SCHOOL OF INNOVATIVE TECHNOLOGIES & ENGINEERING

Module Information Pack

BSc (Hons) Computing and Information Systems (Top Up)

v3.0 – July 2021

Communication & Networking v1.0

CAN2120C

April 2024 – BCIS/24A/PT

Blended Mode (Online and F2F)

Programme Director:	Mr. Pillay Kanaksabee
Programme Coordinator:	Mr. Pillay Kanaksabee
Module Convenor:	Mr. Rishi Heerasing
Office:	Room G2.14 Level 2 SITE BLOCK
Phone:	207 5250 Ext. 34
E-mail:	rheerasing@utm.ac.mu
Academic Tutoring:	None
Lecture Timing & Venue:	Tuesdays 16:30 – 19:30 in Lab G0.3
Credits & Level:	6 credits, Level 3
Pre-requisites (If applicable):	None
Co-requisites (If applicable):	None
Method of Delivery & Frequency:	15 x 3 Hrs sessions of lectures, tutorials and practicals.
Method & Criteria of Assessment:	50% Exam & 50% Coursework

Module Aims:

- Investigate the fundamentals of data communication and the problems that affects communication in relation to computer networks.
- Illustrate the concepts and applications of communications technologies and networks in the context of the OSI and TCP/IP reference models.
- Investigate the various communications standards, protocols, architectures, and transmission techniques currently available.
- LAN Design and Implementation.
- Routing and Switching principles.
- Introduce the need for error detection and correction of data in digital networks.
- Understand the different metrics and concepts in network performance.
- Use of simulation software (Wireshark/Packet Tracer) and network device configuration

Learning Objectives and Outcomes:

- Understand the technical literature, fundamental concepts and 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 difference between data moving along the network layer and the data link layer.
- Understand how simulation software and protocol analysers can be used to assess network performance.
- Understand the types and functions of network interconnect devices.

TENTATIVE CLASS SCHEDULE

WK	Date	Topics Covered
1	07/05/24 Online	Introduction; Communications Model; ISO-OSI Reference Model; TCP/IP Suite. Application Layer
2	**14/05/24 F2F**	**Network Performance**
3	21/05/24 Online	Application Layer (Cont.): Application protocols such as :HTTP, FTP, SMTP, POP/IMAP, DNS
4	28/05/24 Online	Transport Layer: Services and Protocols; TCP vs. UDP; Segment Structure, Reliable Transfer, Flow Control, Connection Management.
5	04/06/24 Online	Network Layer: Services and Path selection; IPv4; IPv6.
6	**11/06/24 F2F**	**Network Layer (Cont.): IPv4 addressing and Calculation**
7	18/06/24 Online	Network Layer (Cont.): Fragmentation; ICMP; DHCP.
8	25/06/24 Online	Data Link Layer: Services; LAN addressing; ARP and RARP. Ethernet.
9	02/07/24 Online	Routing and Switching principles
10	**09/07/24 F2F**	**Error Detection and Correction**
11	16/07/24 Online	Wireless Technologies
12	**23/07/24 F2F**	**Open-book Class Test (25%)**
13	30/07/24 Online	Security
14	**06/08/24 F2F**	Physical Layer: Encoding Techniques **– Assignment Submission (25%)**
15	13/08/24 Online	Buffer

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., (D4.6KUR)**[Ж]
- **Tanenbaum A. (2001) *Computer Networks:* 4th Ed., (D4.6TAN)** [Ж]
- Stallings W (2001) *Data & Computer Communications:* 6th Ed., (D4.6STA) [Ж]
- Hallsall F. (2001) *Data Communications, Computer Networks, and Open Systems:* 4th Ed., (D4.6HAL)
- Lowe D. (2005) *Networking for Dummies:* 7th Ed., Wiley Publishing [Ж]

[Ж] *You can get a copy in e-book format on my website at Nefertum's Shrine.*

OTHER READING MATERIALS e.g. TEXTS/JOURNALS/ARTICLES/WEBSITES:

1. ddison Wesley Companion Website for *Computer Networking: A Top-Down Approach , 4th Edition* at http://wps.aw.com/aw_kurose_network_4
2. rentice-Hall Website for *Computer Networks*, *4th Edition* at http://authors.phptr.com/tanenbaumcn4/
3. ebsite for *Data and Computer Communications, 8th Edition* at http://williamstallings.com/DCC/DCC8e.html

MODULE RESOURCES

The lecture notes, lab exercises and software are available on my website: **Nefertum's Shrine** at http://www.rishiheerasing.net

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

Introduction to Networks

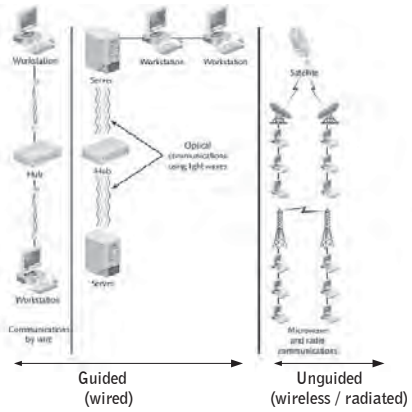
CAN2120C

Communication & Networking

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** and **Security**.

Types of Communication Links



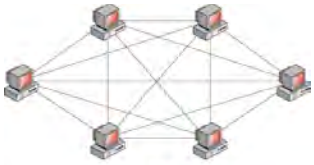
Physical Topology

- The **physical topology** refers to the way a network is laid out physically.
- **2** or more **nodes** connect to a **link. 2** or more **links** form a **topology**. The **topology** is the geometric representation of the relationship of all the links and nodes to one another.
- The are usually **four** basic topologies: **Mesh**, **Star, Bus** and **Ring**.

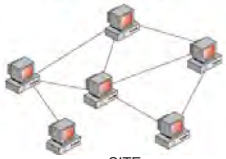
Mesh Topology

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

Full-Mesh:

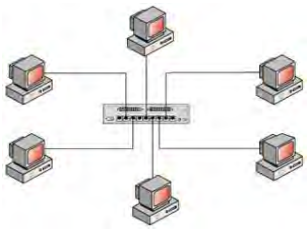


Partial-Mesh:



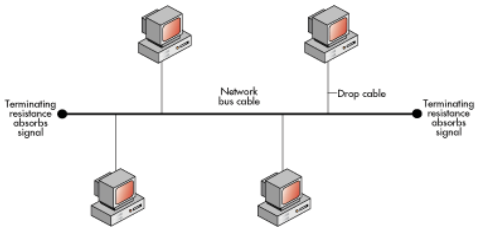
Star Topology

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



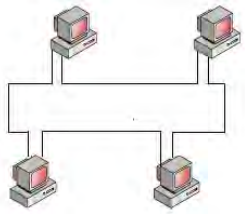
Bus Topology

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



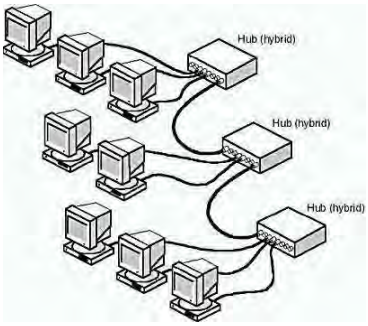
Ring Topology

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



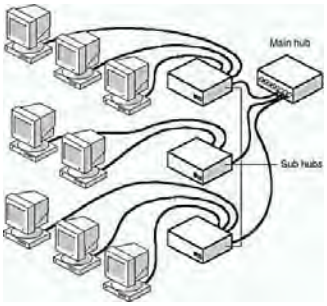
Hybrid: Star Bus Topology

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



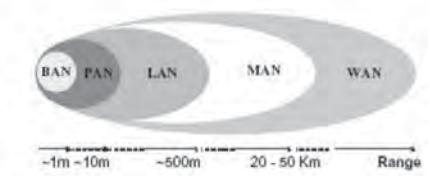
Hybrid: Star Ring Topology

- 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**.



Network Types Defined

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



Body Area Network (BAN)

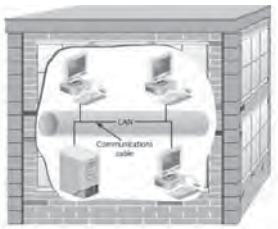
- Short range wireless network which consists of wearable or implanted electronic devices that transmit ID or sensor data to gateway device.
- It is also referred to as Wireless Body Area Network (WBAN) or Body Sensor Network (BSN)

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.
- Personal area networks may be wired by computer buses such as USB and FireWire. However, a Wireless Personal Area Network (WPAN) is made possible with network technologies such as Infrared (IrDA) and Bluetooth.

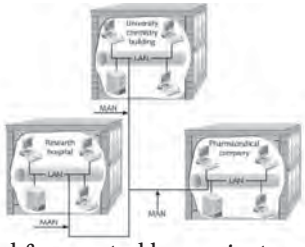
Local Area Network (LAN)

- 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.



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).

Wide Area Network (WAN)

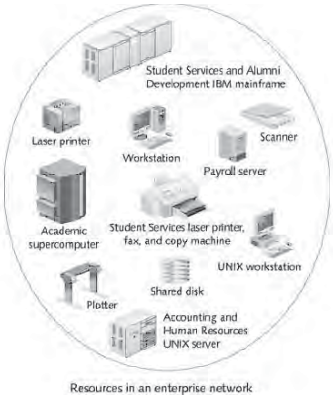
- Provides long-distance transmission of data, voice, image and video information over large geographic areas that may comprise a country, a continent, even the whole world.
- The best example of a WAN is the **Internet**.

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

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

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

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

LAN/WAN History: 1970s

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

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

LAN/WAN History: 1990s

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

LAN/WAN History: 2000s

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

LAN/WAN History: 2010s

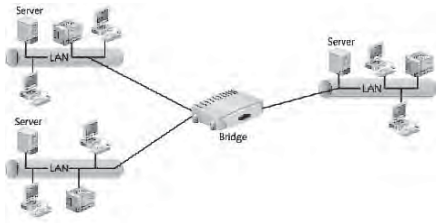
- Cloud Services commonplace
- Internet Of Things (IOT)
- 10G, 25G, 40G and 100G Ethernet has been developed

LAN/WAN Integration

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

Bridges

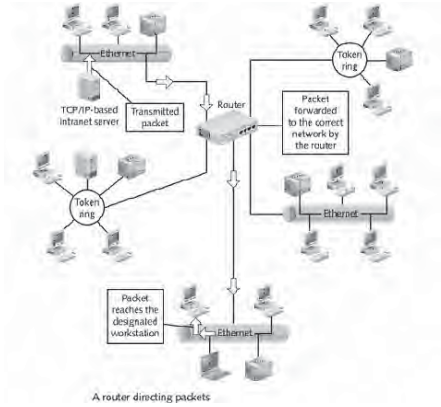
- Connect different LANs or LAN segments using the **same access** method



Routers

- Connect networks having the same or different access methods and media
- Route packets and 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

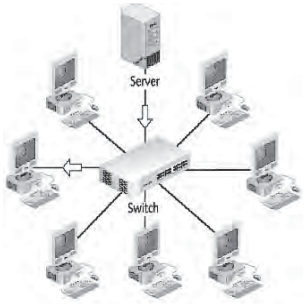
Routers



A router directing packets

Switches

- Link network segments
- Forward and filter frames between segments

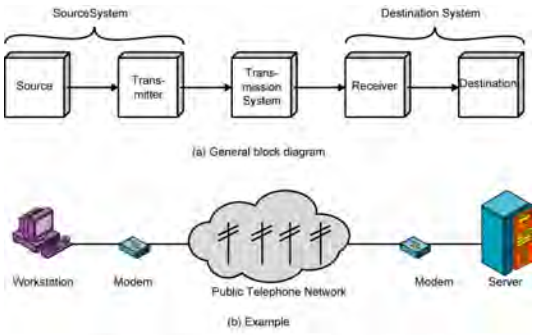


A switch in operation

Data Communications *v.* Networking

- Communication is concerned with the transmission of data over a communication medium/channel between two entities. Here we are more concerned about EE issues such as physical properties of communication medium, physical characteristics of signals and interfaces, format, and timing of signals, etc.…
- Networking 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.

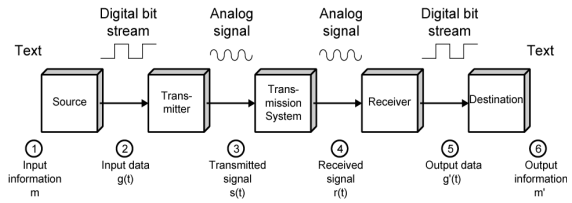
Simplified Communication Model



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



Layered Model

- Systems communicate over a shared communication medium according to an agreed upon convention (standard).
- 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

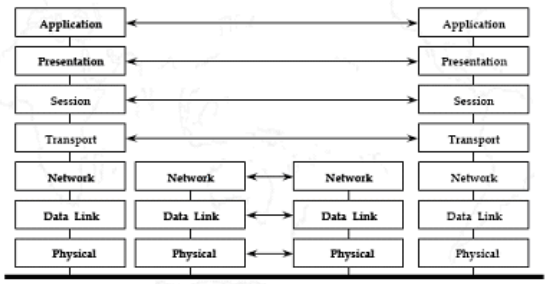
- DARPA (Defence Advanced Research Projects Agency)
- ARPANET => Internet
- TCP/IP Transmission Control Protocol/Internet Protocol
- TCP/IP developed concurrently with ISO model. TCP/IP does not contain protocols relating to all ISO layers. Most of the functionalities of ISO are embedded in TCP/IP.

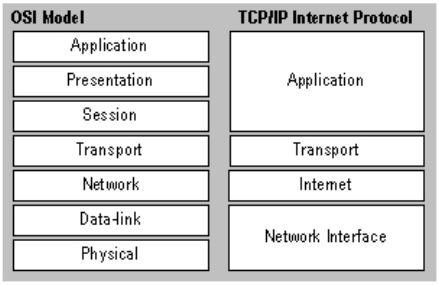
ISO/OSI Model

- 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, IM
- 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 layer protocols (TCP, UDP)

Application-layer protocols defines:

- 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, Viber, 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., Web server sends requested Web page, mail server delivers e-mail

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	Bandwidth	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, 100's msec
stored audio/video	loss-tolerant	same as above	yes, few secs
interactive games	loss-tolerant	few kbps up	yes, 100's msec
instant 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	Underlying transport protocol
e-mail	SMTP [*RFC 2821*]	TCP
remote terminal access	Telnet [*RFC 854*]	TCP
Web	HTTP [*RFC 2616*]	TCP
file transfer	FTP [*RFC 959*]	TCP
streaming multimedia	proprietary (e.g. RealNetworks)	TCP or UDP
Internet telephony	proprietary (e.g., Dialpad)	typically UDP

WEB and HTTP

- Web page consists of objects
- Object can be HTML file, JPEG image, Java applet, audio file,…
- Web page consists of base HTML-file which includes several referenced objects
- Each object is addressable by a URL
- Example URL:

http://pages.intnet.mu/rhh/index.html

HTTP overview

HTTP: HyperText Transfer Protocol

- Web's application layer protocol
- client/server model
  - *client:* browser that requests, receives, "displays" Web objects
  - *server:* Web server sends objects in response to requests

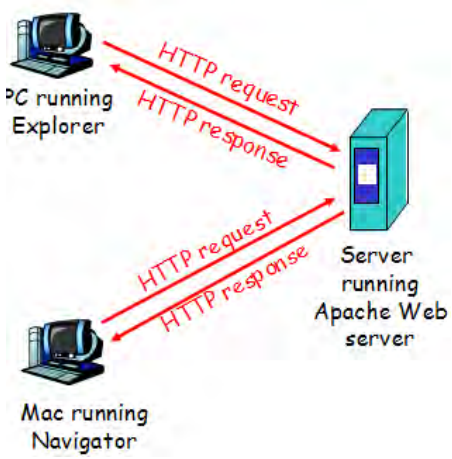
- HTTP 1.0: RFC 1945
- HTTP 1.1: RFC 2068

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

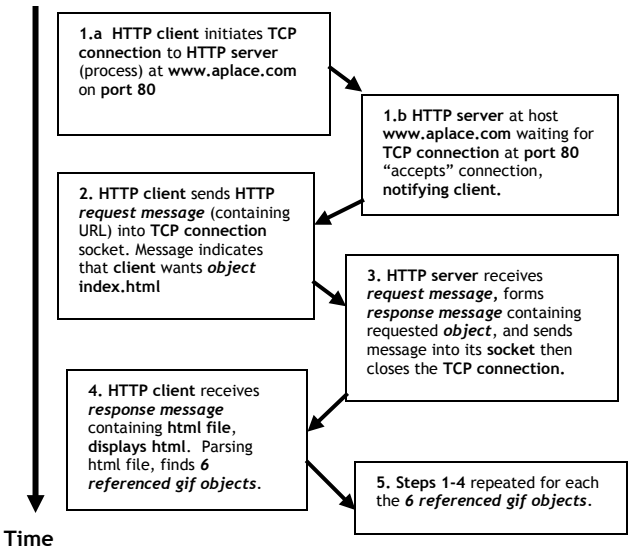
1. Non-persistent HTTP:
   - At most one object is sent over a single TCP connection.
   - HTTP/1.0 uses non-persistent HTTP.
2. Persistent HTTP:
   - Multiple objects can be sent over a single TCP connection between client and server.
   - HTTP/1.1 uses persistent connections in default mode.

Non-persistent HTTP

Suppose a user enters the following URL:

http://www.aplace.com/index.html and that this homepage contains some text and references to 6 gif images in total.

The following interactions will take place:



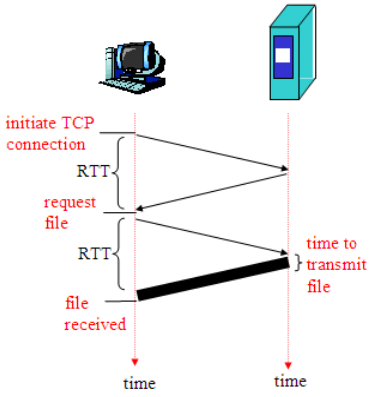
Response Time Modeling

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.

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.

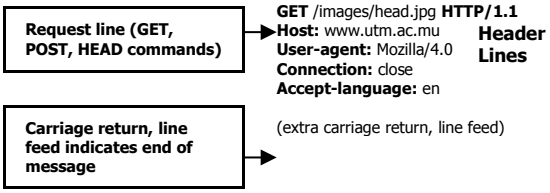
HTTP messages

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

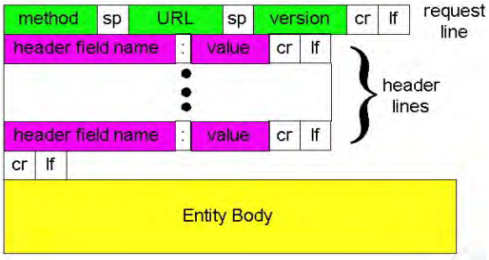
HTTP Request message

- 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:

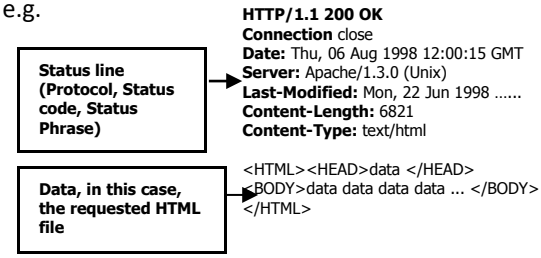
- GET, POST
- HEAD: asks server to leave requested object out of response.

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 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.

Trying out HTTP (client side) for yourself

Telnet to Telecom Plus personal pages web server:

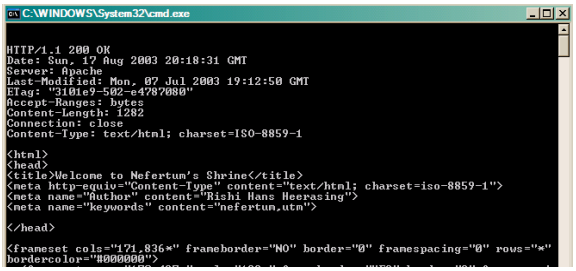
When you are online on your PC, open the Command Prompt Window (or choose **Run**, type **cmd**) and type the following as is: (Pay attention to the spaces)

telnet(space)pages.intnet.mu(space)80(enter)

The command you just typed has open a TCP connection on port 80 on the server **pages.intnet.mu**. The screen should go blank. Now everything you type in will get sent to *port 80* of the server. Next type your request message: (e.g. try to get my site's homepage)

GET(space)/rhh/index.htm(space)HTTP/1.1(enter)(enter)

If you typed well, you should get something like this:



Otherwise, you will get a 400 or 404 error codes.

Note: you might not see your request message on the screen while typing. Don't worry, just type it blindly.

Try it with other referenced objects as well.

Client-Server Interaction: Authorization

Authorization: control access to server content.

- *authorization credentials*: typically username, password
- *stateless*: *client* must present authorization in *each* request
- *authorization*: header line in each request
- if no authorization: header, server refuses access, sends WWW authenticate: header line in response

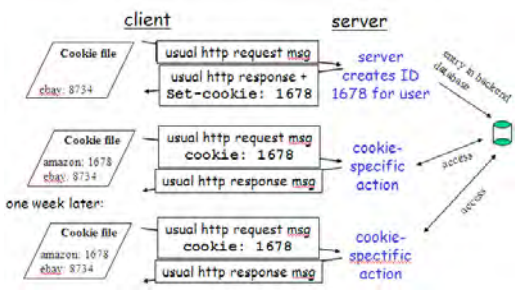
Cookies: Keeping "State"

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.



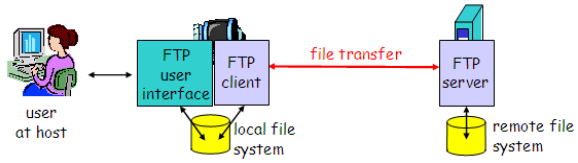
When and where cookies can be used:

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

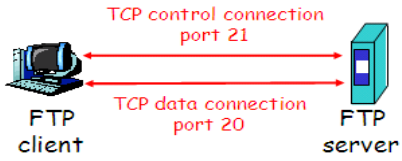
FTP: File Transfer Protocol



- 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., Eudora, Outlook Express, Thunderbird,elm
- outgoing, incoming messages stored on server.

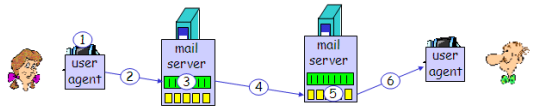
Mail Servers
- mailbox contains incoming messages for user
- message queue of outgoing mail messages
- SMTP protocol between mail servers to send email messages
- client: sending mail server
- server: receiving mail server

SMTP [RFC 2821]

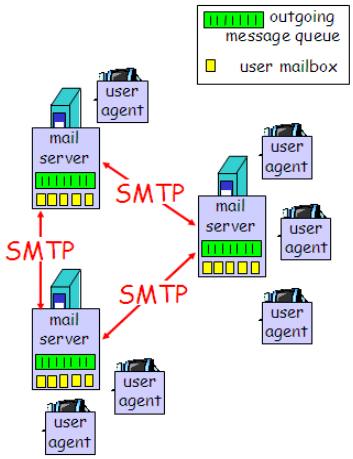
- uses TCP to reliably transfer email message from client to server, port 25
- direct transfer: sending server to receiving server
- Three phases of transfer:
  handshaking (greeting)
  transfer of messages
  closure
- command/response interaction
  commands: ASCII text
  response: status code and phrase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

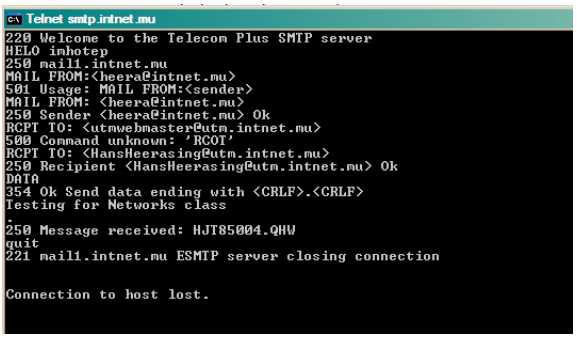
Example: Alice sends a message to Bob

1) Alice uses UA to compose message and "to" bob@utm.intnet.mu
2) Alice's UA sends message to her mail server; message placed in message queue
3) Client side of SMTP opens TCP connection with Bob's mail server
4) SMTP client sends Alice's message over the TCP connection
5) Bob's mail server places the message in Bob's mailbox
6) Bob invokes his user agent to read message



Typical SMTP Interaction





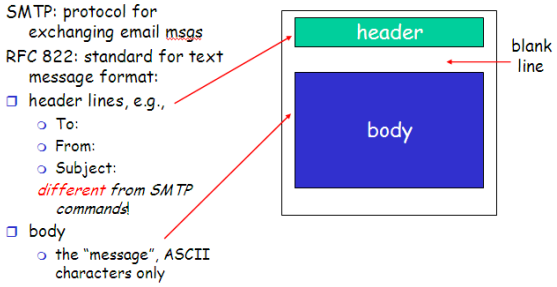
TRY sending a mail to yourself using the Command Prompt alone.

- telnet smtp.intnet.mu 25
- see 220 reply from server, Enter HELO, MAIL FROM, RCPT TO, DATA, QUIT.

Summary

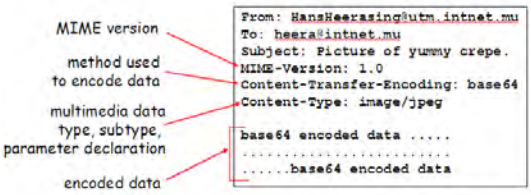
- SMTP uses persistent connections.
- SMTP requires message (header & body) to be in 7-bit ASCII.
- SMTP server uses CRLF.CRLF to determine end of message
- HTTP: pull SMTP: push
- Both have ASCII command/response interaction, status codes.
- HTTP: each object encapsulated in its own response message.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

- SMTP: delivery/storage to receiver's server
- Mail access protocol: retrieval from server
  - POP: Post Office Protocol [RFC 1939] authorization (agent <-->server) and download
  - IMAP: Internet Mail Access Protocol [RFC 1730] more features (more complex) manipulation of stored messages on server
  - HTTP: Hotmail, Yahoo! Mail, etc.

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 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. TPlus: DNS server is dns1.intnet.mu at IP 202.123.2.6
- Host 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

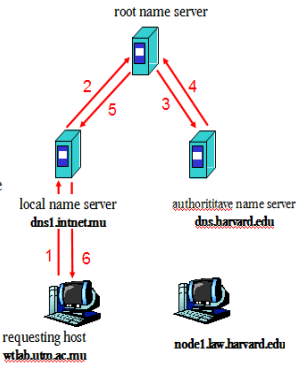
- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server

13 root name servers worldwide

Simple DNS example

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

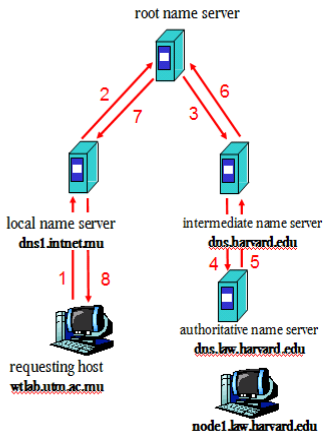
1. contacts its local DNS server, **dns1.intnet.mu**
2. **dns1.intnet.mu** contacts root name server, if necessary.
3. root name server contacts authoritative name server, **dns.harvard.edu**, if necessary



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)

Master Page 18 of 69

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 sending letters amongst themselves.*

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

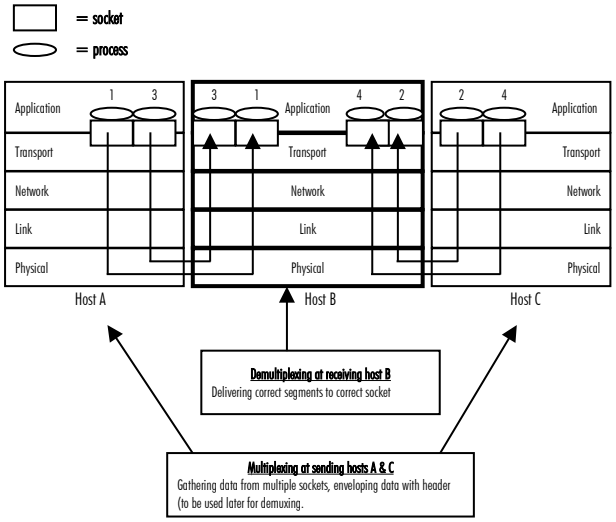
Internet Transport-Layer Services

TCP
- ***reliable, in-order delivery***
- ***congestion control***
- ***flow control, error control***
- ***connection setup***

UDP
- ***no-frills (best-effort service)***
- ***unreliable, unordered delivery***

SERVICES NOT AVAILABLE TO BOTH:
- ***Delay guarantees***
- ***Bandwidth guarantees***

Multiplexing and Demultiplexing

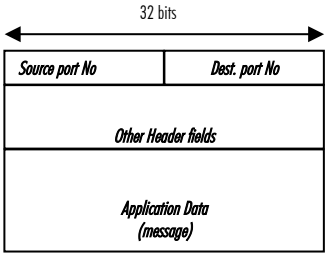


How demultiplexing works?

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 ptotocols*)**

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



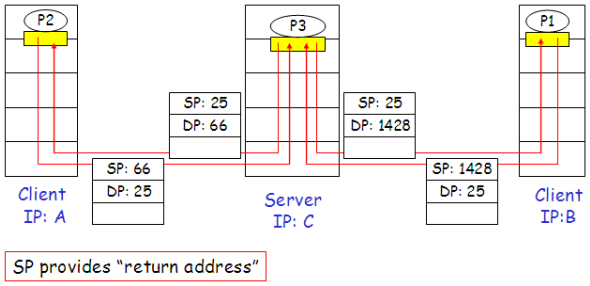
Generic *TCP* or *UDP* segment

Master Page 19 of 69

Connectionless demultiplexing: UDP

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

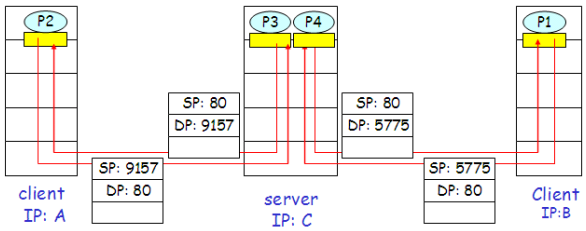
- When host receives ***UDP segment***:
  checks ***destination port number*** in segment.
  directs UDP segment to socket with that ***port number.***
- ***IP datagrams*** with different source ***IP addresses*** and/or ***source port numbers*** directed to same socket.



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.



Connectionless Transport: UDP [RFC 768]

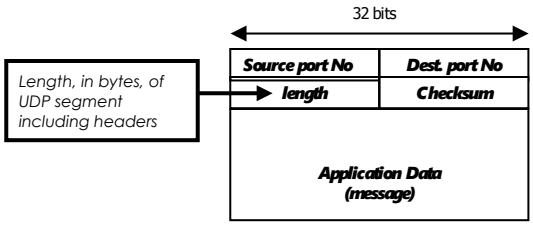
- "no frills" Internet Transport Protocol
- "best effort" service, UDP segments may be:
  - lost
  - delivered out of order to applications
- *connectionless-oriented:*
  - no handshaking between parties
  - each UDP segment handled independently of others

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 ….

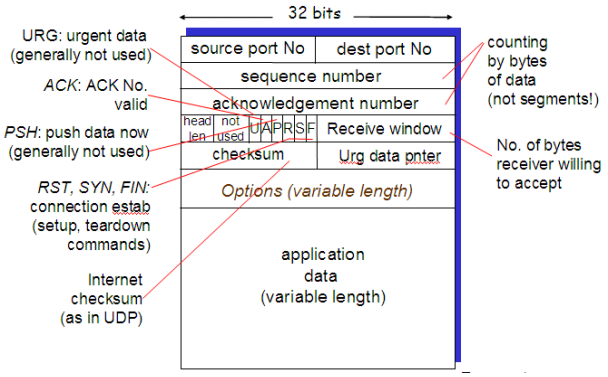
Master Page 20 of 69

Connection-Oriented Transport: TCP [RFC 793]

Transmission Control Protocol

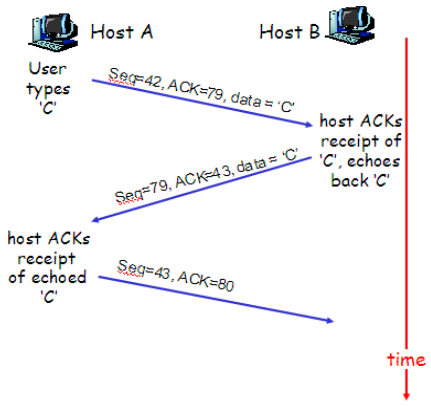
- **point-to-point:**
  - one sender, one receiver
- **reliable, in-order *byte steam:***
  - no "message boundaries"
- **pipelined:**
  - TCP congestion and flow control set window size
- **send & receive buffers**
- **full duplex data:**
  - bi-directional data flow in same connection
  - MSS: maximum 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 Format



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

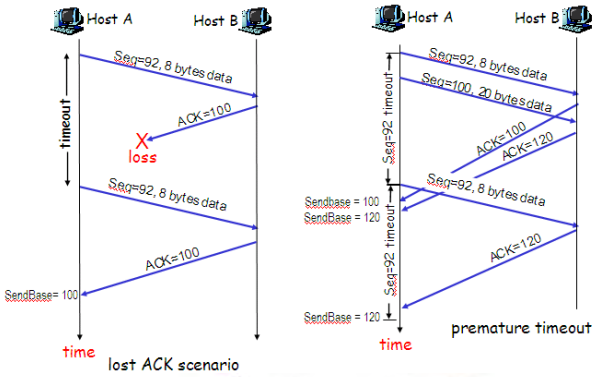
Reliable Data Transfer

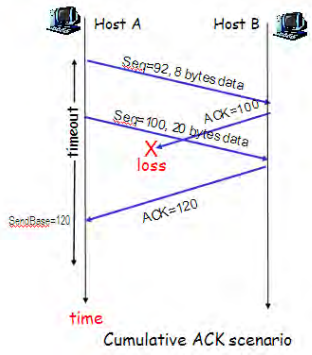
- TCP creates *reliable data transfer* service on top of IP's unreliable service.
- *Pipelined* segments.
- *Cumulative Acks*
- TCP uses single *retransmission timer.*
- ***Retransmissions*** are triggered by:
  - *timeout events*
  - *duplicate ACKS*
- Initially consider simplified TCP sender:
  - ignore duplicate ACKS
  - ignore flow control, congestion control

TCP Sender Events

- <u>Data received from Applications:</u>
  - 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
- <u>Timeout:</u>
  - retransmit segment that caused timeout
  - restart timer
- <u>ACK received:</u>
  - If acknowledges previously unACKed segments
  - update what is known to be ACKed
  - start timer if there are any outstanding segments

3 TCP Transmission Scenarios

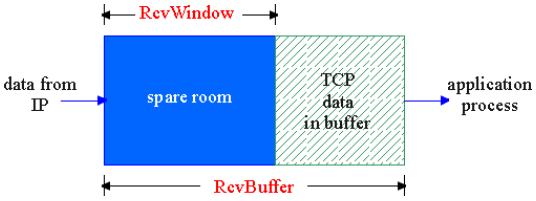




TCP Flow Control

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)

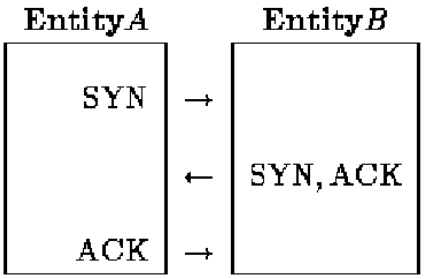
- **spare room in buffer**
  = RcvWindow
  = RcvBuffer-[LastByteRcvd - LastByteRead]
- Reciever advertises spare room by including value of RcvWindow in segments
- Sender limits unACKed data to RcvWindow
- guarantees receive buffer doesn't overflow

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

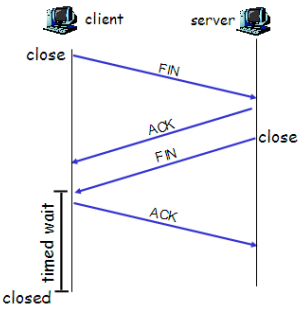


Closing a connection:

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.

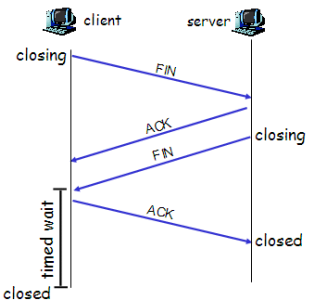


Step 3: client receives FIN, replies with ACK.

- 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.



Master Page 22 of 69

Network Layer

- Network Layer Services
- Routing principles: path selection
- IPv4
- IP Fragmentation, ICMP and DHCP
- IPv6

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?

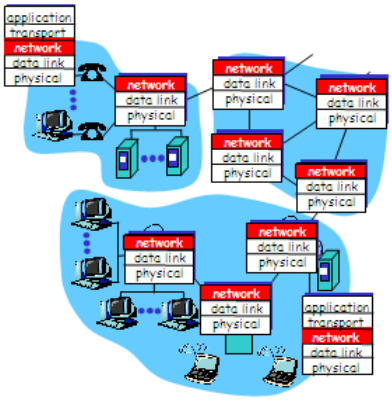
- call setup, teardown for each call *before* data can flow
- each packet carries VC Identifier (not destination host ID)
- *every* router on source-destination path keeps *state* for each passing connection

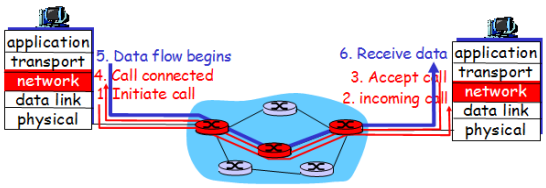
Note: Transport-layer connections only involved in the two end systems.

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

Signaling Protocols

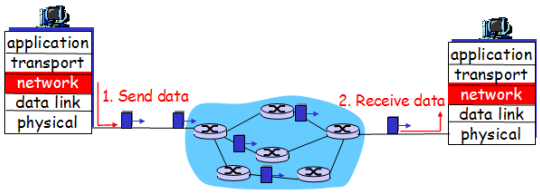
- used to setup, maintain & teardown Virtual Circuit
- used in ATM, frame-relay, X.25 (*more later*)





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 ?				Congestion feedback
		Bandwidth	Loss	Order	Timing	
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

Master Page 23 of 69

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

Routing Principles: path selection

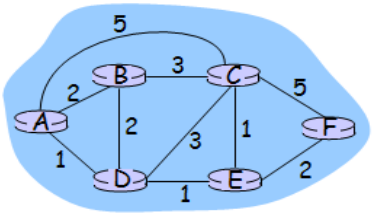
Routing Protocol:

***Goal*:** *Determine "good" path through network from source to destination*

Graph abstraction for routing algorithms:

- graph nodes are routers
- graph edges are physical links
- Link cost: delay, physical cost, or congestion level.

e.g.



What does ***"good"*** path mean?

- typically means **minimum cost** path
- other definitions also possible

Routing Algorithms Classification

Global:

- all routers have complete topology & link cost info.
- **"link state" algorithms**

Decentralized:

- router knows physically-connected neighbours, link costs to neighbours only
- iterative process of computation, exchange of info with neighbours
- **"distance vector" algorithms**

Static:

- routes change slowly over time.

Dynamic:

- routes change more quickly
  - periodic update in changes in link costs

An example of a static, "link-state" algorithm: *Dijkstra's Algorithm*

- net topology, link costs known to all nodes
  - accomplished via "link state broadcast"
  - all nodes have same info
- computes least cost paths from one node ('source") to all other nodes
  - gives routing table for that node.
- iterative: after k iterations, know least cost path to k destinations

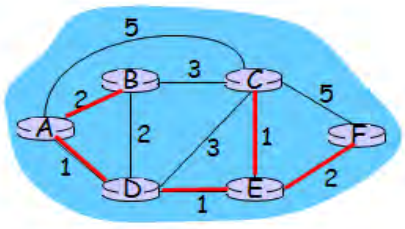
Notation:

- c(i,j): link cost from node i to j. cost infinite if not direct neighbours
- D(v): current value of cost of path from source to destination V
- p(v): predecessor node along path from source to v, that is next v
- N: set of nodes whose least cost path definitively known

Pseudo-Code:

```
1  Initialization:
2   N = {A}
3   for all nodes v
4    if v adjacent to A
5      then D(v) = c(A,v)
6      else D(v) = infinity
7
8  Loop
9    find w not in N such that D(w) is a minimum
10   add w to N
11   update D(v) for all v adjacent to w and not in N:
12      D(v) = min( D(v), D(w) + c(w,v) )
13   /* new cost to v is either old cost to v or known
14    shortest path cost to w plus cost from w to v */
15 until all nodes in N
```

e.g.



Step	start N	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	2,A	5,A	1,A	infinity	infinity
1	AD	2,A	4,D		2,D	infinity
2	ADE	2,A	3,E			4,E
3	ADEB		3,E			4,E
4	ADEBC					4,E
5	ADEBCF					

Master Page 24 of 69

Dynamic, Distance Vector Routing algorithm

iterative:
- ❖ continues until no nodes exchange info.
- ❖ *self-terminating*: no "signal" to stop

asynchronous:
- ❖ nodes need *not* exchange info/iterate in lock step!

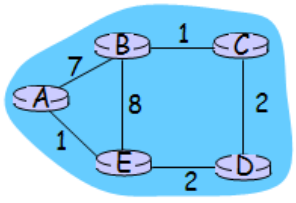
distributed:
- ❖ each node communicates *only* with directly-attached neighbours

Distance Table data structure

- ❖ each node has its own
- ❖ row for each possible destination
- ❖ column for each directly-attached neighbour to node
- ❖ eg: in node X, for destination Y via neighbour Z:

$$D^X(Y,Z) = \text{distance } \textit{from } X \textit{ to } Y, \textit{ via } Z \text{ as next hop}$$
$$= c(X,Z) + \min_w\{D^Z(Y,w)\}$$

Example:



$$D^E(C,D) = c(E,D) + \min_w\{D^D(C,w)\}$$
$$= 2+2 = 4$$
$$D^E(A,D) = c(E,D) + \min_w\{D^D(A,w)\}$$
$$= 2+3 = 5 \quad \text{loop!}$$
$$D^E(A,B) = c(E,B) + \min_w\{D^B(A,w)\}$$
$$= 8+6 = 14 \quad \text{loop!}$$

Distance Table:

$D^E()$	cost to destination via A	B	D
destination A	(1)	14	5
destination B	7	8	(5)
destination C	6	9	(4)
destination D	4	11	(2)

Distance Table gives Routing Table:

$D^E()$	cost to destination via A	B	D
destination A	(1)	14	5
destination B	7	8	(5)
destination C	6	9	(4)
destination D	4	11	(2)

destination	Outgoing link to use, cost
A	A,1
B	D,5
C	D,4
D	D,2

Distance table → Routing table

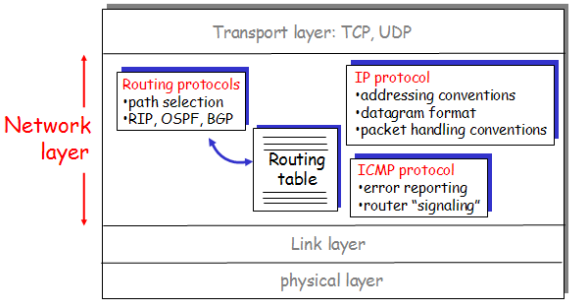
Summary

Iterative, asynchronous: each local iteration caused by:
- ❖ local link cost change
- ❖ message from neighbour: its least cost path change from neighbour

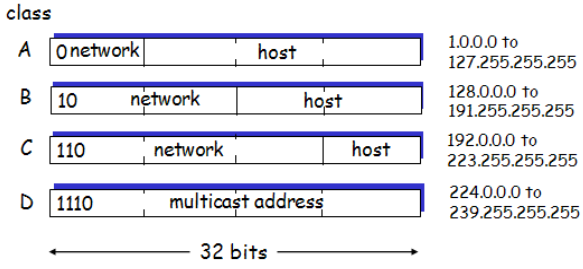
Distributed:
- ❖ each node notifies neighbours *only* when its least cost path to any destination changes
- ❖ neighbours then notify their neighbours if necessary

The Internet Protocol Version 4 (IPv4) 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 four 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.

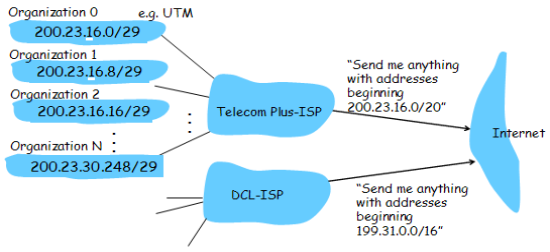
Restrict block sizes to powers of 2

All routers must understand CIDR addressing

Lets see this at work…

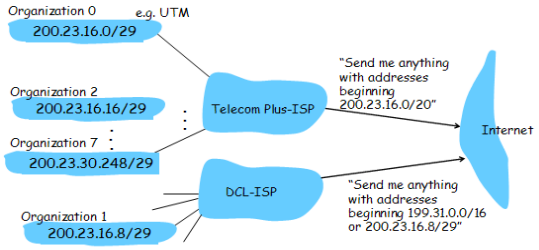
ISP's block	11001000 00010111 00010000 00000000	200.23.16.0/20
Organization 0	11001000 00010111 00010000 00000000	200.23.16.0/29
Organization 1	11001000 00010111 00010000 00001000	200.23.16.8/29
Organization 2	11001000 00010111 00010000 00010000	200.23.16.16/29
…	……	….
Organization 7	11001000 00010111 00011110 11111000	200.23.30.248/29

Hierarchal Addressing: Route Aggregation



Hierarchical addressing: more specific routes

DCL has a more specific route to Organization 1



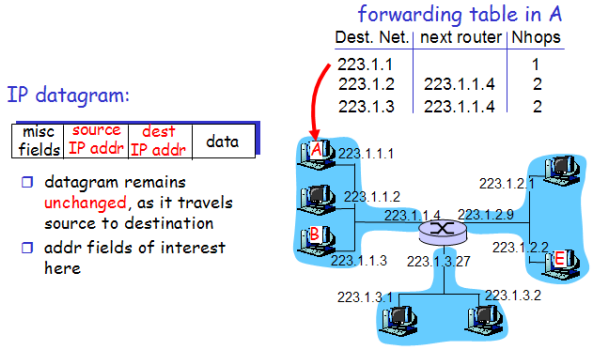
How does Host get IP address?

- 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?

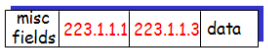
- ***ICANN***: **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers
  - allocates addresses
  - manages DNS
  - assigns domain names, resolves disputes

Getting a datagram from Source to Destination



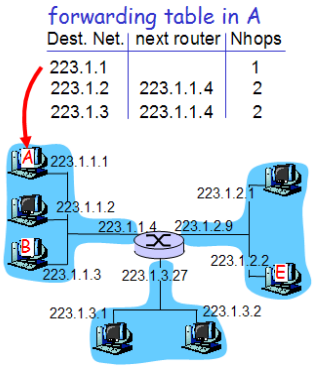
Master Page 26 of 69

Case 1

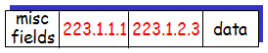


Starting at A, send IP datagram addressed to B:

- 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

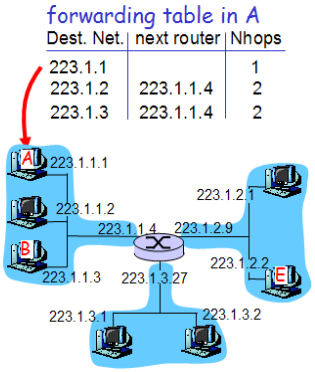


Case 2

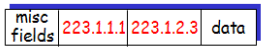


Starting at A, dest. E:

- 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…..

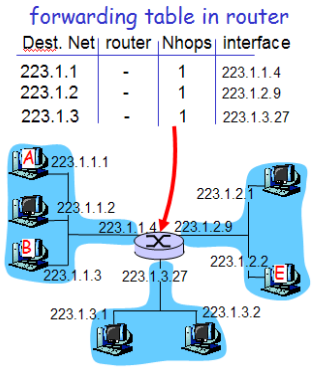


Case 3

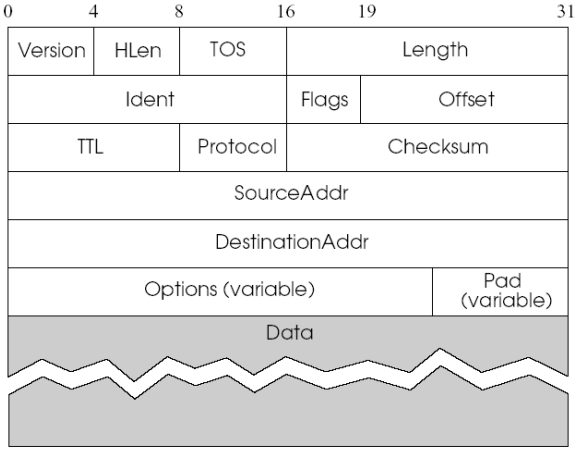


Arriving at 223.1.4, destined for 223.1.2.2

- 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!)



IPv4 Datagram Format (revisited)



Data Link Layer

Slide Set 2

Our goals:

- understand principles behind data link layer services:
  - link layer addressing
- instantiation and implementation of various link layer technologies

Outline

Slide Set 2

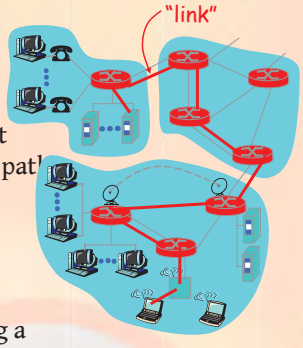
- **Introduction and services**
- LAN addresses and ARP
- Ethernet
- Hubs, bridges, and switches

Link Layer: Introduction

Slide Set 2

Terminology:

- hosts and routers are **nodes** (bridges and switches too)
- communication channels that connect adjacent nodes along communication pat are **links**
  - wired links
  - wireless links



- Layer 2-PDU is a **frame,** encapsulating a datagram

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

Link layer: context

Slide Set 2

- 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

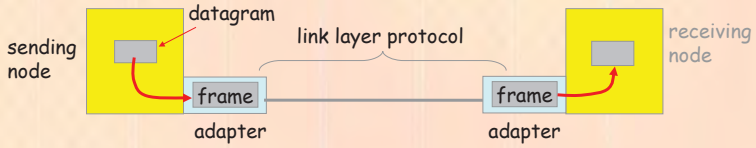
Link Layer Services

Slide Set 2

- **Framing, link access:**
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - '**physical 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
    - Q: why both link-level and end-end reliability?

Adaptors Communicating

Slide Set 2



- link layer implemented in "adaptor" (NIC)
  - Ethernet card, PCMCI card, 802.11 card
- sending side:
  - encapsulates datagram in a frame
  - adds error checking bits, rdt, flow control, etc.
- receiving side
  - looks for errors, rdt, flow control, etc
  - extracts datagram, passes to receiving node
- adapter is semi-autonomous
- link & physical layers

LAN Addresses and ARP

Slide Set 2

32-bit IP address: (Logical)

- *network-layer* address
- used to get datagram to destination IP network (recall IP network definition)

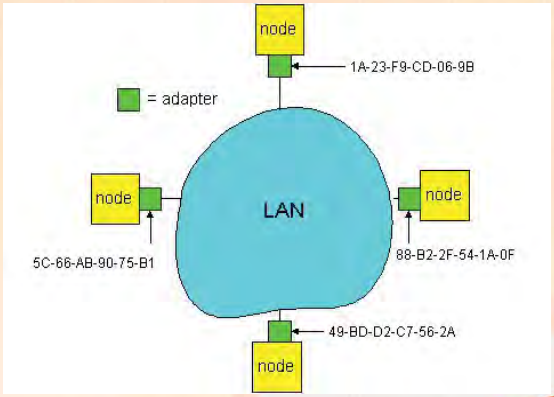
48-bit LAN (or MAC or Physical or Ethernet) address:

- 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 hence cannot be changed.

LAN Addresses and ARP

Slide Set 2

Each adapter on LAN has unique LAN address



LAN Address

Slide Set 2

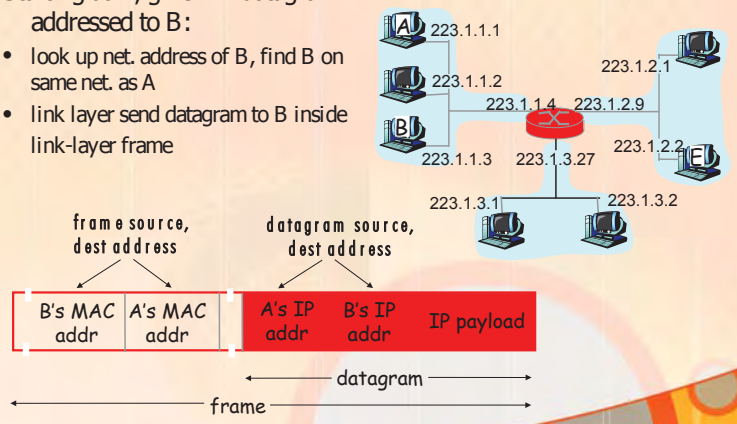
- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:
  - (a) MAC address: like NIC Number
  - (b) IP address: like postal address
- MAC flat address => portability
  - can move LAN card from one LAN to another
- IP hierarchical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

Recall earlier routing discussion

Slide Set 2

Starting at A, given IP datagram addressed to B:

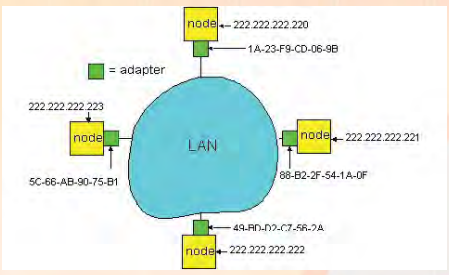
- look up net. address of B, find B on same net. as A
- link layer send datagram to B inside link-layer frame



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

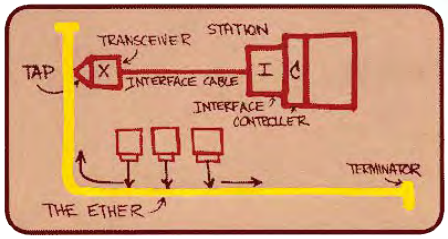
Slide Set 2

- 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

Ethernet

"dominant" LAN technology:

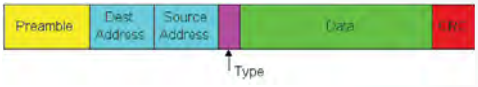
- cheap $20 for 100Mbps !
- first widely used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10,100,1000 Mbps, 10 Gbps



Metcalfe's Ethernet sketch

Ethernet Frame Structure

Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

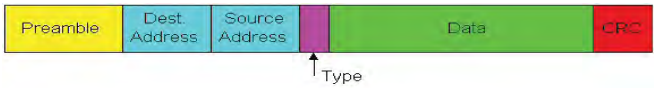


Preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- used to synchronize receiver, sender clock rates

Ethernet Frame Structure (more)

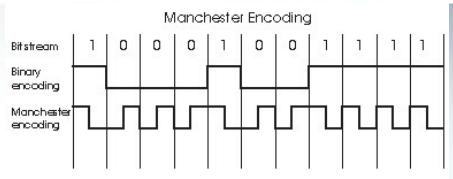
- Addresses: 6 bytes
  - if adapter receives frame with matching destination address, or with broadcast address (e.g. ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- Type: indicates the higher layer protocol, mostly IP but others may be supported such as Novell IPX and AppleTalk)
- CRC: checked at receiver, if error is detected, the frame is simply dropped



Unreliable, connectionless service

- Connectionless: No handshaking between sending and receiving adapter.
- Unreliable: receiving adapter doesn't send *acks* or *nacks* to sending adapter
  - stream of datagrams passed to network layer can have gaps
  - gaps will be filled if app is using TCP
  - otherwise, app will see the gaps

Manchester Encoding



- Used in 10BaseT, 100BaseT, 1000 BaseT
- Each bit has a transition
- Allows clocks in sending and receiving nodes to synchronize to each other
  - no need for a centralized, global clock among nodes!
- This is physical-layer stuff !

Gigabit Ethernet

- use standard Ethernet frame format
- allows for point-to-point links and shared broadcast channels
- in shared mode, CSMA/CD is used; short distances between nodes to be efficient
- uses hubs, called here "Buffered Distributors"
- Full-Duplex at 1 Gbps for point-to-point links
- 10, 40, 100 Gbps now !!!

Interconnecting LAN segments

Slide Set 2

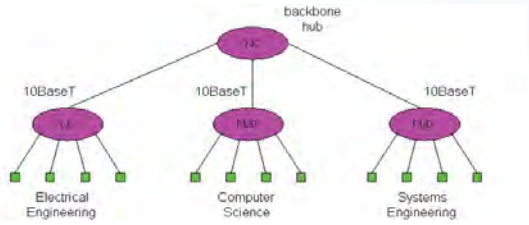
- Hubs
- Bridges
- Switches
  - Remark: switches are essentially multi-port bridges.
  - What we say about **bridges** also holds for **switches**!

19

Interconnecting with hubs

Slide Set 2

- Backbone hub interconnects LAN segments
- Extends max distance between nodes
- But individual segment collision domains become one large collision domain
  - if a node in CS and a node EE transmit at same time: collision
- Can't interconnect 10BaseT & 100BaseT



20

Bridges

Slide Set 2

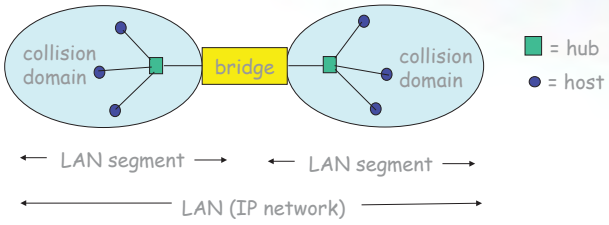
- **Link layer device**
  - stores and forwards Ethernet frames
  - examines frame header and selectively forwards frame based on MAC destination address
  - when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent
  - hosts are unaware of presence of bridges
- plug-and-play, self-learning
  - bridges do not need to be configured

21

Bridges: traffic isolation

Slide Set 2

- Bridge installation breaks LAN into LAN segments
- bridges filter packets:
  - same-LAN-segment frames not usually forwarded onto other LAN segments
  - segments become separate collision domains



22

Self learning

Slide Set 2

- A bridge has a bridge or forwarding table
- entry in bridge table:
  - (*Node LAN Address, Bridge Interface, Time Stamp*)
  - stale entries in table dropped (TTL can be 60 min)
- bridges *learn* which hosts can be reached through which interfaces
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender/location pair in forwarding table

23

Filtering / Forwarding

Slide Set 2

When bridge receives a frame:

index bridge table using MAC dest address
if entry found for destination
then{
if dest on segment from which frame arrived
then drop the frame
else forward the frame on interface indicated
}
else flood

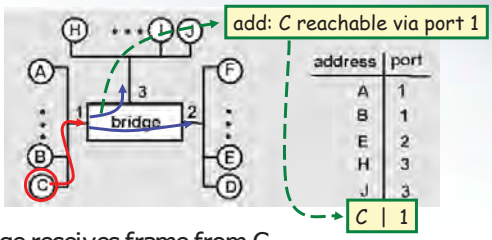
forward on all but the interface on which the frame arrived

24

Bridge Learning: example

Slide Set 2

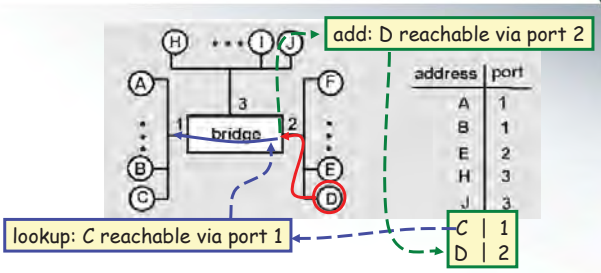
Suppose C sends frame to D and D replies back with frame to C.



- Bridge receives frame from C
  - Insert entry in bridge table that C is on interface 1
  - because D is not in table, bridge sends frame into interfaces 2 and 3 (flooding)
- frame received by D

Bridge Learning: example

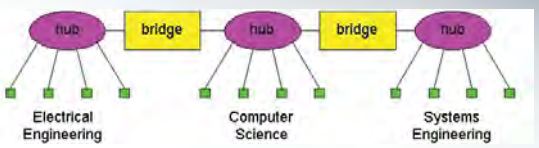
Slide Set 2



- D generates frame for C, sends
- bridge receives frame
  - Insert entry in bridge table that D is on interface 2
  - bridge knows C is on interface 1, so *selectively* forwards frame to interface 1

Interconnection without backbone

Slide Set 2

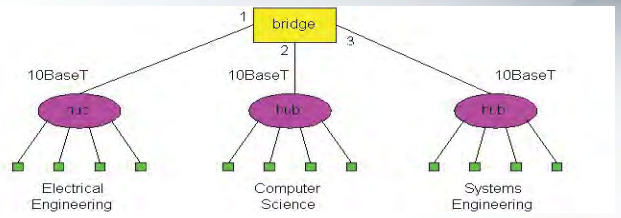


- Not recommended for two reasons:

- single point of failure at Computer Science hub
- all traffic between EE and SE must pass through the CS segment

Backbone configuration

Slide Set 2



Recommended !

Some Bridge features

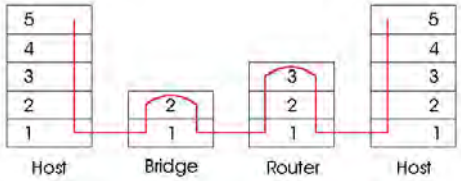
Slide Set 2

- Isolates collision domains resulting in higher total maximum throughput
- limitless number of nodes and geographical coverage
- Can connect different Ethernet types
- Transparent ("plug-and-play"): no configuration necessary

Bridges vs. Routers

Slide Set 2

- ***Both*** store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are link layer devices
- ***Routers*** maintain routing tables, implement routing algorithms
- ***Bridges*** maintain bridge tables, implement filtering, learning and spanning tree algorithms



Routers vs. Bridges

Bridges + and -

+ Bridge operation is simpler requiring less packet processing
+ Bridge tables are self learning
- All traffic confined to spanning tree, even when alternative bandwidth is available
- Bridges do not offer protection from *broadcast storms*

Routers vs. Bridges

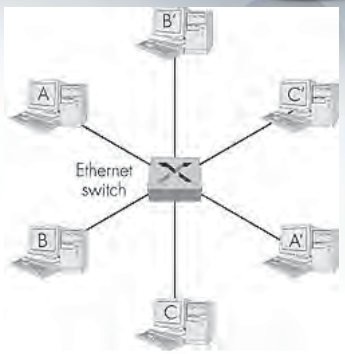
Routers + and -

+ arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)
+ provide protection against broadcast storms
- require IP address configuration (not plug and play)
- require higher packet processing

- bridges do well in small (few hundred hosts) while routers used in large networks (thousands of hosts)

Ethernet Switches

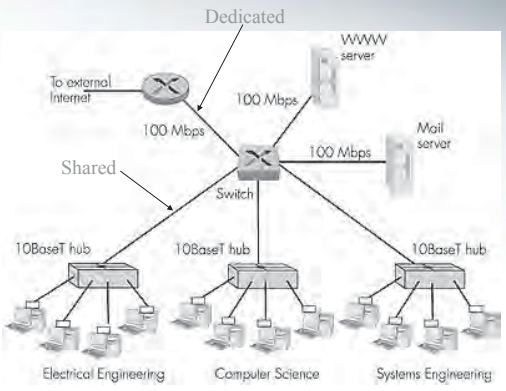
- Essentially a multi-interface bridge
- layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-A' and B-to-B' simultaneously, no collisions
- large number of interfaces
- often: individual hosts, star-connected into switch
  - Ethernet, but no collisions!



Ethernet Switches

- cut-through switching: frame forwarded from input to output port without awaiting for assembly of entire frame
  - slight reduction in latency
- Store-N-Forward switching: frame buffered completely and error-checked (via CRC) before being forwarded.

A typical LAN (IP network)



Summary comparison

	hubs	bridges	routers	switches
traffic isolation	no	yes	yes	yes
plug & play	yes	yes	no	yes
optimal routing	no	no	yes	no
cut through	yes	no	no	yes

Wireless LANs

Slide Set 3

Wireless LANs

- The Big Thing in local area networking today
- Gives mobility to users within the corporate premises
- Not a competitor yet for wired Ethernet LAN but wireless speed increasing everyday; mostly used to extend the wired LAN's resources

Wireless vs Wired: Pros and Cons

Parameter	Wireless	Wired
Security	Less Secure	More Secure
Data Rate	Slower (300 Mbps)	Faster (10 Gbps)
Setup and Deployment Cost	Cheaper	More Expensive
Connection Reliability	Less Reliable	More Reliable
Mobility	Higher	Much Lower
Deployment Speed	Faster	Slower
Range and Coverage	Smaller*	Larger
Robustness	Better	Weaker
Flexibility to change	Higher	Lower

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

A 802.11g Access Point with two antennas

USB: Most popular and portable. Works with any device with USB ports (popular)

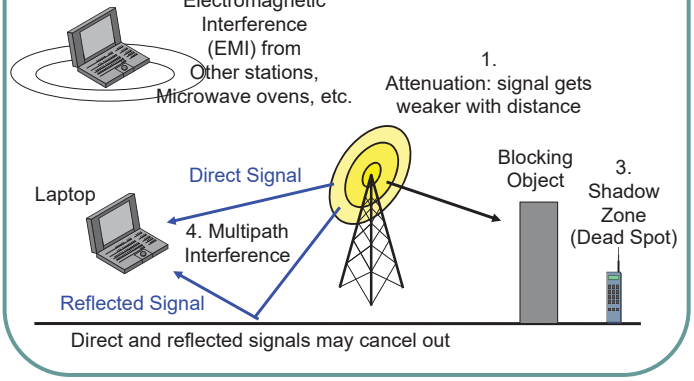
PCMCIA: used in old laptops with no built-in WLAN Adapter (obsolete)

PCI: used in Desktop PCs

Some Terminologies

- An Access Point (AP) or wireless Access Point is usually a device that only allows wireless clients (stations) to connect to it. Examples of wireless clients (smartphone, laptops, PDAs, tablets, Smart TVs, etc...)
- A wireless router is an AP which also contains a number wired ethernet ports that allows wired clients to connect to it. Basically, it is an AP+network switch.
- A wireless gateway is usually a wireless router which integrates a modem to provide Internet access as well. Basically, it is an AP+Switch+Modem (This is the one most of us have at home (Residential Gateway).
- A Hotspot is usually the same thing as a wireless gateway.

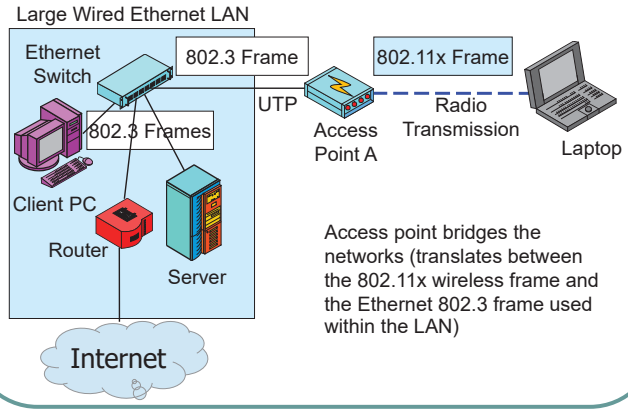
Wireless Propagation Problems



Wireless Propagation Problems

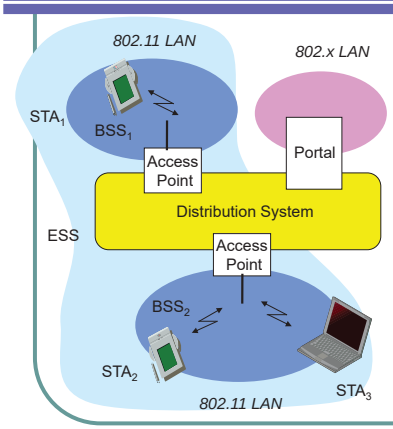
- Some problems are Frequency-Dependent
  - Higher-frequency signals attenuate faster
    - Absorbed more rapidly by moisture in the air
  - Higher-frequency signals blocked more by obstacles
    - At lower frequencies, signal refract (bend) around obstacles like an ocean wave hitting a buoy
    - At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

Typical 802.11 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)

Architecture of a wireless 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)
- 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

Typical AP modes of Operation

1. Infrastructure (Local/Managed) Mode
2. Client (Relay/Repeater) Mode ***
3. Sniffer (Monitor) Mode ***
4. Rogue Detector Mode ***
5. Bridge (Mesh) Mode ***

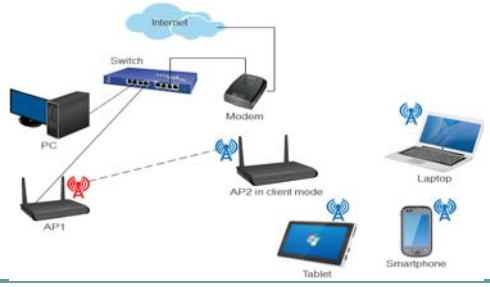
***(not available on all AP models)

1. Infrastructure (Local/Managed) Mode

The tablet, smartphone and laptop all connect wirelessly to the AP.

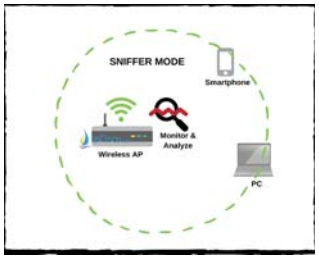
2. Client (Relay/Repeater) Mode

In this scenario, AP1 has internet connection, but the 3 stations are not in range to connect to it. AP2 is configured as client mode and connects to AP1 to allow the stations connected to the former to get internet access.



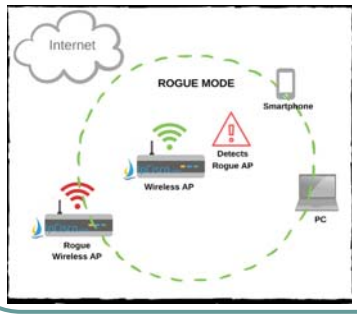
3. Sniffer (Monitor) Mode

In sniffer or monitor mode, the AP does not broadcast any SSID hence no wireless clients can connect to it but it can still receive wireless frames from stations. A laptop can connect remotely to the AP and perform sniffing with the appropriate software e.g. Wireshark



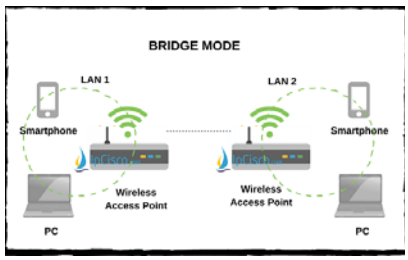
4. Rogue Detector Mode

In this mode, the AP is used to detect rogue devices. This detection is perform by inspecting the MAC address.



5. Bridge (Mesh) Mode

In Bridge mode, the two APs effectively establishes a point-to-point connection between themselves bridging 2 wireless LAN segments. If more than 2 APs are present, they can then establish point-to-multipoint connections effectively creating a mesh.



Ad-hoc or P2P Mode

In this mode, the stations connect to each other without the need of an access point (AP)

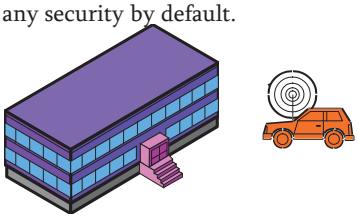
802.11 Wireless LAN Standards

802.11-Standard	Standard Year	Frequency (GHz)	RANGE (Typical) (I/O)	Modulation Type	Max. Data Rate (Mbit/s)
802.11a	1999	5 GHz	35m/120m	OFDM	54 Mbit/s
802.11ac	2013	5 GHz	70m/250m	OFDM	6,93 Gbit/s
802.11ad	2012	60 GHz	10m/N/A	SC-OFDM	6,76 Gbit/s
802.11b	1999	2,4 GHz	35m/140m	DSSS	11 Mbit/s
802.11g	2003	2,4 GHz	45m/100m	DSSS/OFDM	54 Mbit/s
802.11n	2009	2,4/5 GHz	70m/250m	OFDM	600 Mbit/s

DSSS, direct sequence spread spectrum
FHSS, frequency hopping spread spectrum
OFDM, orthogonal frequency division multiplex
SC-OFDM, single carrier orthogonal frequency division multiplex

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
  - This was possible as the first generation of APs did not have any security by default.



802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Initial flawed security method developed by the 802.11 Working Group for 802.11 devices in 1997.
  - All stations share the same encryption key with the access point. This key cannot be changed as it was a static key
  - 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

802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - 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. 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 SSID broadcast once all permitted stations have been allowed to join the wireless network.
  - Enable Access Point firewall features to mitigate potential attacks.

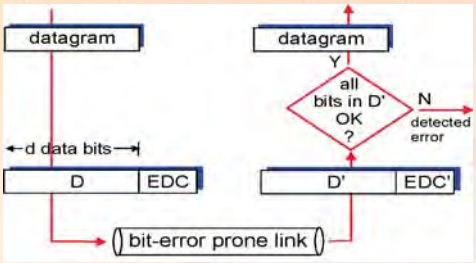
Error Control: Detection and Correction

Slide Set 4

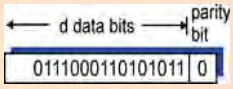
Error Detection

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)

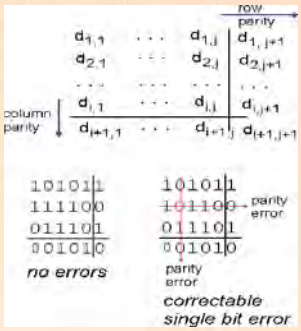
Even Parity Scheme:
Parity bit chosen so that total number of 1s including the parity bit is **EVEN.**

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

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

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)



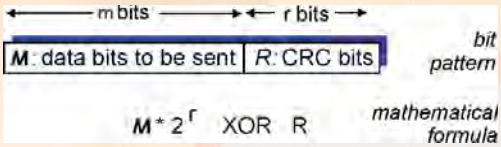
This is an example of even parity: The parity bits are chosen in such a way that the total number of 1s is either a column or row is even

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)

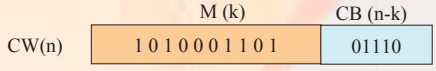
The FCS bits are used at Receiver for error detection

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)

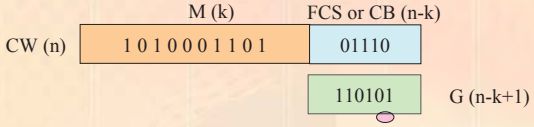
So, the total frame length is k + (n – k) = n bits or Code Word (CW)



CRC Generation

Slide Set 4

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)



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

Slide Set 4

- *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

Slide Set 4

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

Slide Set 4

- Given
  - M = 1 0 1 0 0 0 1 1 0 1
  - G = 1 1 0 1 0 1 (i.e. $x^5+x^4+x^2+1$)

  At the Sender (source) side
- 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

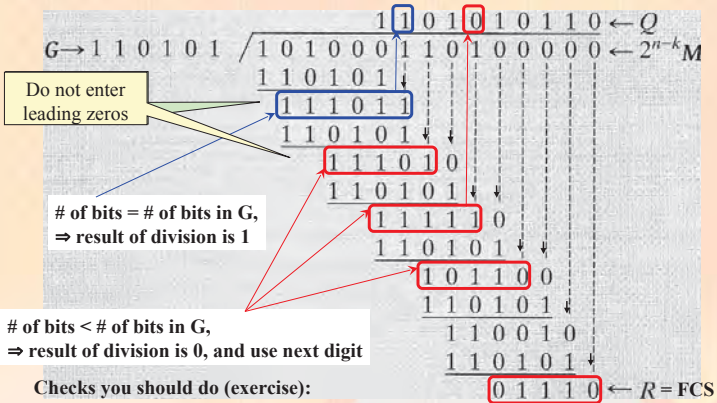
Slide Set 4

- 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

Slide Set 4



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 / 11100011000000
         110011
          101111
          110011
           111000
           110011
            101100
            110011
             111110
             110011
CRC =        11010
```

CW to transmit is? Answer: 1110001111010

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)

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, and insert the message bits in the remaining boxes. There are 13 boxes in all that will represent the 13 bits in the codeword.

- 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** 1 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** 1 or more errors as long as 1 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 the length of the message M.

Network Performance

Slide Set 5

Key Terms

- Bandwidth / Capacity of the network
- Throughput – Actual Rate of data passing a certain point in the network
- Latency (Delay) - delay incurred by a data from start to finish
  - Transmission Delay
  - Propagation Delay
  - Queuing/Buffer Delay
  - Processing Delay, etc...

Bandwidth/Capacity

Bandwidth can have two contexts in networking:

The first, Bandwidth measured in Hertz, refers to the range of frequency that a channel or link can have i.e. highest frequency – lowest frequency.

The second, bandwidth measured in bits per second, refers to the maximum rate of data that can be carried by a channel or link. This is often referred to as the Capacity to avoid confusion.

Bandwidth/Capacity

The Capacity of a channel or link is directly proportional to the Bandwidth available.

The higher the Bandwidth, the higher the capacity

This is shown by either the Nyquist and Shannon-Hartley Theorems below:

Nyquist: C = 2Blog2 M where M = no. of signal levels

Shannon-Harteley: C = B log2 (1 + S/N) where S/N is the Signal power to Noise power ratio.

Throughput

Throughput is the actual rate of data passing a particular point in the network. It is measured in bits per second just like Capacity.

The throughput is always less or equal to the capacity of a channel or link.

The throughput can never exceed the capacity of a channel.

For example, in wireless LAN 802.11g, the capacity is 54 Mbps, but the throughput at a certain distance from the transmitter will always be less than 54 Mbps.

Latency

Latencies are the delays present in a communication system.

Some of these latencies are negligible but some are not.

The one-way latency is the sum of all the delays added up from source to destination.

The two-way latency is also referred as to the Round-Trip-Time (RTT) or response time.

Transmission Delay

Transmission Delay or Transmit time is the time needed to inject the data on the network for ongoing transmission. It is directly proportional to the size of data and inversely proportional to the bandwidth of the channel or link.

$$\text{Transmit Time} = \frac{\text{Size of data (in bits)}}{\text{Bandwidth (in bits per second)}}$$

Propagation Delay

Propagation Delay or Travel time is the time taken for the data signal to travel from source to destination. It is directly proportional to the distance between source and destination and inversely proportional to the speed of the signal.

$$\text{Propagation Delay} = \frac{\text{Distance (in meters)}}{\text{Speed (in m/s)}}$$

Queuing/Buffer Delay

Queuing Delay or Buffer Delay is the time taken to 'absorb' the data at the receiver It is usually assumed to be equal to the transmit time if the same amount of data is received and bandwidth is unchanged.

$$\text{Buffer Time} = \frac{\text{Size of data (in bits)}}{\text{Bandwidth (in bits per second)}}$$

Processing Delays

Processing Delay is the time taken to process some information in order to take a decision.

Processing delays such as: Switching delay, Error detection delay, when intermediate devices such as hubs, bridges, switches and routers are present.

These delays depend of the speed of the processing unit, the type and amount of memory, as well as, the switching technology used within those devices.

Switching Delay

Switching Delay = Time taken to move data from incoming port to appropriate outgoing port.

In a switch, this is the time taken to decide which appropriate outgoing port to forward a frame after inspecting the forwarding table.

In a router, this is the time taken to decide which appropriate outgoing port to route a packet after inspecting the routing table.

Error Detection Delay

Error Detection Delay = Time taken to check for errors withing a frame or packet header.

Error detection delay **only** takes place in a switch operating in **Store-N-Forward** mode **because it buffers the frame completely**.

Note: No error detection in switches operating in cut-through mode.

In a router, error detection occurs for both the frame content and the packet header as well.

Switch Buffer time in Cut-through mode

In cut-through mode, the switch does not buffer the entire frame before it starts switching and retransmitting the frame via the appropriate output port.

The buffer time is therefore less than that of a switch operating in Store-N-Forward mode.

Buffer time at switch in cut-through mode =

$$\frac{\text{Minimum Buffer bits}}{\text{Bandwidth in bps}}$$

Performance Statistics

- The main network performance parameter is the **response time** as seen previously.
- Another parameter is **availability**; the percent of time the network is available. **Downtime** is the percent of time the network is not available.
- Failure statistics include:
  - **Mean time between failures (MTBF)** indicates the reliability of a network component.
  - **Mean time to repair (MTTR)** equal to the mean time to diagnose plus the mean time to respond plus the mean time to fix a problem.

MTTRepair = **MTTDiagnose** + **MTTRespond** + **MTTFix**

Availability

$$\text{Availability} = \frac{uptime}{uptime + downtime} = \frac{MTBF}{MTBF + MTTR}$$

Availability	Lost Time (hours)	Lost Time (minutes)	Lost Time (seconds)
60.00%	3504		
65.00%	3066		
70.00%	2628		
75.00%	2190		
85.00%	1314		
90.00%	876		
95.00%	438		
96.00%	350.4		
97.00%	262.8		
98.00%	175.2		
99.00%	87.6		
99.50%	43.8		
99.90%	8.76	525.6	
99.99%	0.876	52.6	3153.6
99.999%	0.0876	5.3	315.36
99.9999%	0.00876	0.5	31.536
99.99999%	0.000876	0.1	3.1536

1 year = 365 days/yr * 24 hrs/day = 8760 hrs/yr

Just as a remind

Reliability

$$\text{Reliability} = e^{-T/\Phi}$$

$$\text{Reliability} = e^{-\Lambda T}$$

$$\text{Reliability} = e^{-N}$$

Reliability	Failures per year	Failures per 10 years	Failures per 100 years
10.00%	2.30		
20.00%	1.61		
30.00%	1.20		
40.00%	0.92		
50.00%	0.69		
60.00%	0.51		
70.00%	0.36		
80.00%	0.22	2.23	
90.00%	0.11	1.05	
95.00%	0.05	0.51	
99.00%	0.01	0.10	1.01
99.50%	0.005	0.05	0.50
99.90%	0.001	0.01	0.10
99.99%	0.0001	0.001	0.01
99.999%	0.00001	0.0001	0.001
99.9999%	0.0000010	0.00001	0.0001
99.99999%	0.00000010	0.000001	0.00001

1 yr mission = 365 days/yr * 24 hrs/day = 8760 hrs/yr

Where $\Phi = MTBF$, $\Lambda =$ *Failure Rate*

$N =$ *number of failures,* $T =$ *mission time*

Network Security

Slide Set 6

What is this chapter about?

This chapter is to address

- security needs
- security services
- security mechanisms and protocols

for data stored in computers and transmitted across computer networks

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 example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard, Rott…
- Detection
  - missing items, burglar alarms, CCTV, …
- Reaction
  - attack on burglar, call the police, replace stolen items, 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
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, 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
  - i.e. Physical and Administrative mechanisms
- Modern World
  - Data is found inside computers in digital format
  - Computers are interconnected
  - **Hence computer and network security 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)
    - against viruses
- 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
  - 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 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 internally ("fetiche")
    - release the content ("palabre")
    - traffic analysis ("veille mouvement")
  - Hard to detect, try to prevent… How?

Attacks

- Active attacks involves interruption, 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

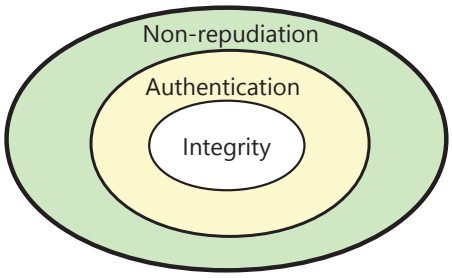
ISO 7498-2 Security Services

- 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, deletion 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 security 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

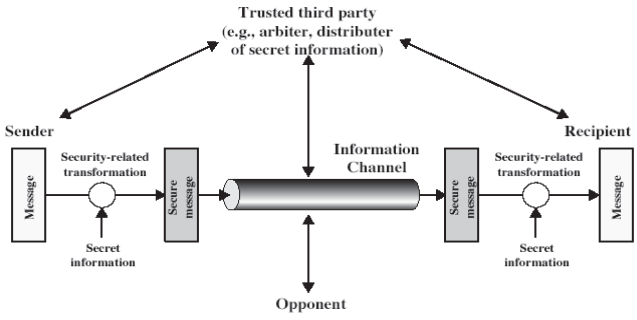
Security Mechanisms

- 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 (more later)
  - Firewalls, Honeynet, Honeypot (more later)

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

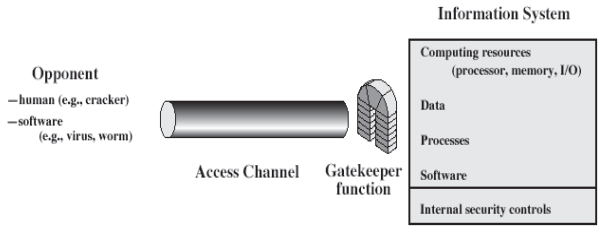
Model for Network Security



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
  - 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.

Network Planning & Design

Slide Set 7

Learning Outcomes

- Be familiar with the overall process of design and implementing a network
- Be familiar with techniques for developing a logical network design
- Be familiar with techniques for developing a physical network design
- Be familiar with network design principles

Outline

- **Introduction**
  - Traditional Network Design
  - Building Block Network Design
- **Needs Analysis**
  - Geographic Scope
  - Application Systems
  - Network Users
  - Categorizing Network Needs
  - Deliverables
- **Technology Design**
  - Designing Clients and Servers
  - Designing Circuits and Devices
  - Network Design Tools
  - Deliverables
- **Cost Assessment**
  - Request for Proposal
  - Selling the Proposal to Management
  - Deliverables

Traditional Network Design

- The traditional network design approach follows a structured systems analysis and design process similar to that used to build application systems.
  - The network analyst meets with users to determine the needs and applications.
  - The analyst estimates data traffic on each part of the network.
  - The analyst designs circuits needed to support this traffic and obtains cost estimates.
  - Finally, a year or two later, the network is implemented.

Traditional Network Design

- Three forces are making the traditional design approach less appropriate for many of today's networks:
  - 1. The underlying technology of computers, networking devices and the circuits themselves are rapidly changing.
  - 2. Network traffic is growing rapidly.
  - 3. The balance of costs has changed dramatically over the last 10 years.

Building Block Network Design

- While some organizations still use the traditional approach, many others use a simpler approach to network design, the building block approach.
- This approach involves three phases: needs analysis, technology design, and cost assessment (Fig. 11-1).
- When the cost assessment is initially completed, the design process returns to the needs analysis phase and cycles through all three phases again, refining the outcome of each phase.
- The process of cycling through all three design phases is repeated until a final design is decided on (Fig. 11-2).

Figure 11-1 Building Block Network

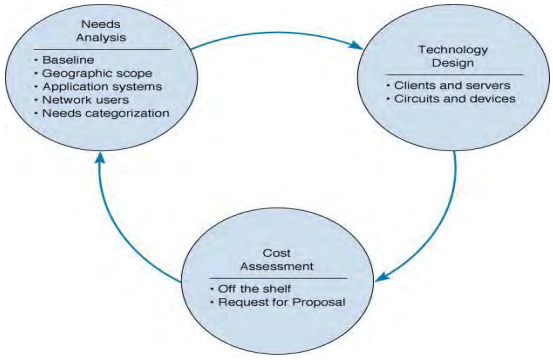
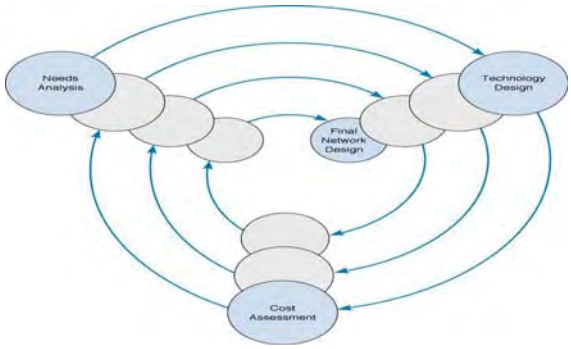


Figure 11-2 Reaching a Final Network Design



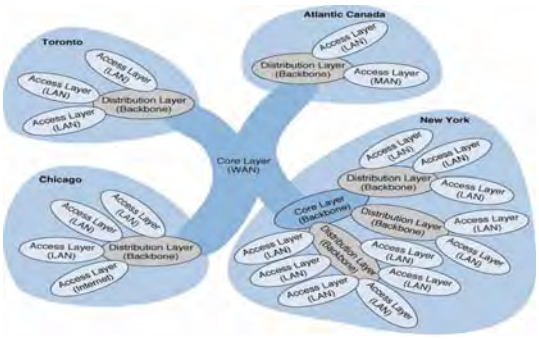
Needs Analysis

- The first step is to analyze the needs of network users along with the requirements of network applications.
- Most efforts today involve upgrades and not new network designs, so most needs may already be understood.
- LAN and BN design issues include improving performance, upgrading or replacing unreliable or ageing equipment, or standardizing network components to simplify network management.
- At the MAN/WAN level, circuits are leased and upgrades involve determining if capacity increases are needed.
- The object of needs analysis is to produce a logical network design, which describes what network elements will be needed to meet the organization's needs.

Geographic Scope (Figure 11-3)

- Needs analysis begins by breaking the network into three parts based on their geographic and logical scope:
  - The access layer which lies closest to the user
  - The distribution layer which connects the access layer to the rest of the network
  - The core layer which connects the different parts of the distribution layer together.

Figure 11-3 Geographic Scope



Application Systems

- The designers must review the applications currently used on the network and identify their location so they can be connected to the planned network (*baselining*).
- Next, applications expected to be added to the network are included.
- It is also helpful to identify the hardware and software requirements and protocol type for each application.

Network Users

- In the past, application systems accounted for the majority of network traffic. Today, much network traffic comes from Internet use (i.e. e-mail and WWW).
- The number and type of users that will generate network traffic may thus need to be reassessed.
- Future network upgrades will require understanding how the use of new applications, such as video, will effect network traffic.

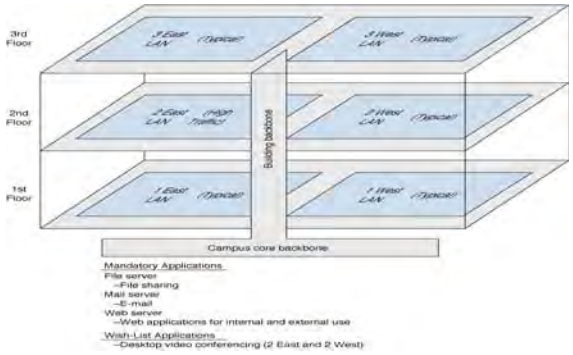
Categorizing Network Needs

- The next step is to assess the traffic generated in each segment, based on an estimate of the relative magnitude of network needs (i.e. *typical* vs. *high volume*). This can be problematic, but the goal is a relative understanding of network needs.
- Once identified, network requirements should be organized into *mandatory requirements*, *desirable requirements*, and *wish-list requirements*.

Deliverables

- The key deliverable for the needs assessment stage is a set of network maps, showing the applications and the circuits, clients, and severs in the proposed network, categorized as “typical” or “high volume”.

Fig. 11-4 Logical Network Design



Technology Design

- After needs assessment has been completed, the next design phase is to develop a technology design (or set of possible designs) for the network.

Designing Clients and Servers

- For the technology design, the idea behind the building block approach is to specify the computers needed in terms of standard units.
- “Typical” users are allocated “base level” client computers, as are servers supporting “typical” applications.
- “High volume” users and servers are assigned “advanced” computers.
- The definition for a standard unit, however, keeps changing as hardware costs continue to fall.

Designing Circuits and Devices

- Two interrelated decisions in designing network circuits and devices are: 1) deciding on the fundamental technology and protocols and 2) choosing the capacity each circuit will operate at.
- Capacity planning means estimating the size and type of the "standard" and "advanced" network circuits for each type of network.
- This requires some assessment of the current and future circuit loading in terms of average vs. peak circuit traffic.

Estimating Circuit Traffic

- The designer often starts with the total characters transmitted per day per circuit, or if possible, the maximum number of characters transmitted per two second interval if peak demand must be met.
- While no organization wants to overbuild its network and pay for unneeded capacity, going back and upgrading a network often significantly increases costs.

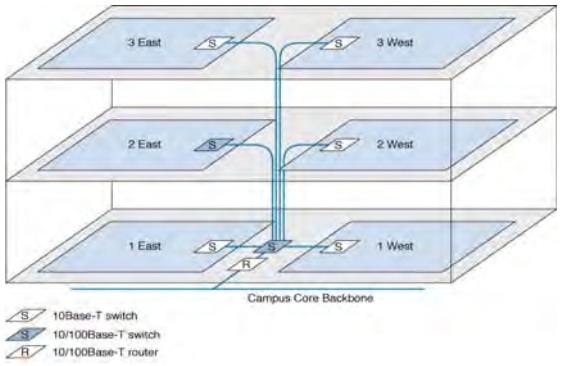
Network Design Tools

- Network modeling and design tools can perform a number of functions to help in the technology design process.
- Some modeling tools require the user to create the network map from scratch. Other tools can "discover" the existing network.
- Once the map is complete, the next step is to add information about the expected network traffic and see if the network can support the level of traffic that is expected. This may be accomplished through simulation models.
- Once simulation is complete, the user can examine the results to see the estimated response times and throughput.

Deliverables

- The key deliverables at this point are a revised set of network maps that include general specifications for the hardware and software required.
- In most cases the crucial issue is the design of the network circuits.

Fig. 11-5 Physical Network Design



Cost Assessment

- Cost assessment's goal is to assess the costs of various network alternatives produced as part of technology design. Costs to consider include:
  - Circuit costs for both leased circuits and cabling.
  - Internetworking devices such as switches and routers.
  - Hardware costs including servers, memory, NICs & UPSs.
  - Software costs for operating systems, application software and middleware.
  - Network management costs including special hardware, software, and training.
  - Test and maintenance costs for monitoring equipment and supporting onsite repairs.
  - Operations costs to run the network.

Request for Proposal (RFP)

- While some components can be purchased "off-the-shelf", most organizations develop an RFP before making large network purchases.
- The RFP creates a competitive environment for providing network equipment and services.
- Once vendors have submitted network proposals, the organization evaluates them against specific criteria and selects the winner(s).
- Multi-vendor selections have the advantage of maintaining alternative equipment and services sources, but are also more difficult to manage.

Request for Proposal

- Background Information
  - Organizational profile; Overview of current network; Overview of new network; Goals of the new network
- Network Requirements
  - Choice sets of possible network designs (hardware, software, circuits); Mandatory, desirable, and wish list items, Security and control requirements; Response time requirements; Guidelines for proposing new network designs
- Service Requirements
  - Implementation time plan; Training courses and materials; Support services (e.g., spare parts on site); Reliability and performance guarantees
- Bidding Process
  - Time schedule for the bidding process; Ground rules; Bid evaluation criteria; Availability of additional information
- Information Required from Vendor
  - Vendor corporate profile; Experience with similar networks; Hardware and software benchmarks; Reference list

Selling the Proposal to Management

- An important hurdle to clear in network design is obtaining the support of senior management.
- Gaining acceptance from senior management lies in speaking their language and presenting the design in terms of easily understandable issues.
- Rather than focusing on technical issues such as upgrading to gigabit Ethernet, it is better to make a business case by focusing on organizational needs and goals such as comparing the growth in network use with the growth in the network budget.

Deliverables

- There are three key deliverables for this step:
  - 1. An RFP issued to potential vendors.
  - 2. After the vendor has been selected, the revised set of network maps including the final technology design, complete with selected components.
  - 3. The business case written to support the network design, expressed in terms of business objectives.

Encoding Techniques

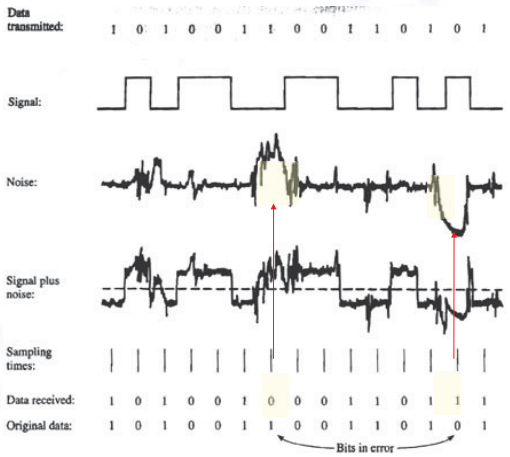
Slide Set 8

Terminology

- **Unipolar Signals**
  - Binary data represented by signals of the *same* polarity, e.g. 0 -> +5 V, 1 -> +10 V ⇒ DC content
- **Bipolar (Polar) Signals**
  - Binary data represented by signals of *opposite* polarity, e.g. 0 -> +5 V, 1 -> -5 V ⇒ ideally Zero DC content
- **Mark and Space**
  - Binary 1 and Binary 0 respectively
- **Duration of a bit (T_b)**
  - Time taken for transmitter to emit a data bit
- **Data rate, R (= $1/T_b$)**
  - Rate of data transmission measured in **bits per second (bps)**
- **Duration of a Signal Element (T_s)**
  - Minimum duration of a signal pulse
- **Modulation (signaling) rate, D ($1/T_s$)**
  - Rate at which the signal level changes with time measured in **bauds = signal elements per second**

Not always Tb = Ts !!!
e.g. Multi-symbol transmission (M = 4, 8, ...): Tb < Ts

Interpretation of the Received Signal



Encoding Schemes

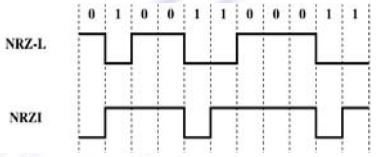
Schemes for encoding digital data as digital signals

- **Non-return to Zero** (NRZ) Group:
  - Non-return to Zero-Level (NRZ-L)
  - Non-return to Zero Inverted (NRZ-I)
- **Multi-level Binary** Group:
  - Bipolar-AMI (Alternate Mark Invert)
  - Pseudoternary
- **Bi-Phase** (RZ) Group:
  - Manchester
  - Differential Manchester
- **Scrambling** Group:
  - B8ZS (Bipolar with 8-Zeros Substitution)
  - HDB3 (High Density Bipolar 3-Zeros)

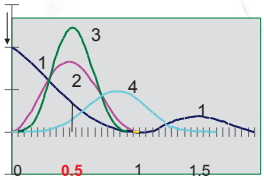
Aspects of comparison between schemes

- **Clocking:** Synchronizing RX to TX can be achieved using:
  - An external clock, or better:
  - A built-in synchronizing mechanism in the **signal** itself! (so, a code with many signal transitions is better)
- **Error detection**
  - Mostly handled by higher layers, e.g. data-link control
  - But error detection capabilities built into the signal encoding scheme would help!
    Advantage: Implemented much faster (in hardware)
- **Performance with interference and noise**
  - Some encoding schemes perform better than others: e.g. with differential encoding: data is encoded as signal transition/no signal transition, and data detection at RX is **less affected by noise.**
- **Cost and complexity**
  - Some codes require signaling at a rate greater than the data rate (e.g. RZ) At higher signaling rates this requires higher bandwidth, faster circuits, etc. (larger costs)

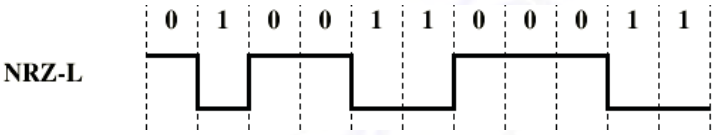
NRZ Group Pros and Cons:



- Pros
  - Easy to implement
  - Modest bandwidth requirements
- Cons
  - Large DC component
  - Poor TX-RX synchronization:
    e.g. **No signal transitions for long strings of 0's or 1's** (so few edges are available for synchronization)
- Used for magnetic recording
- Not used much for signal transmission

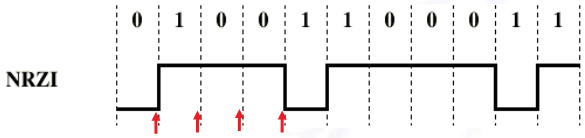


NRZ-L: Non-return to Zero Level



- Two different signal voltages for the 0 and 1 data bits
- Voltage level is constant (no return to zero, so no signal transition) for the full duration of the data bit interval
- e.g. positive voltage for space and 0V for mark
- More often, negative voltage for one data value and positive for the other (bipolar signal) (Why?)
- An example of absolute encoding: Mapping data **directly** to signal **levels**

NRZ-I: Non-return to Zero Invert

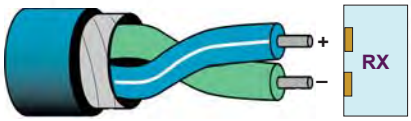


- Still constant voltage level for bit duration of (hence NRZ)
- But data is encoded as presence or absence of signal transition at the beginning of bit time:
  - Transition (low to high or high to low): Denotes binary 1
  - No transition: Denotes binary 0
- This is an example of differential encoding:Encoding data as a change/no change in signal level.

Differential Encoding

- Data is represented by signal transitions rather than signal levels
- Advantages;
  - With noise, signal transitions (or lack of them) are detected more easily than signal levels ⇒ Better noise immunity
  - In complex transmission layouts, it is easy to accidentally lose sense of polarity

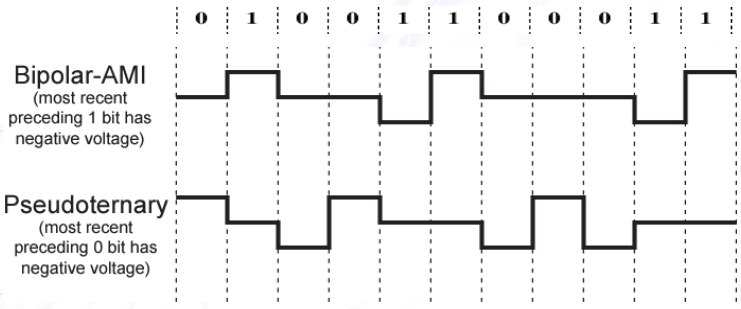
Effect of swapping terminals on:
- **NRZ-L**
- **NRZI**



The Multilevel Binary Group

- Uses more than two signal levels (3 in this case)
- Signal is multi-level but data is still binary!
- Bipolar-AMI (Alternate Mark (1) Inversion)
  - 0 data is represented by no line signal
  - 1 data represented by positive or negative pulse
  - The "1" pulses alternate in polarity (why? 2 reasons!)
  - Advantages:
    - No net DC component (for any data sequence!)
    - Lower bandwidth than NRZ
    - No loss of sync with a long string of 1'z (but zeros still a problem- Will try to solve it later)
    - Alteration of pulse polarity also useful for error detection

Bipolar-AMI and Pseudoternary



Pseudoternary

- Opposite of Bipolar-AMI:
  - 1 represented by no line signal
  - 0 represented by alternating positive and negative pulses
- Could be called Bipolar-ASI: (Why?)
- No advantage or disadvantage over bipolar-AMI

The Multilevel Binary Group: Advantages

- No net DC component
- Spectrum centered at the middle of the BW
- Lower bandwidth than NRZ
- No loss of sync with a long string of 1'z (but zeros still a problem- Will try to solve it later)
- Alteration of pulse polarity also useful for error detection.

Disadvantages of Multilevel Binary

$N = \text{Log}_2 (M)$

No. of bits sent during each signal element

No. of signal levels used

- Coding scheme not as efficient as NRZ:
  - We send only one bit at a time (1 or 0 data) ⇒ Only $M = 2^1 = 2$ signal levels should be enough, but we are sending 3 levels > 2 !
  - We use 3 levels ⇒ Enough to represent $\log_2 3 = 1.58$ bits > 1 bit !
- Receiver Design and Noise Performance
  - Now receiver must distinguish between three signal levels (+A, -A, 0) ⇒ Need better receiver design
  - Requires approximately 3dB higher SNR for the same probability of bit error (bit error rate)

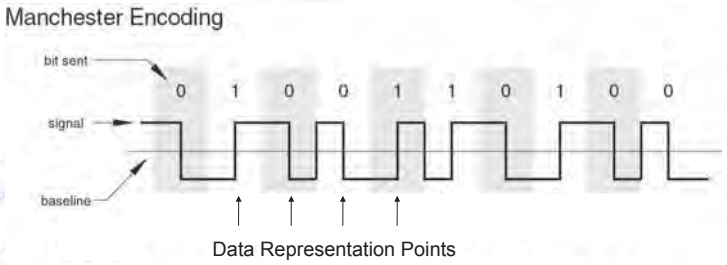
The Biphase Group (2 signal phases per bit)

- Manchester
  - Transition in middle of each bit period
  - Transition serves both as a clock edge and data representation
    - Low to high represents 1
    - High to low represents 0
  - Used by the IEEE 802.3 specification for Ethernet LAN (short distances)
- Differential Manchester
  - Dedicated mid-bit transition used **only** for clocking
  - Data representation is at start of bit:
    - No transition at start of a bit period represents 1
    - Transition at start of a bit period represents 0 (Inverts on 0's – opposite of NRZ-I)
  - An example of differential encoding
  - Used by IEEE 802.5 specification for Token Ring LAN

Manchester Encoding

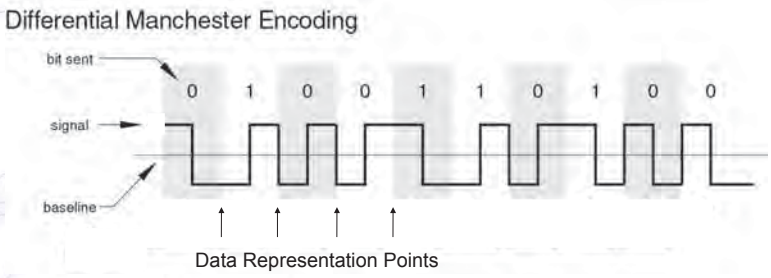
- **Mandatory transition in middle of each bit period**
  - **→ Low to high represents 1**
  - **→ High to low represents 0**
- **Transitions at start of bit only where required**

Note: This is not differential



Differential Manchester Encoding

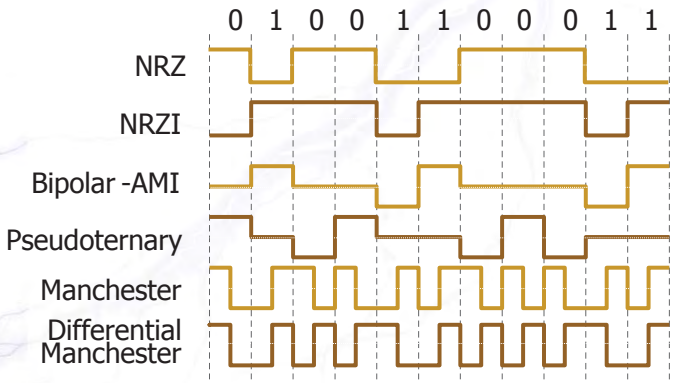
- **Mandatory mid-bit transition for clocking**
- **Data represented by transition or no transition at bit start:**
  - **→ Transition (either direction) represents 0 (Invert on zeros)**
  - **→ No transition represents 1**



Biphase Pros and Cons

- Pros
  - Guaranteed mid bit transitions
    - Synchronization facility (self clocking codes)
  - Ideally no dc component (using bipolar signals)
  - Error detection
    - Detecting absence of expected (mandatory) transitions
- Cons
  - At least one transition per bit time and possibly two
    - Modulation (signaling) rate as high as twice that of NRZ
    - So, requires more bandwidth
    - Therefore, used over shorter distances (in LANs)

1. Digital data, Digital signal Encoding



Scrambling Group: B8ZS, HDB3

- Use bit scrambling to replace data bit sequences that would otherwise produce a constant signal voltage, with a more appropriate bit sequence producing signal changes
- Helps overcome constant DC problems with Multilevel Binary codes (poor synchronization)
- So, a "filling" (replacement) bit sequence is inserted where necessary
- Criteria for a "Filling sequence"
  - Should produce enough transitions for synchronization
  - Must be recognized by receiver for replacement with original data
  - Not likely to be generated by noise (difficult for noise/interference to produce it)
  - Should occupy the same bit length as original data (so no extra overhead in the data rate)

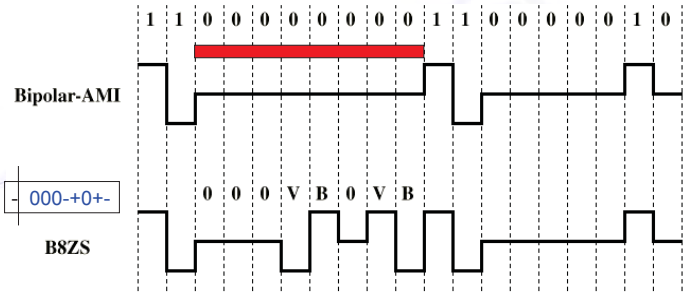
Scrambling Group: B8ZS, HDB3

- Advantages:
  - No long sequences of zero level line signal
  - No DC component
  - No reduction in useful data rate (No extra data sent)
  - Built-in error detection capability

B8ZS

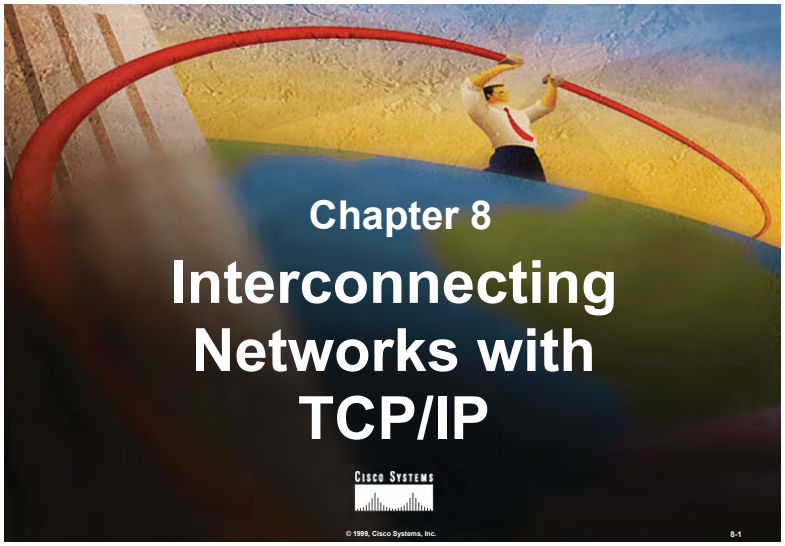
- Bipolar With 8 Zeros Substitution
- Improvement on bipolar-AMI
- If an octet of 8 zeros and the last pulse preceding was positive (+):Transmitter encodes the 8 zeros as 000+-0-+
  (how many level changes does this introduce?)
- If an octet of 8 zeros and last voltage pulse preceding was negative (-): Transmitter encodes as 000-+0+-
  (shown in Fig. 5.6)
- Each insertion has *two* intentional violations of the basic AMI code rule: (violations alternate in polarity- no net DC added)
  +000+-0-+
  -000-+0+-
- A strange event ⇒ unlikely to be caused by noise
- Receiver should detect it and interpret as an octet of 8 zeros (original data)
- No additional data sent ⇒ No penalty on genuine data rate

B8ZS

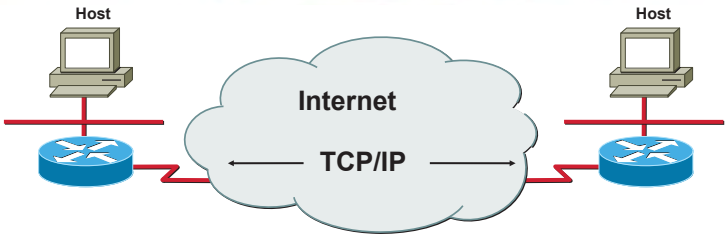


V: Violation
B: Bipolar (Valid)

See how the insertion satisfies the 5 requirements:
-Detectable at RX
-Difficult for noise to generate
-Introduces transitions
-Does not introduce DC (alternate violations)
-Error detection capability



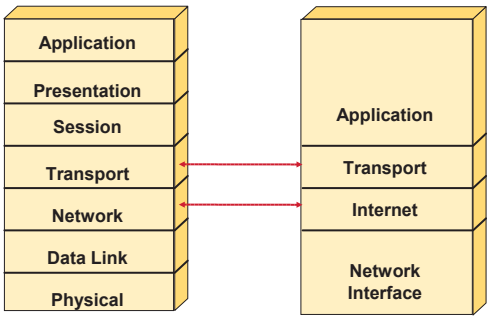
Introduction to TCP/IP



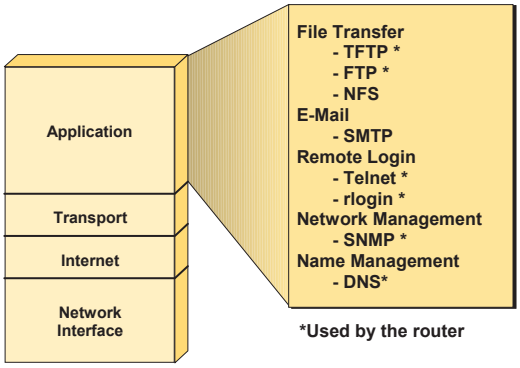
Early protocol suite

Universal

TCP/IP Protocol Stack

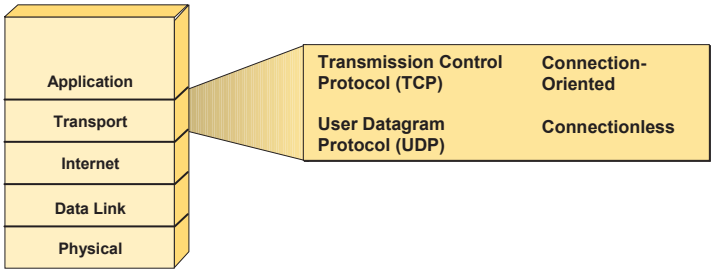


Application Layer Overview

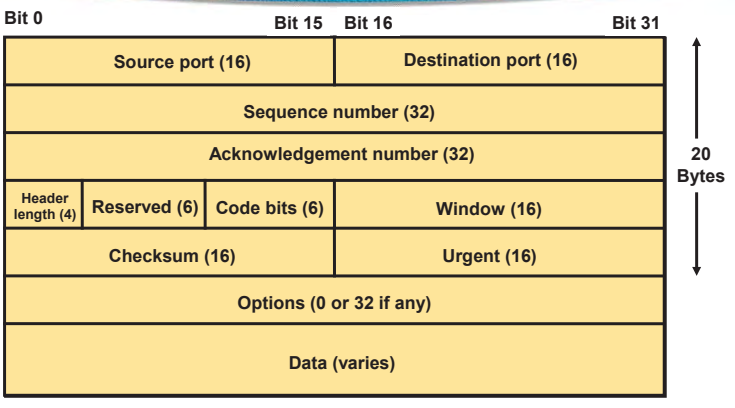


*Used by the router

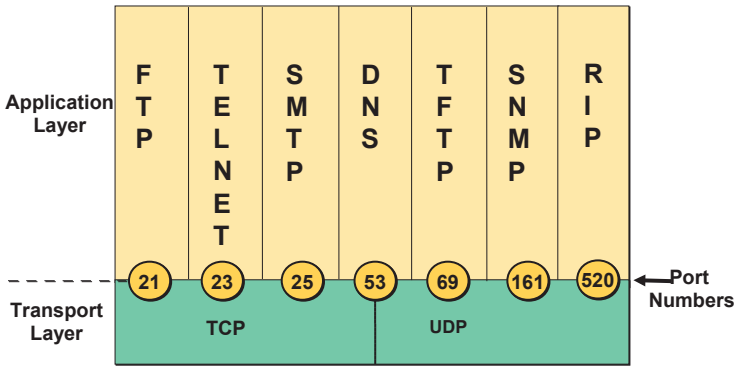
Transport Layer Overview



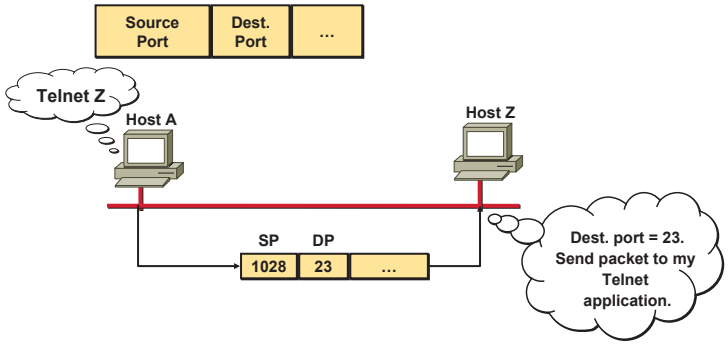
TCP Segment Format



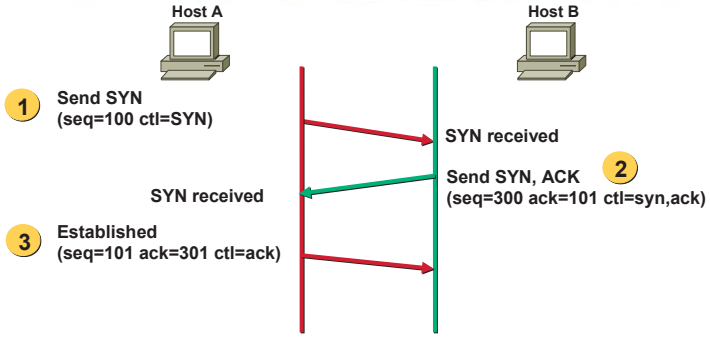
Port Numbers



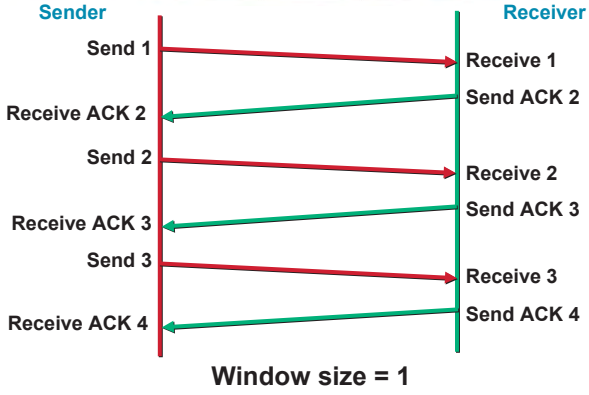
TCP Port Numbers



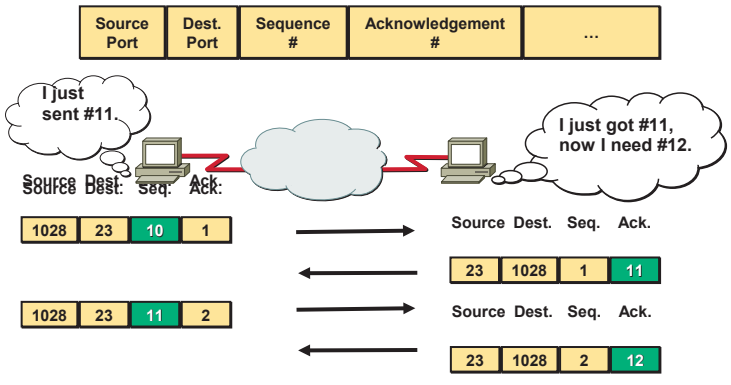
TCP Three Way Handshake/Open Connection



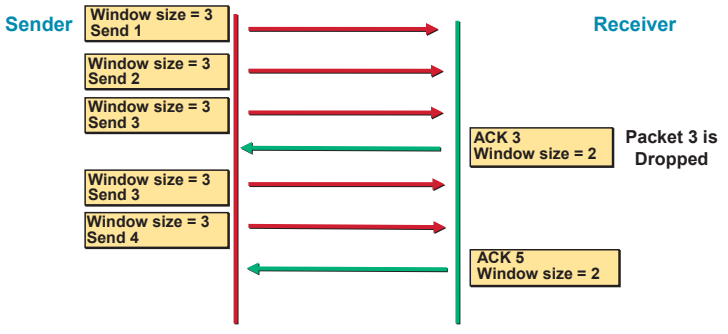
TCP Simple Acknowledgment



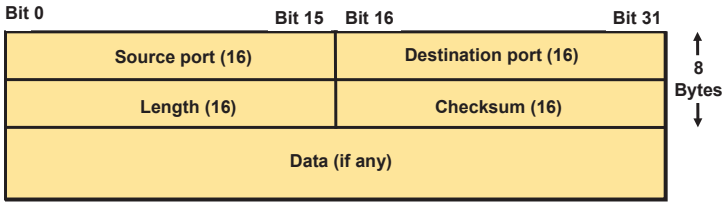
TCP Sequence and Acknowledgment Numbers



TCP Windowing

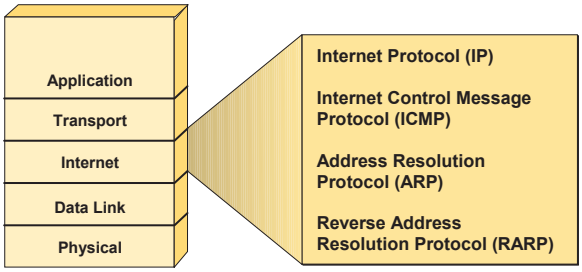


UDP Segment Format



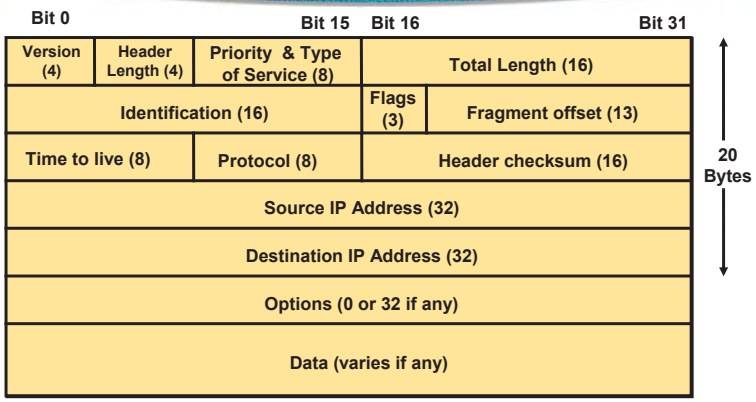
No sequence or acknowledgment fields

Internet Layer Overview

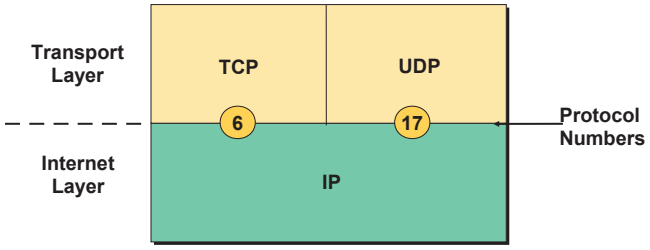


OSI network layer corresponds to the TCP/IP internet layer

IP Datagram

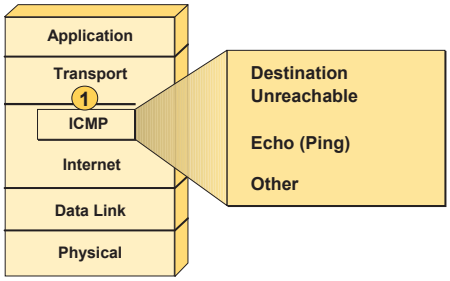


Protocol Field

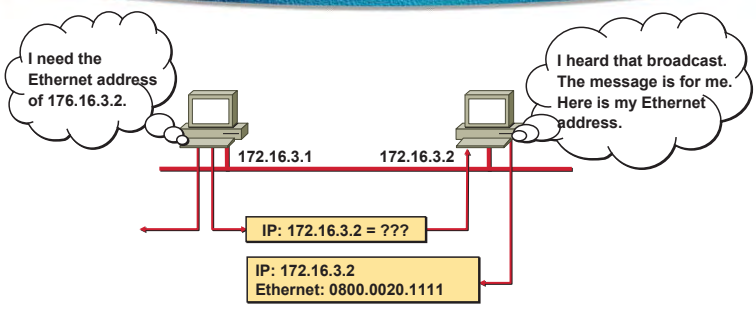


Determines destination upper-layer protocol

Internet Control Message Protocol



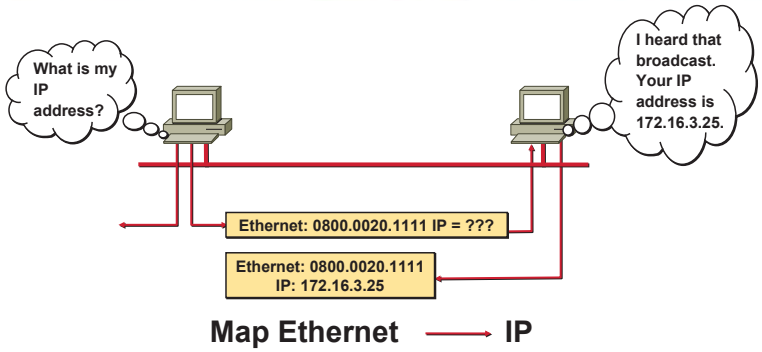
Address Resolution Protocol



Map IP → Ethernet

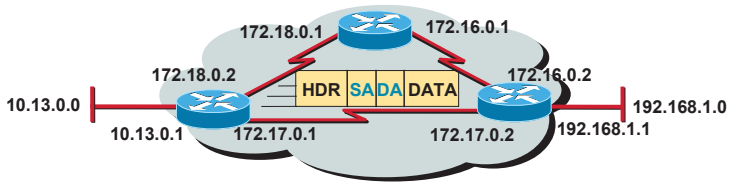
Local ARP

Reverse ARP



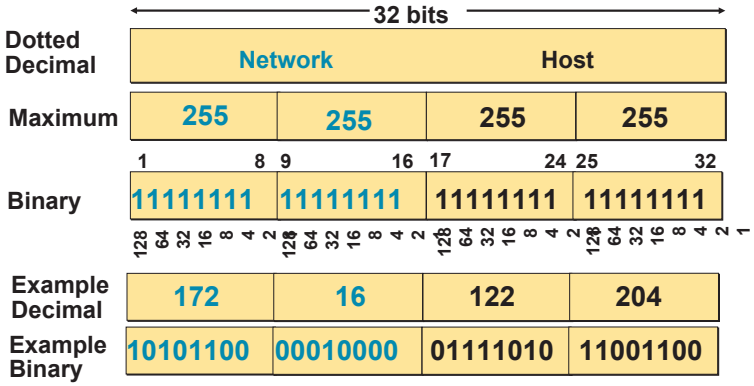
Map Ethernet → IP

Introduction to TCP/IP Addresses

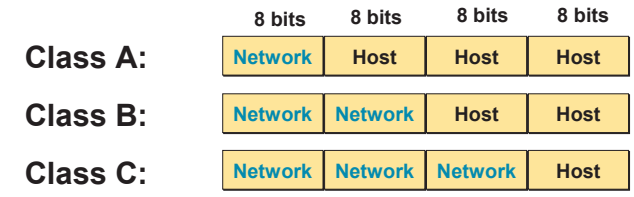


- Unique addressing allows communication between end stations
- Path choice is based on location

IP Addressing



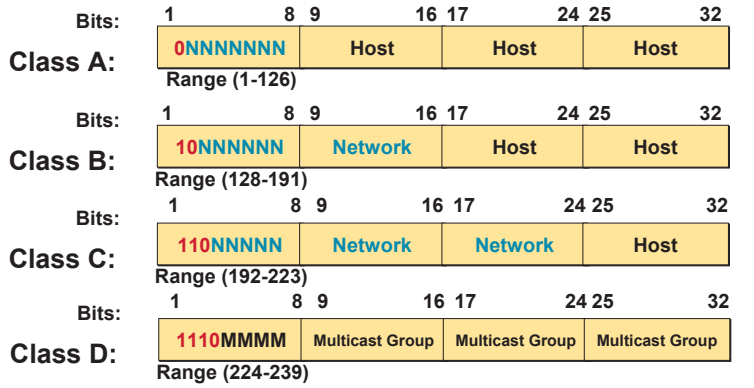
IP Address Classes



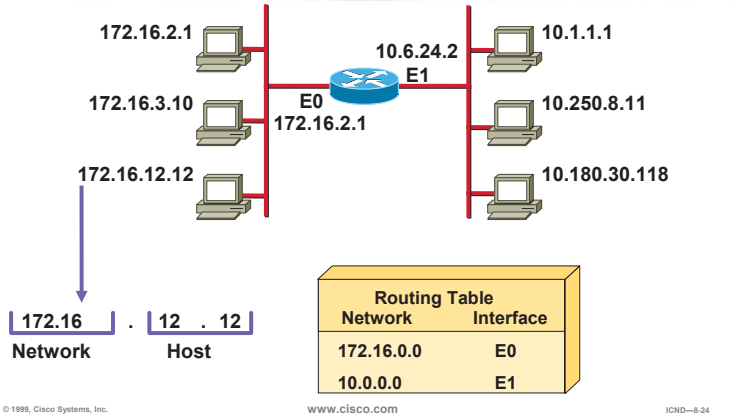
Class D: Multicast

Class E: Research

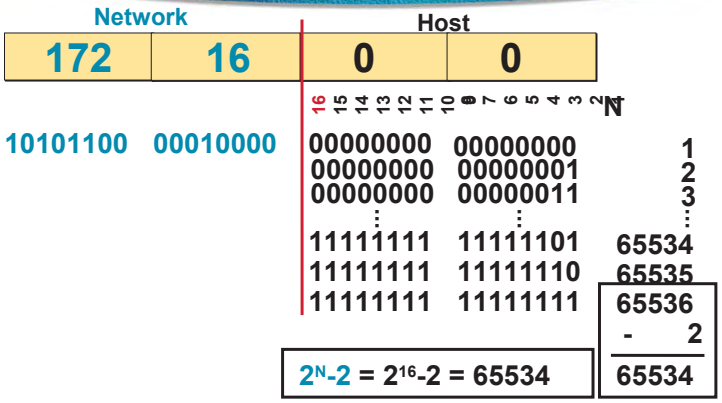
IP Address Classes



Host Addresses



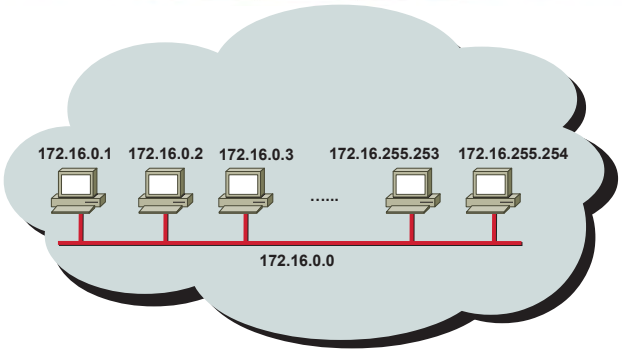
Determining Available Host Addresses



IP Address Classes Exercise Answers

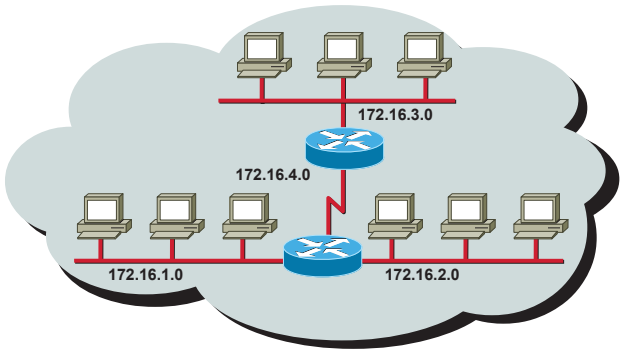
Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
241.257.201.10			

Addressing without Subnets



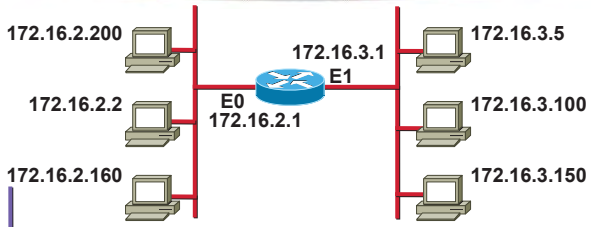
Network 172.16.0.0

Addressing with Subnets



Network 172.16.0.0

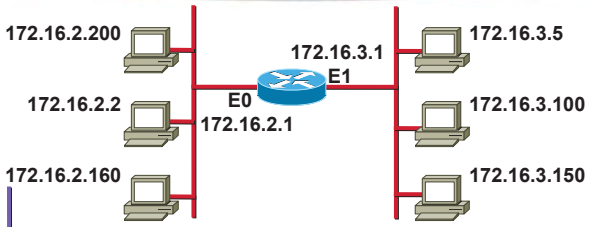
Subnet Addressing



172.16 . 2 . 160
Network Host

New Routing Table Network	Interface
172.16.0.0	E0
172.16.0.0	E1

Subnet Addressing



172.16 . 2 . 160
Network Subnet Host

New Routing Table Network	Interface
172.16.2.0	E0
172.16.3.0	E1

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.

Decimal Equivalents of Bit Patterns

128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	=	0
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

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

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

Network number extended by eight bits

Subnet Mask with Subnets (cont.)

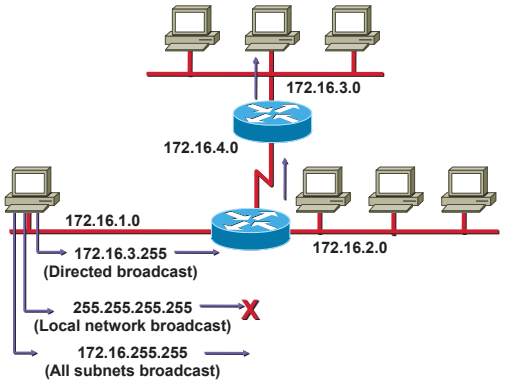
	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
Network Number	172	16	2	128

Network number extended by ten bits

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		

Broadcast Addresses



Addressing Summary Example

	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10 100000	Host 1
255.255.255.192	11111111	11111111	11111111	11 000000	Mask 2
172.16.2.128 8	10101100	00010000	00000010	10 000000	Subnet 4
172.16.2.191 9	10101100	00010000	00000010	10 111111	Broadcast 5
172.16.2.129	10101100	00010000	00000010	10 000001	First 6
172.16.2.190	10101100	00010000	00000010	10 111110	Last 7

3

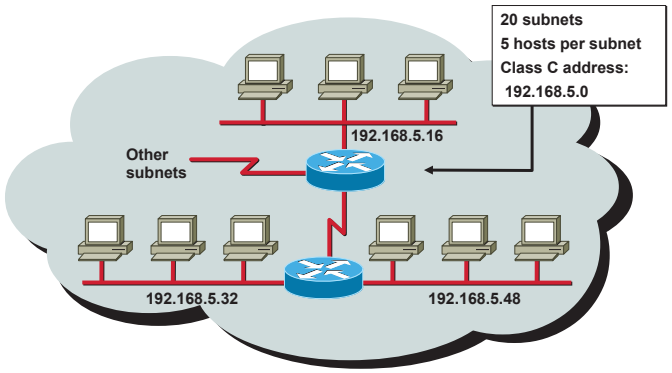
Class B Subnet Example

IP Host Address: 172.16.2.121
Subnet Mask: 255.255.255.0

	Network	Network	Subnet	Host
172.16.2.121:	10101100	00010000	00000010	01111001
255.255.255.0:	11111111	11111111	11111111	00000000
Subnet:	10101100	00010000	00000010	00000000
Broadcast:	10101100	00010000	00000010	11111111

Subnet Address = 172.16.2.0
Host Addresses = 172.16.2.1–172.16.2.254
Broadcast Address = 172.16.2.255
Eight bits of subnetting

Subnet Planning



Class C Subnet Planning Example

IP Host Address: 192.168.5.121
Subnet Mask: 255.255.255.248

	Network	Network	Network	Subnet	Host
192.168.5.121:	11000000	10101000	00000101	01111001	
255.255.255.248:	11111111	11111111	11111111	11111000	
Subnet:	11000000	10101000	00000101	01111000	
Broadcast:	11000000	10101000	00000101	01111111	

Subnet Address = 192.168.5.120
Host Addresses = 192.168.5.121–192.168.5.126
Broadcast Address = 192.168.5.127
Five Bits of Subnetting

Broadcast Addresses Exercise Answers

Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248			
15.16.193.6	255.255.248.0			
128.16.32.13	255.255.255.252			
153.50.6.27	255.255.255.128			

Group Network Design Assignment

BCIS/24A/PT
CAN2120C- CN

This assignment is worth 25% of the total marks for this module. The deadline for this assignment is **6th August 2024 at 11:59 pm**. Group Leader need to upload the assignment for his/her group in pdf format at bcis24apt@rishiheerasing.net for that purpose**.**

Objectives

In this assignment, you are required to design a network solution for a typical organisation that requires its users to communicate internally and externally.

Organisation Requirements

A new educational institute **LearnIT** has just opened up with the aim of offering IT related courses to its students. It shall host student computer labs as well as host its website and other online services on premises. The institute has subscribed to a 100 Mbps Internet connection and was granted a **block of global IP address: 202.123.21.120 /29** from its ISP.

It terms of infrastructure; the institute shall require the following:

- A server to host the institute's website and another server for the Learning Management System (LMS) on which students can access course materials from home. Each of these shall be reached on a different sub-domain names e.g. **www.LearnIT.com** and **lms.LearnIT.com** respectively. Other servers might be procured wherever necessary.
- The institute wants to set up **five** computer labs, each containing **20 PCs** on **static IP addressing**, each having **restricted** internet connectivity.
- Additionally, **one network point** on dynamic IP addressing shall be available in each of the five classrooms and are to be used by the lecturers for connecting their laptops. These **five network points** require **unrestricted** internet connectivity.
- **Three PCs** will be given to the system administrator in the Server Room for network and system management purposes. Also, **one PC** will be made available for **each of the three administrative staff** and **each of the three Teaching Assistants** (TA).
  Note: The **staff PCs** should have **unrestricted Internet connectivity** but the **TA PCs** must have **internal network access** (website and LMS) **only**.
- Finally, a secured wireless network should be made available to students over the campus which can allow students **internal access to the LMS and web server** but with **restricted access** to the Internet.

Your task is to come up with a logical, efficient and scalable network design that will be suitable for this institute. The institute has allowed an adequate budget to purchase any equipment that may be required. There is currently no network or hardware infrastructure present apart for the ISP's modem/router in the Server Room.

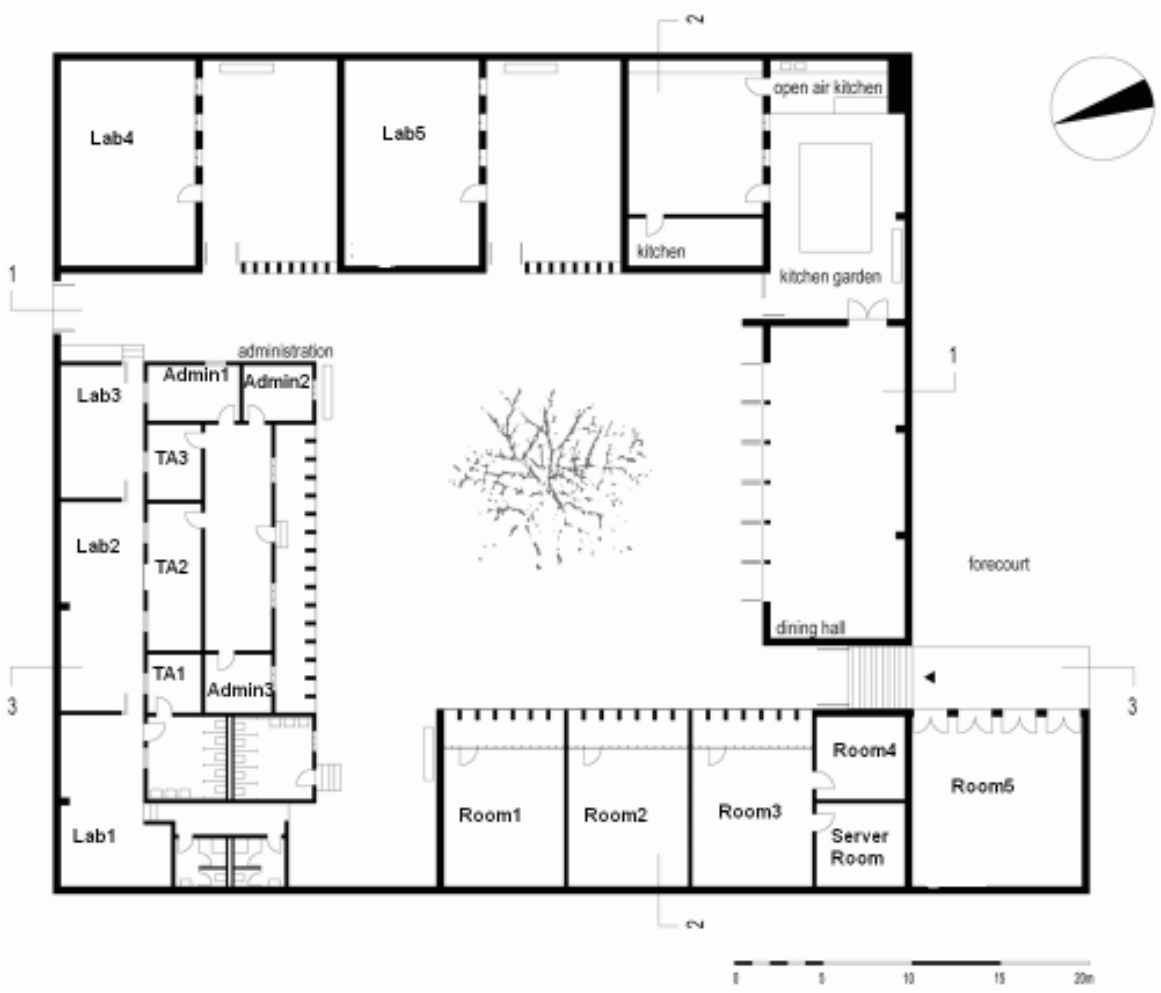
Design Details

When drawing up your network designs make sure you split the design up in a way that emphasizes the function of the components. Keep the design as simple as possible allowing efficient troubleshooting while guaranteeing the least downtime in the system. Always split up networks in terms of function, since PCs with similar function most probably will often communicate between themselves. You are free to use some form of physical subnetting or use VLANs. Also do not forget about the ISP link in the Server Room !!!

Deliverables

Build a report giving all the necessary network designs (logical and physical network diagrams should be provided that will allow any technician to build your network structure from scratch). You are free to use any network case tool for the designs and this should be incorporated in your report. You will also need to provide all the configuration information for all client, servers, circuits and devices that you find pertinent in your solution.
Additionally, you will have to perform a cost-assessment and come up with a tentative budget for your solution. Your solution should address any security issues.

Institute Layout



UNIVERSITY of TECHNOLOGY, MAURITIUS

BSc (Hons) Computing & Information Systems (Top-Up)

BCIS/22A/PT

Examinations for 2022 / Semester 1

MODULE: COMMUNICATION & NETWORKING

MODULE CODE: CAN2120C

DURATION: 2½ Hours

READING TIME: None

Instructions to Candidates

1. Answer **ALL FOUR** questions
2. Each question carries equal marks
3. Always start a new question on a fresh page
4. Total marks: **100**
5. Use of silent calculators is allowed in the Examination Room
6. Appendix is provided

This examination paper contains 4 questions and consists of 6 pages.

ATTEMPT ALL FOUR QUESTIONS

Question 1: (25 marks)

(a) State **two** popular electronic mail **access** protocols?

(3 marks)

(b)

i. What is DNS?

ii. Briefly, describe what it does and how it works?

iii. Why does DNS use a distributed approach as opposed to a single server?

(2+3+2 marks)

(c) HTTP supports both non-persistent and persistent connections. Describe each type of connection and state which HTTP protocol version supports each type?

(6 marks)

(d) Assume that a new application layer protocol is developed for a video conferencing application. Which transport layer protocol do you think will be more suitable and why?

(3 marks)

(e) FTP is a popular application layer protocol for transferring data between an FTP client and an FTP server. Give three advantages of using FTP for data transfer.

(6 marks)

Question 2: (25 marks)

(a) Describe what you understand by flow control in relation to a connection-oriented protocol such as TCP.

(5 marks)

(b) Describe the steps involved in a TCP connection establishment?

(3 marks)

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

i. Give the format of Class C address and a type of network it is most suited for.

ii. Give two advantages of creating subnets within a larger network.

Iii. On an isolated network, two hosts have been configured to work on the same subnet with IP addresses 10.10.201.254 and 10.15.201.254. Can this configuration work? What could the subnet mask be?

iv. Give four differences between IPv4 and IPv6?

(3+3+4+4 marks)

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

i. DHCP

ii. ICMP

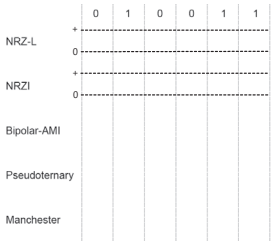
iii. ARP

(3 marks)

Question 3 (25 marks)

(a) For bit pattern **010011**, sketch the waveforms for each of the code indicated.

Assume that space is positive for NRZ-L; the voltage for the previous bit for NRZ-I was mark and was positive; the most recent preceding mark for AMI had a negative voltage; the most recent preceding space for pseudoternary had a negative voltage.



(10 marks)

(b) Describe fully how you can use a (11/7) **Hamming code** to:

(i) detect and;

(ii) correct;

if the following codeword is received: **10101010100**

(5 marks)

(c) Explain the purpose of the **ident** and **offset** fields in an IPv4 packet header. Hence, sketch the fragmentation process that will occur if an initial **4200** bytes datagram is to be transmitted in a network with a **MTU** size of **1500** bytes.

(Pay attention to the values of the above fields in the IP fragments.)

(5 marks)

(d) State **five** network security services.

(5 marks)

Question 4 (25 marks)

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

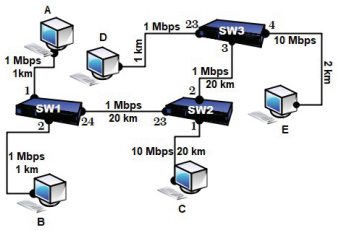
(i) Outline **two** popular flavours of this standard. Give the operating frequency, typical indoor range and maximum speed of each flavour.

(ii) What are the **two** main 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+2+2 marks)

(b) The diagram below shows a network layout consisting of five hosts A to E with three switches SW1, SW2 and SW3 connecting them. The bandwidth and length of the links are as shown below:



(i) Calculate the ***one-way latency*** if **Host A** has to send 1500 bytes of data to **Host E** with all the switches operating in ***Store-N-Forward*** mode and has a switching time of 1 millisecond per 100 bytes of data and assuming that the average speed of the signal in the links is $2x10^8$ m/s.

(5 marks)

(Please Turn Over)

(ii) Assume that the forwarding table of the above switches are empty initially: Give the forwarding tables for each of the three switches after the four consecutive transmissions below:

1. Host A to Host E
2. Host D to Host A
3. Host E to Host C
4. Host C to Host D

(6 marks)

(c) Please find below a packet capture. Extract the **source MAC address**, the **destination IP address** in quad dotted decimal, the **source port number** and the **window size** for the segment. Deduce the **application layer protocol** used.

```
565f 01ef 5cd2 dada 4b4c ac37 84ef 187c 1460 0800
4500 0040 b3d4 4000 4006 ef77 c0a8 010c 4260 9357
cdce 0015 7a3e b548 aeb5 5018 faa2 af8f 0000 5553
4552 2072 6973 6869 6865 6572 6173 696e 676e 6574
```

(1+2+2+1+1 marks)

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

UNIVERSITY of TECHNOLOGY, MAURITIUS

BSc (Hons) Computing & Information Systems (Top-Up)

BCIS/23B/PT

Examinations for 2023-24 / Semester 1

MODULE: COMMUNICATION & NETWORKING

MODULE CODE: CAN2120C

DURATION: 2½ Hours

READING TIME: None

Instructions to Candidates

1. Answer **ALL FOUR** questions
2. Each question carries equal marks
3. Always start a new question on a fresh page
4. Total marks: **100**
5. Use of silent calculators is allowed in the Examination Room
6. Appendix is provided

This examination paper contains 4 questions and consists of 6 pages.

ATTEMPT ALL FOUR QUESTIONS

Question 1: (25 marks)

(a) SMTP is the most popular electronic mail protocol. Describe briefly the protocol and how it works?

(3 marks)

(b)

i. What is DNS?
ii. Briefly, describe what it does and how it works?
iii. Why does DNS use a distributed approach as opposed to a single server?

(2+3+2 marks)

(c) HTTP supports both non-persistent and persistent connections. Describe each type of connection and state which HTTP protocol version supports each type?

(6 marks)

(d) Assume that a new application layer protocol is being developed for a video conferencing application. Which transport layer protocol do you think will be more suitable and why?

(3 marks)

(e) FTP is a popular application layer protocol for transferring data between an FTP client and an FTP server. Give three advantages of using FTP for data transfer.

(6 marks)

Question 2: (25 marks)

(a) Describe what you understand by flow control in relation to a connection-oriented protocol such as TCP.

(5 marks)

(b) Describe the steps involved in a TCP connection establishment?

(3 marks)

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

i. Give the format of Class D addresses and what are they usually used for.
ii. Give two advantages of creating subnets within a larger network.
iii. On an isolated network, two hosts share a subnet mask of 255.255.240.0 with IP addresses 130.12.206.254 and 130.12.216.254. Can the two hosts communicate directly with this configuration? Justify your answer?
iv. Give four differences between IPv4 and IPv6?

(3+3+4+4 marks)

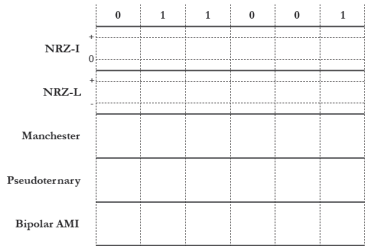
(d) Describe very briefly the purpose of the following protocols:
i. DHCP
ii. ICMP
iii. ARP

(3 marks)

Question 3: (25 marks)

(a) For bit pattern **011001**, sketch the waveforms for each of the code indicated.

Assume: that space was negative for NRZ-L; voltage for the previous mark for NRZ-I was positive; most recent preceding mark for AMI had a positive voltage; the most recent preceding space for pseudoternary had a negative voltage.



(10 marks)

(b) Describe fully how you can use a (11/7) **Hamming code** to:
(i) detect and;
(ii) correct;
a **message M** if the following **codeword** is **received**: **10101010100**

(5 marks)

(c) Explain the purpose of the **ident** and **offset** fields in an IPv4 packet header. Hence, sketch the fragmentation process that will occur if an initial **4200** bytes datagram is to be transmitted in a network with a **MTU** size of **1500** bytes.

(Pay attention to the values of the above fields in the IP fragments.)

(5 marks)

(d) State **five** network security services.

(5 marks)

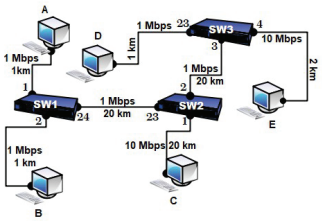
Question 4 (25 marks)

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

(i) Outline **two** recent flavours of this standard. Give the operating frequency, typical indoor range and maximum speed of each flavour.
(ii) What are the **two** main modes of operation of this standard and explain the difference between the two.
(iii) Mention **one** security issue with this wireless technology and explainhow this issue can be addressed.

(3+2+2 marks)

(b) The diagram below shows a network layout consisting of five hosts A to E with three switches SW1, SW2 and SW3 connecting them. The bandwidth and length of the links are as shown below:



(i) Calculate the ***one-way latency*** if **Host A** has to send 1000 bytes of data to **Host E** with all the switches operating in ***Store-N-Forward*** mode and has a switching time of 10 millisecond per 1000 bytes of data and assuming that the average speed of the signal in the links is $2x10^8$ m/s.

(5 marks)

(Please Turn Over)

(ii) Assume that the forwarding table of the above switches are empty initially:
Give the forwarding tables for each of the three switches after the four consecutive transmissions below:

1. Host A to Host E
2. Host D to Host A
3. Host E to Host D
4. Host C to Host D

(6 marks)

(c) From the frame capture below: Extract the **destination MAC address**, the datagram **source IP address**, **total length** in *decimal*; the segment **source port number, windows size** in *decimal* and whilst examining the application header content, provide the **server domain name**.

```
04b0 e7f6 85fb 5c87 9c99 4e9a 0800 4500 01e9 0935 4000 8006
7753 c0a8 0119 4cdf 69e6 f1d9 0050 a032 d443 a46a 7f3b 5018
0103 9391 0000 4745 5420 2f20 4854 5450 2f31 2e31 0d0a 486f
7374 3a20 7777 772e 7265 6e65 7761 6c6f 6666 6169 7468 2e6f
7267 0d0a 436f 6e6e 6563 7469 6f6e 3a20 6b65 6570 2d61 6c69
7665 0d0a 5570 6772 6164 652d 496e 7365 6375 7265 2d52 6571
```

(1+1+1+1+1+2 mark)

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