Chapter 1. Introduction:

1. What are the Internet and the WWW?

The Internet is a network of networks.
The WWW is a distributed system that runs on the top of the Internet.

2. Types of Networks. (Section 1.2)

Personal Area Networks
Local Area Networks
Metropolitan Area Netwroks
Internetworks
Wide Area Networks

3. Network Hierarchies (Section 1.3.1)

To reduce their design complexity, most networks are organized as a stack of **layers** or **levels**, each one built upon the one below it. The purpose of each layer is to offer certain **services** to the higher layers while shielding those layers from details of how the offered services are actually implemented.
A **protocol** is an agreement between the communicating parties on how communication is to proceed.
Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations and services the lower layer makes available to the upper one.

4. Layers, protocols and Interfaces (Section 1.4)

Seven layers of OSI (from up to bottom): Application, Presentation, Session, Transport, Network, Data Link, Physical
Four layers of TCP/IP (from up to bottom): Application, Transport, Internet, Link
Five layers used in book: Application, Transport, Network, Link, Physical

DIFFERENCES Between OSI and TCP/IP

The biggest contribution of the OSI model is that it makes the **distinction** between the three concepts of Services, Interfaces and Protocols explicit.
Each layer performs some services for the layer above it.
A layer's interface tells the processes above it how to access it.
The peer protocols used in a layer are the layer's own business.

The TCP/IP model did not originally clearly distinguish between Services, Interfaces and Protocols (although people have tried to retrofit it after the fact to make it mroe OSI-like).

OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer. TCP/IP model supports only connectionless in the network layer but both in the transport layer.

CO and CL

Connection-oriented service is modeled after the telephone system. To use a connection-oriented network service, the service user first **establishes** a connection, uses the connection, and then **releases** the connection. In some cases when a connection is established, the sender, receiver and subnet conduct a **negotiation** about the parameters

to be used.
Connectionless service is modeled after the postal system. Each **packet** carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all subsequent messages. When the intermediate nodes receive a message in full before sending it on to the next node, this is called **store-and-forward switching**. The alternative, in which the onward transmission of a message at a node starts before it is completely received by the node, is called **cut-through switching**.

5. Service Primitives (1.3.3,1.3.4,1.3.5)
CO & CL: check the previous question.

A **service** is formally specified by a set of **primitives** (operations) available to user processes to access the service. If the **protocol stack** is located in the operating system, the **primitives** are normally system calls.

Primitives in Berkeley socket interface: LISTEN, CONNECT, ACCEPT, RECEIVE, SEND, DISCONNECT.

DIFFERENCES BETWEEN SERVICE AND PROTOCOL
A **service** is a set of **primitives** (operations) that a layer provides to the layer above it. A **protocol**, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer.
A **service** is like an abstract data type or an object but does not specify how these operations are implemented. In contract, a **protocol** relates to the implementation of the service and as such is not visible to the user of the service.

6. Network Reference Models (TCP/IP and OSI Reference) (1.4.1,1.4.2 and 1.4.3)
Example Question:

Briefly explain the design principles and benefits of the Open Systems Interconnection (OSI) Layer Division approach (and layered approaches in general) for network design.

Benefits of OSI = Layer design + distinction of three concepts of OSI, check No.4 question of the chapter.

Chapter 2. The Physical Layer:

We will mainly focusing on bandwidth and delay in this topic.

1. Nyquist theorem (2.1.3)
Baud rate and bit rate.

$$maximum\, data\, rate = 2B\log_2(V)$$

$$maximum\, number\, of\, bits/sec = Blog_2(1+S/N)$$

We call the rate at which the signal changes the **symbol rate** to distinguish it from the **bit rate**. The bit rate is the symbol rate multiplied by the number of bits per symbol. An older name for the symbol rate is the **baud rate**.

Latency or delay

Latency is the time **delay** associated with sending a message over a link.

$Transmission\, delay = Message\, in\, bits / Rate\, of\, transmission = M / R\ seconds$

$Propagation\, delay = Length\, of\, the\, channel / speed\, of\, signals$

$Latency = L = M / R + P\text{-}delay$

2. Guided media- Copper vs Fibre (2.2.3 and 2.2.4).

Copper: cheaper, no specialist skills required

Fibre: higher bandwidths, greater distance between repeaters (5km vs. 50km), not physically influenced by interferences or surges, thin/lightweight, no leakage, difficult to tap

Chapter 3. The Data Link layer

1. Design Issues (3.1)

Units, Services, Framing

FUNCTIONS OF DATA LINK LAYER

a. Providing a well-defined service interface to the network layer.
b. Dealing with transmission errors.
c. Regulating the flow of data so that slow receivers are not swamped by fast senders.

2. Framing (3.1.2)

To make it easy for a receiver to find the start of new frames while using little of the channel bandwidth:

a. Byte/Character count
b. Flag bytes with byte stuffing
c. Flag bits with bit stuffing
d. Physical layer coding violations

3. Flow Control and Error control (3.1.3 and 3.1.4)

Flow control:

a. Feedback control
b. Rate based

Error correcting:

a. Hamming code
b. Binary convolutional codes
c. Reed-Solomon codes
d. Low-Density Parity Check code

Hamming code:

a. n = m + r
b. d+1 (detecting) 2d+1 (correcting)
c. correct one => $(n+1)2^m \leq 2^n$ => $(m+r+1) \leq 2^r$

Error detecting:

a. Parity
b. Checksum, e.g., 16-bit internet in IP, Flectcher's checksum
c. CRC

4. Flow control protocols: Stop and Wait, Go-back N and Selective repeat.

	Utilization	Pros	Cons
Stop and Wait	50%		
One Bit	100%		Synchronization issues
Go-Back-N	100%	Senders do not need to wait for ack before sending next	Receiver discards all subsequent frames from error point, sending no ack, until the next frame in sequence
Selective Repeat	100%	Cumlative ack NAK	Receiver needs more buffer

LINK UTILIZATION FORMULA

B: the bit-rate of the link (unit: bit/sec)

L: length of the frame (unit: bit)

$T_f = Time\ needed\ to\ transmit\ a\ frame\ of\ length\ L$

$T_p = Propagation\ delay\ of\ the\ channel$ (unit: sec)

$T_a = Time\ for\ transmitting\ an\ Ack$ (assume this is zero)

$U = (Time\ of\ transmitting\ a\ frame)/(Total\ time\ for\ the\ transfer) = T_f / T_t$

$U = T_f/(T_f + 2T_p) = (L/B)/(L/B + 2T_p) = L/(L + 2T_pB)$

Chapter 4. The MAC sub Layer (Updated)

1. Multiple access protocols (4.2)
a. ALOHA (pure/slotted)
b. CSMA (Carrier Sense Multiple Access)
c. Collision Free
d. Limited Contention
e. Wireless LAN protocols

2. CSMA (4.2.2)

Require state detection to determine transmission rights dynamically.

a. Persistent and Non-Persistent CSMA

1-persistent CSMA, Non-Persistent CSMA, p-persistent CSMA

b. CSMA/CD (CSMA with Collision Detection)

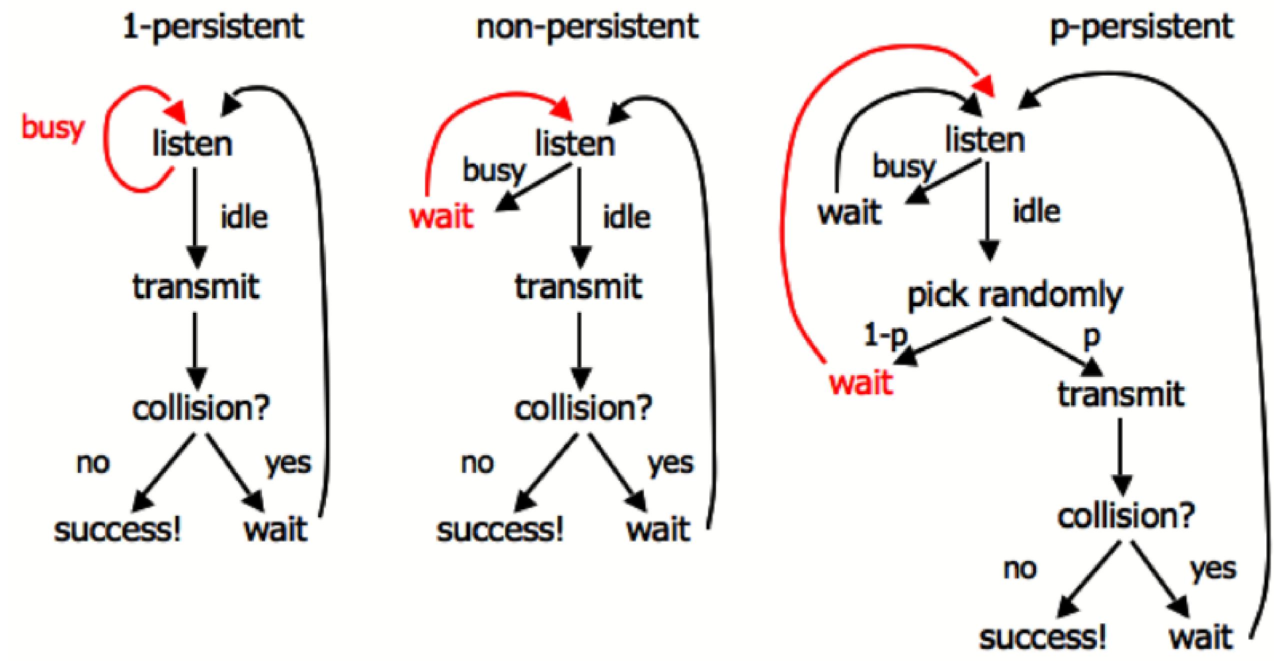
Principle that transmission aborted when collision detected

After collision detected, abort, wait random period, try again

Channel must be continually monitored, implies only half-duplex system

DIFFERENCES (Summarized from last line, P266 & 4th line, last paragraph, P268)

	Collision during transmission
CSMA	Transmit a whole frame anyway, react to collisions after the transmission is over
CSMA/CD	Abort the transmission when collides



3. Collison-Free & Limited Contention Protocols (4.2.3 and 4.2.4)

Collision Free Protocols

a. Bit Map Protocol

1 bit per station overhead

Division of transmission right, and transmission event. Reservation based protocol

b. Binary Countdown Protocol

Avoid the 1 bit per station scalability problem by using binary station addressing

No collisions as higher-order bit positions are used to arbitrate

Higher numbered stations have a higher priority

ATTENTION: As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up.

c. Token Passing

Pass a small message called a token from one station to the next in the same predefined order.

In a **token ring** protocol, the topology of the network is used to define the order in which stations send.

COMPARISON BETWEEN CONTENTION AND COLLISION FREE

Higher loads: contention is less attractive because overhead associated with channel arbitration becomes greater

Low loads: collision free is less attractive because of a higher delay between transmissions

Limited Contention Protocols

ADVANTAGE: increase the probability of stations acquiring transmission rights by arbitrarily dividing stations and using a binary algorithm to determine rights allocation

Adaptive Tree Walk Protocol: All stations compete for right to transmit, if a collision occurs, binary division is used to resolve contention

level of tree to search first: $i = \log_2 q$, q is the number of competing stations

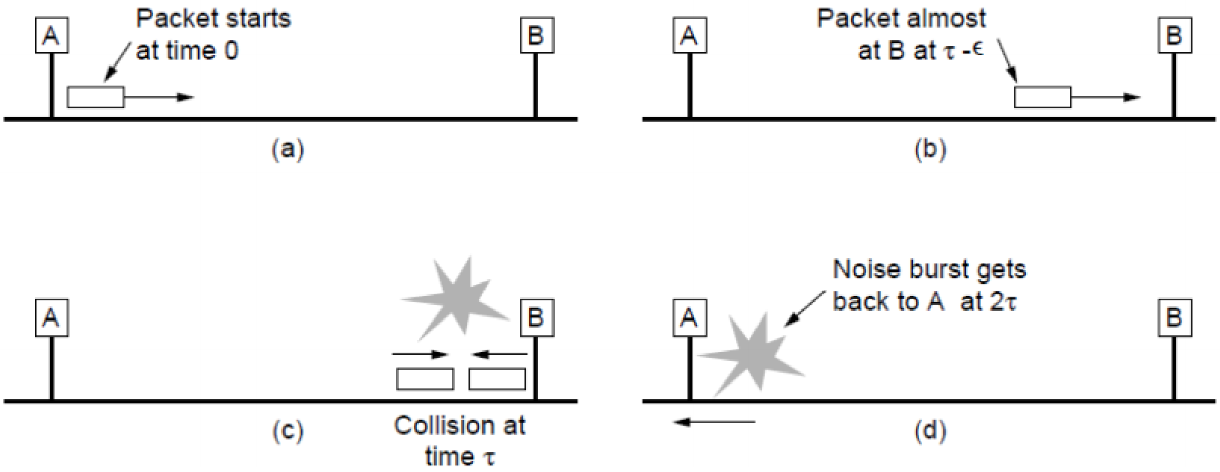
4. Wireless Protocols (4.2.5)

Two problems: Hidden terminal, Exposed terminal

MACA (Multiple Access with Collision Avoidance)
a. Send asks receiver to transmit short control frame
b. Stations near receiver hear control frame
c. Sender can then transmit data to receiver

MACAW (MACA for Wireless)

5. Classic Ethernet (4.3.2) (Discussion around Figure 4.15)
Classic Ethernet
a. Each type of Ethernet has a maximum cable length per segment
b. Multiple cable lengths can be connected by repeaters – a physical device which receives, amplifies and retransmits signals in both directions



Minimum packet size problem: collisions should be detected before completing the transmission of current frame.

$$\textit{minimum packet} = \textit{bit-rate} * \tau$$

For a 10Mbps Ethernet, typically the worst τ would be nearly 50 µsec, sot 500 bits is the smallest size. This number is rounded up to 512 bits or 64 bytes for safety.

6. Practice relevant questions from Assignment 1.

Chapter 5. The Network Layer

1. Design Goals and Store and forward packet switching (5.1.1)
Design Goals
a. Services should be independent of router technologies
b. Transport layer should be shielded from number, type and topology of routers
c. Network addressing should use a uniform numbering plan

Switching: Hosts generate packets and injects into the network, Router routes packets through the network

(Dupe! Check CO & CL above) When the intermediate nodes receive a message in full before sending it on to the next node, this is called **store-and-forward switching**. The alternative, in which the onward transmission of a message at a node starts before it is completely received by the node, is called **cut-through switching**.

2. Virtual circuits (5.1.3)

If connection-oriented service is used, a path from the source router all the way to the destination router must be established before any data packets can be sent. This connection is called a **VC (virtual circuit)** and the network is called a **virtual-circuit network**.

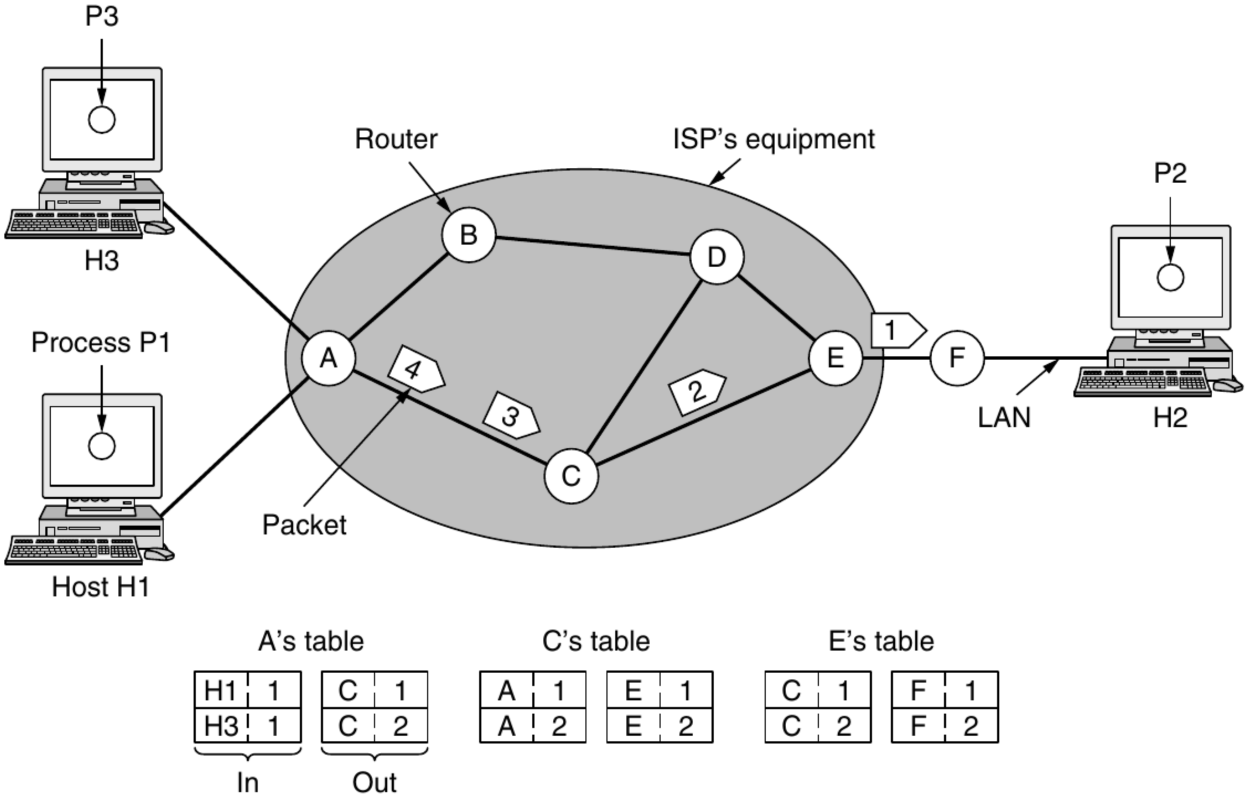


Figure 5-3. Routing within a virtual-circuit network.

ALSO CHECK

a. How to update a routing table when new info comes in

b. Datagram routing

DIFFERENCES BETWEEN VC AND DATAGRAM

Issue	Datagram network	Virtual-Circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of Service	Difficult	Easy if enough resources can be

		allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

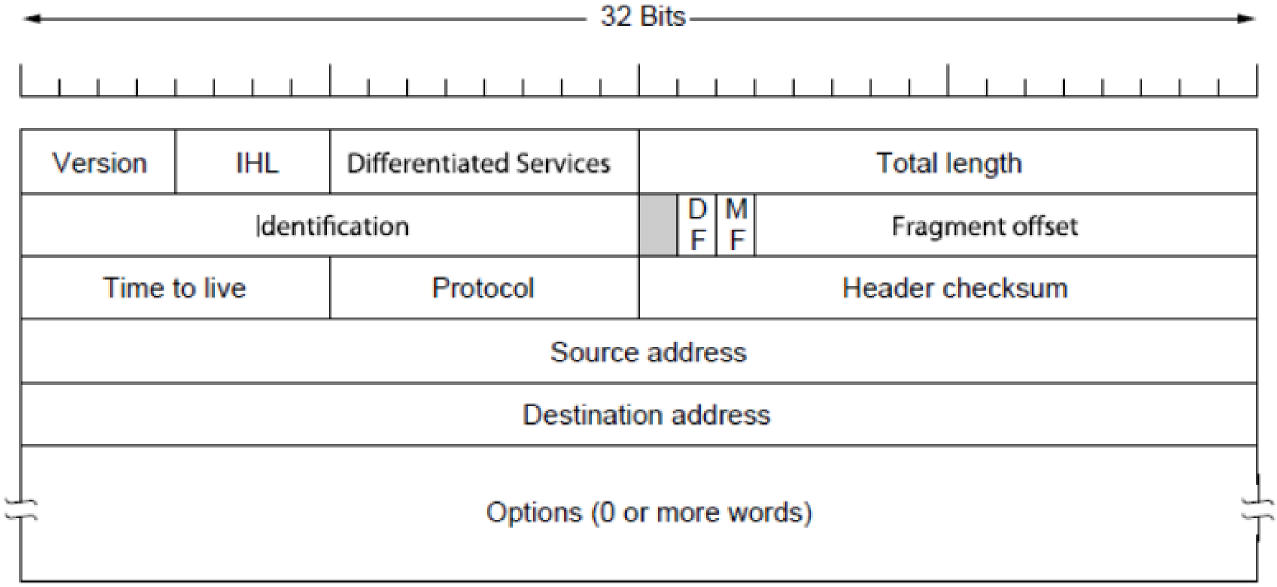
3. IP protocol and IPv4 Structure (5.6.1)

Internet Protocol

a. Provides a “best-effort” service to route datagrams from source host to destination host

b. These hosts may be: On *same* network, or, On *different* networks

c. Each network is called an **Autonomous System** (AS)



4. Addressing (5.6.1 and 5.6.2)

Classful network

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address
Class A	0	8	24	2^{7}	2^{24}	2^{31}	0.0.0.0	127.255.255.255
Class B	10	16	16	2^{14}	2^{16}	2^{30}	128.0.0.0	191.255.255.255
Class C	110	24	8	2^{21}	2^{8}	2^{29}	192.0.0.0	223.255.255.255
Class D	1110	N/D	N/D	N/D	N/D	2^{28}	224.0.0.0	239.255.255.255
Class E	1111	N/D	N/D	N/D	N/D	2^{28}	240.0.0.0	255.255.255.255

*CHECK DECIMAL IP REPRESENTATION AND **CIDR***

Useful link: http://www.ipaddressguide.com/cidr

Longest Matching Prefix: Packet are forwarded to the entry with the longest matching prefix or smallest address block
Appendix by Fred: It seems that routing rules in this course are always *smaller the first*, so we do not need to take the sequence of routing rules into consideration. (Check tutorial W6Q9.)