Finals Studying Notes

Multiple Choice Questions

HDLC frame format

8 Bit	8 Bits	8/16 Bits	Variable	16/32 Bits	8 Bits
Header				Trailer (Tail)	
Flag	**Address**	**Control**	**Info**	**CRC**	**Flag**

- Flag : Six one bits surrounded by padded 0 bits (01111110)
- Address : Identifies the frames destination
- Control : Defines the type of a frame and how it should be handled
- Info : The actual data being transmitted
- CRC : check bits calculated over the address, control, and info bits.

I-Frames

I-frames are designed to carry user data from the network layer. In addition, they can include flow and error control information (piggybacking).

S-Frames

Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate (e.g., when the station either has no data of its own to send or needs to send a command or response other than an acknowledgment). S-frames do not have information fields.

U-Frames

Unnumbered frames are used to exchange session management and control information between connected devices. Unlike S-frames, U-frames contain an information field, but one used for system management information, not user data. As with S-frames, however, much of the information carried by U-frames is contained in codes included in the control field. U-frame codes are divided into two sections: a 2-bit prefix before the P/F bit and a 3-bit suffix after the P/F bit. Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.

P/F Bit

Poll/Final is a single bit with two names. It is called Poll when part of a command (set by the primary station to obtain a response from a secondary station), and Final when part of a response (set by the secondary station to indicate a response or the end of transmission). In all other cases, the bit is clear.

ICMP - Internet Control Management Protocol

ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets.

Used by utilities such as ping and traceroute

Sliding window

A sliding window protocol is a feature of packet-based data transmission protocols. Sliding window protocols are used where reliable in-order delivery of packets is required, such as in the Data Link Layer (*OSI model*) as well as in the Transmission Control Protocol (*TCP*).

Stop-and-wait

Transmission and Receive buffer are both 1 frame in size. Therefore the sender must wait for the receiver to receive its current frame before sending another.

Go-Back-N

Sliding window protocol where $W_t > 1$[1] but $W_r = 1$[2]. This mean the receiver declined to receive any packet except the next sequential one. If a packet is lost in transit all the following ones will be ignored until the missing packet is retransmitted.

Selective Repeat

the sender sends a number of frames specified by a window size even without the need to wait for individual ACK[3] from the receiver as in Go-Back-N ARQ[4]. The receiver may selectively reject a single frame, which may be retransmitted alone

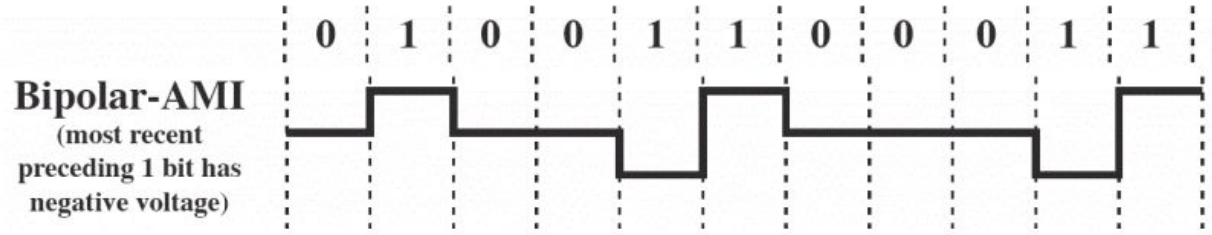
---

[1] W_t = Window size of transmitter
[2] W_r = Window size of receiver
[3] Acknowledgement frame
[4] ARQ = Automatic Repeat-reQuest

Types of encoding

Bipolar-AMI[5]

For each bit in sequence:
If current bit is a 0: no pulse
If current bit is a 1:
If a previous bit is positive, encode as negative bit
If a previous bit is negative, encode as positive bit



B8ZS - Bipolar-AMI with 8 Zero Substitution

Based off of Bipolar-AMI with the following differences:
If octet of all zeros and last voltage pulse preceding was positive, encode as 000+-0-+
If octet of all zeros and last voltage pulse preceding was negative, encode as 000-+0+-
Receiver detects and interprets as octet of all zeros

HDB3

Based off of bipolar-AMI, this encoding technique substitutes phases of four zeros with one or two pulses

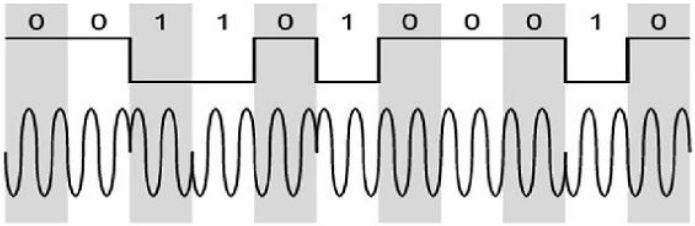
	Number of Bipolar Pulses (ones) since Last Substitution	
Polarity of Preceding Pulse	**Odd**	**Even**
–	000–	+00+
+	000+	–00–

10100000110000110000000
+0-000V0+-B00V-+B00V00
+0-000-0+-+00+-+-00-00

[5] AMI = alternate mark inversion

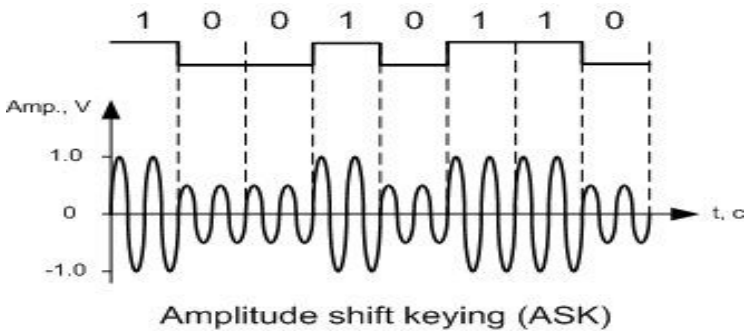
PSK

Phase Shift Keying: The phase of a wave is shifted when the data is a 1 and is kept normal when the data is a 0



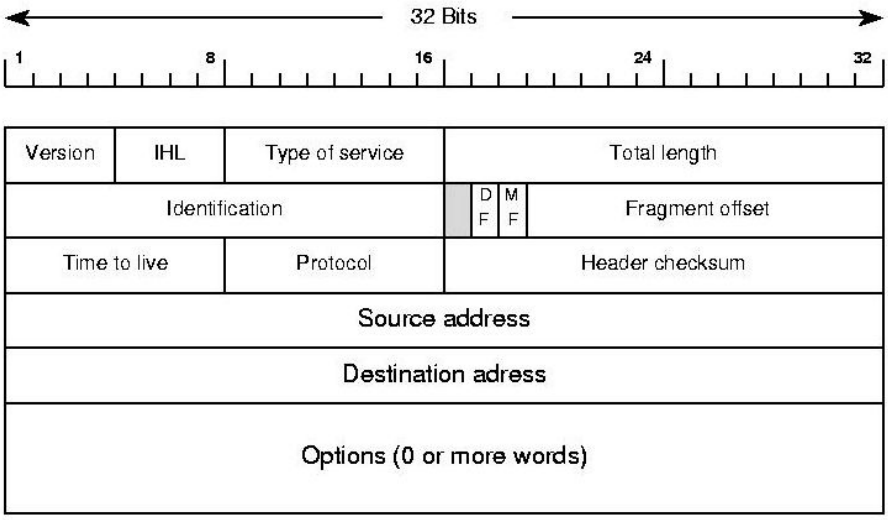
ASK

Amplitude Shift Keying: The amplitude of a wave is shifted when data is a 1 and kept normal when data is a 0



Amplitude shift keying (ASK)

Format of an IP datagram



Version: This field specifies the version of IP used for transferring data. The size of the Version field is 4 bits. Both the sender and the receiver must use the same version of IP to ensure proper interpretation of the fields in the datagram.

IHL (Header Length): The size of the Header Length or the IHL field is 4 bits. The Header Length field is used to specify the length of header, which can range from 20 to 60 bytes. You must multiply the value in this field by four to get the length of the IP header. For example, if the value in this field is 3, the length of the header is 3*4, which is 12 bytes.

Service Type: The Service Type field is used to set priorities or precedence for data transmission. The size of the field is 8 bits. This field is also used to determine the type of service that is required for a particular application. The priority is set using the first three bits and the service type is set using the next three bits. The last two bits are reserved for future use. The Service Type field has two components, Precedence and Types of Service. In the sections that follow, the components of the Service Typefield are explained in detail.

Total Length: The Total Length field specifies the total length of the datagram. The size of the field is 16 bits. The Total Length field can be calculated as follows:

$$Total\ length\ of\ the\ datagram\ =\ Length\ of\ the\ header\ +\ Length\ of\ the\ data$$

TTL (Time to live): TTL is the amount of time a frame is retained on the network. The TTL is 8 bits long and measured in seconds

Protocol: The Protocol field is used to specify the protocol used to create the data present in the Data field. The size of this field is 8 bits.

Value (Decimal)	Protocol
1	Internet Control Message Protocol (ICMP)
2	Internet Group Management Protocol (IGMP)
3	Gateway-to-Gateway Protocol (GGP)
4	Internet Protocol (IP)
6	Transmission Control Protocol (TCP)
8	Exterior Gateway Protocol (EGP)
9	Interior Gateway Protocol (IGP)
17	User Datagram Protocol (UDP)
41	Internet Protocol Version 6 (IPv6)
86	Dissimilar Gateway Protocol (DGP)
88	Interior Gateway Routing Protocol (IGRP)
89	Open Shortest Path First (OSPF)

Different types of routing

Classless Inter Domain Routing (CIDR)

Ip addresses in the format of xxx.xxx.xxx.xxx/yy where yy is the amount of bits that are to be reserved as the network prefix.

E.g.
10.0.0.0/8 = 10.0.0.0 to 10.255.255.255
10.0.0.0/24 = 10.0.0.0 to 10.0.0.255

Subnets and Subnet Masks

A subnet address is the mask thats is the bitwise AND result of the primary address and the subnet mask. This results in an address that is masked to the subnet address.

Requirements for Routing

- Correctness
- Simplicity
- Robustness
- Stability
- Fairness
- Optimality
- Efficiency

Routing Protocols

RIP - Routing Interface Protocol

Uses hop count as a metric to prevent looping. The largest number of hops a RIP network can sustain is 15.

OSPF - Open Shortest Path First

BGP - Border Gateway Protocol

Nyquest Theorm

Things needed for final

Hamming code

If odd bits, result is = 0
If even bits, result is = 1

Decode

Take codeword,
Find p1-8,
Including the parity bits,
If even, no error
If odd, error has occurred

Fragmentation

Connecting one Network to another
Message is going from network A to network B
MTU = maximum transfer unit
Router verifies MTU and routes packets
MTU includes header
Total amounts = ceil(total size/MTU)
Problem: header
So mtu = mtu-header

Identifier	Total Length	Offset	More Flag
00H	1196	0	1

00H	1196	147	1
...	...	...	...
00H	164	882	0

Classful addressing

A company contains a class B block address,
165.100.0.0. the company requires 1000 subners and 60 hosts per subnet.

Find the custom subnets and default subnet mask

Take the address = 165.100.0.0
Bits of the host id = 00000000.00000000

Allocate subnets, 2^10 = 1024. We need 10 bits
Aka 11111111.11111111.11111111.11000000
Aka 255.255.255.192

Big Q

CDIR:
Range = 124.34.56.0/23

2^32-n, n has to be greater than 28, Therefore n=27

Subnet 1 addresses = 124.34.56.0/27 to 124.34.56.31/27
Subnet 2 addresses = 124.34.56.32/27 to 124.34.56.63/27
Subnet 3 addresses = 124.34.56.64/27 to 124.34.56.95/27
Subnet 4 addresses = 124.34.56.96/27 to 124.34.56.127/27

Routing tables:
R1:

NetID	Next node loval	Iface
124.34.56.0/27	Local	A
124.34.56.32/27	124.34.56.97/27	-
124.34.56.64/27	Local	B
124.34.56.96/27	Local	C

Default gateway	127.34.56.97/27	

R2:

Netid	Local or not	Interface
123.34.56.0/27	124.34.56.97/24	-
124.34.56.32/27	Local	A
124.34.55.64/27	Local	C
124.34.56.96/27	Local	B
Default gateway	Isp address	

ICMP:

A=124.34.56.1/27
B=124.34.56.33/27

A:
No point to point
Send packet to R1

R1:
Looks at dest IP, 124.34.56.33/27
Find first address by binary and
124.34.56.32/27
Passes to that address, which isn't local
A.k.a. send to R2

R2:
Looks at dest IP,
Finds the first address,
That's in the routing table.
Sends to B over a

B:
Received packet