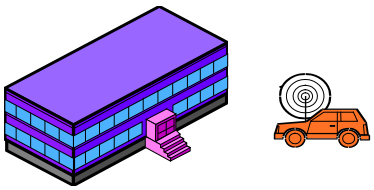
802.11x Wireless LAN Standards

<---- Obsolete ----->

IEEE Standard	802.11b WiFi 1	802.11a WiFi 2	802.11g WiFi 3	802.11n WiFi 4	802.11ac WiFi 5	802.11ax WiFi 6	802.11be WiFi 7
Adoption Year	1999	1999	2003	2009	2014	2019	2024
Frequency	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz	2.4/5/6 GHz
Max Data Rate	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.9 Gbps	9.6 Gbps	46.1 Gbps
Typical indoor range	35m	30m	35m	70m	35m	30m	30m

802.11x Security

- Automated Drive-By Hacking (War Driving)
  - Can read traffic from outside the corporate walls
  - Can also send malicious traffic into the network



802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Initial flawed security method developed by the 802.11 Working Group for 802.11 devices
  - All stations share the same encryption key with the access point
  - This key is cannot be changed
  - This is a shared static key

802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Shared static keys means that a large volume of traffic is encrypted with the same key
  - With so much traffic generated with one unchanging key, cryptanalysts (code-breakers) can crack the key by collecting data for a few days
  - Once the key is cracked, the attacker can read all messages and send attack messages into the network without going through a firewall filter
  - Software that automates the hacking process is widely available e.g. AirSnort
    - Locate vulnerable access points by driving around (war driving)
    - Collect traffic and crack the key
    - **No longer recommended to use WEP nowadays**

802.11 Security, Continued

- Because of the security issues around WEP, the Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) in 2003. Shortly afterward in 2004, they released WPA2 and in 2018 they released WPA3.

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

802.11 Security, Continued

- Wireless Protected Access (WPA)
  - Stopgap security method introduced before full 802.11i security could be developed
  - It was often possible to upgrade older WEP products to WPA because the underlying hardware was the same as WEP.
  - It uses Temporal Key Integrity Protocol (TKIP). It addressed the two flaws present in WEP by using MIC instead of CRC-32 and increasing the IV of RC4 from 40 bits to 48 bits.

802.11 Security, Continued

- Wireless Protected Access 2 and 3
  - In WPA2, encryption and integrity check are performed within single logical block – CCM and both are based on AES.
  - In WPA3, both encryption and data integrity are enhanced even further from WPA2. The only downside is that more processing power is required. Not many wireless devices support WPA3 yet.

802.11 Security, Continued

- Ways to strengthen your Wireless LAN
  - Do not use WEP. Use WPA, WPA2 or WPA3 instead
  - Enforce MAC address Association (i.e only allowed wireless adapters can join your wireless network)
  - Disable BSSID broadcast once all permitted stations have been allowed to join the wireless network.
  - Enable Access Point firewall features to prevent potential attacks.

UNIVERSITY TECHNOLOGY MAURITIUS

BSc (Hons) Business Information Systems

BSc (Hons) Software Engineering

BSc (Hons) Computer Science with Network Security

BEng (Hons) Telecommunications

BIS/09/FT – BSE/09/FT - BCNS/09/FT - BCNS/09/FT - BTEL/09/FT

Examinations for 2009 - 2010 / Semester 2

MODULE: NETWORKS

MODULE CODE: CAN1102

DURATION: 2 HOURS

READING TIME: None

Instructions to Candidates

1. Answer **Section A and any 2 questions from Section B**
2. Always start a new question on a fresh page for **Section B**.
3. Total marks: **100**
4. Use of silent calculators is allowed in the Examination Room.
5. Appendix provided

This questionnaire contains 4 Questions and consists of 8 pages.

SECTION A: COMPULSORY

Question 1 (50 Marks)

The following 25 multiple-choice questions contain only **one** correct answer. You do not need to copy the questions, write your response legibly i.e. (a), (b), (c) or (d) on your script in five columns **with** the respective question number.

1. Drop cables are used in _____ topology?
(a) Star
(b) Bus
(c) Mesh
(d) None of the above

2. Which topology requires a multipoint connection?
(a) Star
(b) Bus
(c) Ring
(d) None of the above

3. What is the central device in a star topology?
(a) STP Server
(b) Hub/Switch
(c) Router
(d) Bridge

4. Which one is NOT a characteristic of a Local Area Network?
(a) It is usually private-owned
(b) It usually spans over a hundred meters
(c) It usually has low bandwidth
(d) It is fairly easy to manage

5. Which one is an example of unguided medium?
(a) Shielded Twisted Pair Cable
(b) Coaxial Cable
(c) Fibre Optic Cable
(d) None of the above

6. What does SMTP stand for?
(a) Special Message Transfer Protocol
(b) Simple Mail Transportation Protocol
(c) Sample Mail Transfer Protocol
(d) Simple Mail Transfer Protocol

7. Which control signal is NOT involved during connection tear-down?
(a) SYN
(b) ACK
(c) FIN
(d) None of the above

8. Which of the following applies to UDP?
(a) It is a connection-oriented protocol
(b) It is used by HTTP
(c) It has a fixed segment header
(d) It is used by SMTP

9. How many bytes are there in an IPv4 address?
(a) 16
(b) 32
(c) 64
(d) 4

10. Which one is a feature of IPv6, different from IPv4?
(a) Fragmentation
(b) 128-bit address
(c) Variable length header
(d) A field of "more fragments" (MF)

11. Which one of the following maps MAC address onto IP address?
(a) ARP
(b) DNS
(c) Dynamic DNS
(d) RARP

12. Which of the following is NOT a characteristic of a Ethernet network?
(a) Ethernet is a very popular LAN technology
(b) Ethernet senses the channel first before transmitting
(c) Ethernet operates only at half-duplex
(d) Ethernet is a very expensive technology

13. Which of the following is NOT true about the MAC address?
(a) It uniquely identifies a network adapter
(b) It can be changed when a host is moved to another network.
(c) It is 48-bits in size
(d) It is usually stored in a ROM chip on the network adapter.

14. Which ONE is a function of the Network layer?
(a) To be responsible for path determination of packets
(b) To be responsible for in-order delivery of packets
(c) To be responsible for connection-setup management
(d) To be responsible for congestion control

15. Which of the following is NOT true about a 100 Base-T/TX standard?
(a) The transmission speed is 100 Mbps
(b) It uses Fibre optic cable
(c) It uses a baseband signal
(d) It can operate at full-duplex

16. What does CSMA stands for?
(a) Code Synchronisation Model Access
(b) Coding Synchronisation Model Access
(c) Carrier Sense Model Access
(d) Carrier Sense Multiple Access

17. The number of links needed in a full-mesh topology with 20 hosts is?
(a) 200
(b) 210
(c) 180
(d) 190

18. Which of the following is not an application layer protocol?
(a) SMTP
(b) ICMP
(c) DNS
(d) TFTP

19. What is the port number associated with HTTP?
(a) 21
(b) 25
(c) 23
(d) None of the above

20. What is the default subnet mask for a Class B network?
(a) 255.255.255.0
(b) 255.255.255.255
(c) 255.0.0.0
(d) None of the above

21. You are asked to create 14 Class C subnets with at least 14 hosts per subnet. Which subnet mask must you use?
(a) 255.255.255.192
(b) 255.255.255.224
(c) 255.255.255.240
(d) 255.255.255.248

22. Which one does NOT apply to private-key encryption?
(a) It is also called symmetric encryption
(b) It uses a pair of keys
(c) It is also called secret-key encryption
(d) It uses a single, shared, key

23. In IEEE 802.11, a ____ is made of stationary or mobile wireless clients and an optional central base station, known as the access point (AP).
(a) ESS
(b) CSS
(c) BSS
(d) None of the above

24. What is the purpose of the TTL field in an IPv4 header?
(a) It is used for error correction
(b) It is used to identify the host address
(c) It is used to ensure that packets do not roam around indefinitely
(d) It is used for fragmentation

25. Gigabit Ethernet has a maximum data rate of ____ Mbps.
(a) 10
(b) 100
(c) 1000
(d) 10,000

[25 x 2 marks]

SECTION B
ATTEMPT ANY TWO QUESTIONS

Question 2 (25 marks)

(a) Contrast the ISO-OSI Reference model and the TCP/IP protocol stack. Mention the differences and similarities between the layers.

[6 marks]

(b) Given the following URL: ***http://www.sussex.ac.uk/public/index.html***

i. What is the top-level domain?
ii. Briefly, describe the initial interactions that takes place after the URL is loaded in the Address bar of a web browser connected to the Internet?
iii. Give a sample HTTP request message sent by the web browser paying attention to the request and header lines.
iv. Why does DNS use a distributed approach as opposed to a single server?

[2+3+5+2 marks]

(c) A user has been allocated an email account with id: ***Bond007@mi5.com***

i. Give a potential domain name for the user's mail server.
ii. What is the purpose of a Mail Access Protocol ?
iii. Define and give one difference between POP3 and IMAP4?

[1+2+4 marks]

Question 3 (25 marks)

(a) Describe briefly the difference between flow control and congestion control in relation to a connection-oriented protocol such as TCP.

[6 marks]

(b) What is the initial rate of data transfer in the slow start phase of TCP congestion control, if the MSS is 960 bytes and an average RTT of 50 milliseconds?

[2 marks]

(c) Each host on the Internet is currently assigned an IP address 32 bits long (IPv4). IPv4 addresses are usually written as a series of four decimal numbers. IPv4 addresses traditionally belong to one of five classes of address, depending on the type of network.

i. Describe the structure of Class D network and what it is reserved for.
ii. Give two advantages of creating subnets within a larger network.
iii. On an isolated network two hosts with IP addresses 128.129.130.131 and 128.129.150.151 share a common 255.255.224.0 subnet mask. Can the two hosts communicate directly with each other?
iv. Give four differences between IPv6 and IPv4?

[3+2+5+4 marks]

(d) Describe very briefly the purpose of the following protocols:

i. DHCP
ii. SMTP
iii. ARP

[3 marks]

Question 4 (25 marks)

(a) Name four types of active attacks and mention the security services they respectively attack?

[4 marks]

(b) Distinguish between authentication and non-repudiation.

[4 marks]

(c) A datagram of 2700 bytes has to travel over a network with a MTU size of 900 bytes. Explain how fragmentation can be used to solve this problem.

You should give the value of the 3 key fields used in fragmentation for each fragment created.

[8 marks]

(d) Nowadays many companies are shifting towards the IEEE 802.11x standard for extending their network.

i. Outline **two** popular flavours of this wireless standard. Elaborate on the operating frequency, range and speed of each flavour.
ii. What are the **two** modes of operation of this standard and explain the difference between the two.
iii. Mention **one** security issue with this wireless technology and explain how this issue can be addressed.

[3+4+2 marks]

******END OF PAPER******

UNIVERSITY of TECHNOLOGY, MAURITIUS

B.Sc. (Hons.) Business Information Systems
B.Sc. (Hons.) Computer Science with Network Security
B.Eng.(Hons) Telecommunications

BIS/12/FT – BCNS/12/FT - BTEL/12/FT

Examinations for 2012-2013 / Semester 2

MODULE: NETWORKS

MODULE CODE: CAN1102

DURATION: 2¼ HOURS

Instructions to Candidates

1. Answer **ALL THREE** questions.
2. Always start a new question on a fresh page.
3. Questions carry **unequal** marks.
4. Maximum marks achievable: **100**
5. Use of silent calculators is permitted in the Examination Room.
6. Appendix is provided

This question paper contains 3 questions and 4 pages.

ANSWER ALL QUESTIONS

Question 1 (34 Marks)

(a) Assume that you enter the following URL in the address bar of a popular web client and that both the client and server accepts HTTP version 1.1.

`http://www.rishiheerasing.net/images/thief.png`

i. What will be the initial request made by the client?
ii. Explain how HTTP version 1.1 allows 'surfing' experience to be greatly improved.
iii. Give a sample HTTP request message with at least 4 main header lines that is sent by the web client.
iv. Assume that the web resource is actually found on the server, give at least 3 header lines that you would expect in the sample response HTTP message.

[2+4+4+3 marks]

(b) Authentication and Integrity are two important network security services.
i. Explain what you understand by authentication.
ii. Describe **one** mechanism that you could use to ensure data integrity alone during transmission.

[2+3 marks]

(c) FTP is a popular protocol used to transfer files from one host to another.
i. Explain briefly how it works.
ii. Give **three** advantages that it has over HTTP for files transfer.

[3+3 marks]

(d) In respect of the ISO/OSI Reference model,
i. Give **three** important functions handled by Layer 6.
ii. Give **one** advantage of the layered approach used by such a model.
iii. Give **two** disadvantages of having too many layers in a communication model.

[6+2+2 marks]

Question 2 (33 Marks)

(a) In relation to a TCP segment structure, give the fields responsible for:
i. Connection Management
ii. Flow Control
iii. Error Control
iv. Reliable, in-order delivery.

[2+1+1+2 marks]

(b) Describe the **four** header fields present in a UDP segment.

[4 marks]

(c) Each host on the Internet is currently assigned an IP address 32 bits long (Ipv4). Ipv4 addresses are usually written as a series of four decimal numbers. IPv4 addresses traditionally belong to one of five classes of address, depending on the type of network.

i. Give the address range for a Class B network.
ii. What are Class D network addresses primarily used for?
iii. Can two hosts A and B with addresses 192.168.27.27 and 192.168.27.37 respectively communicate directly with each other if they share a subnet mask of 255.255.255.240?
iv. Describe one short-term technique which has been used to solve the shortage of Ipv4 addresses.
v. Give **three** main differences between IPv4 and IPv6.

[2+2+5+5+3 marks]

(d) A datagram of 3200 bytes has to travel over a network with a MTU size of 1500 bytes. Explain how fragmentation can be used to solve this problem.

You should give the value of the 3 key fields used in fragmentation for each fragment created.

[6 marks]

Question 3 (33 Marks)

(a) Explain how CSMA/CD operates and describe how Ethernet deals with collisions.

[5 marks]

(b) Explain how the following protocols work:
i. ARP
ii. DHCP
iii. DNS
iv. SMTP

[4 x 4 marks]

(c) The IEEE 802.11x standard is popular in extending wired networks.

i. Outline **two** popular flavours of this wireless standard. Elaborate on the operating frequency, range and speed of each flavour.
ii. What are the **two** modes of operation of this standard and explain the difference between them.
iii. Mention **one** security issue with this wireless technology and explain how this issue can be addressed.

[3+2+2 marks]

(d) Given the following received codeword C and the generator polynomial G. Determine if an error has taken place during transmission. *You should justify your answer.*

C: 110110011
G: $x^3 + x$

[5 marks]

****** End of Exam Paper ******