IPV6

- In this notation, 128 bits are divided into eight sections, each 2 bytes in length. Two bytes in hexadecimal notation require four hexadecimal digits
- Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.
- ex : FDEC:BA98:7654:3210:ADBF:BBFF:2922:FFFF
- adress lenght is 4 times IPv4
- abbreviation of IPv6 :
  - . The leading zeros of a section can be omitted. Using this form of abbreviation, 0074 can be written as 74.Note that 3210 cannot be abbreviated
  - if there are consecutive sections consisting of zeros only. We can remove all the zeros altogether and replace them with a double colon(::).if there are two runs of zero sections only one can be compressed (the longest)
- mixed representation (ipv4 embedded inside ipv6 as rightmost 32 bit/last 2 sections) :FDEC:14AB:2311:BBFE:AAAA:BBBB:130.24.24.18
- adress types
  - unicast : for single interface
  - multicast : A multicast address also defines a group of computers. However, there is a difference between anycasting and multicasting. In multicasting, each member of the group receives a copy
  - anycast : An anycast address defines a group of computers that all share a single address. Apacket with an anycast address is delivered to only one member of the group, the most reachable one. An anycast communication is used, for example, when there are several servers that can respond to an inquiry. The request is sent to the one that is most reachable
  - ipv6 doesnt define broadcasting

adress space allocation

Figure 26.5 Address space allocation

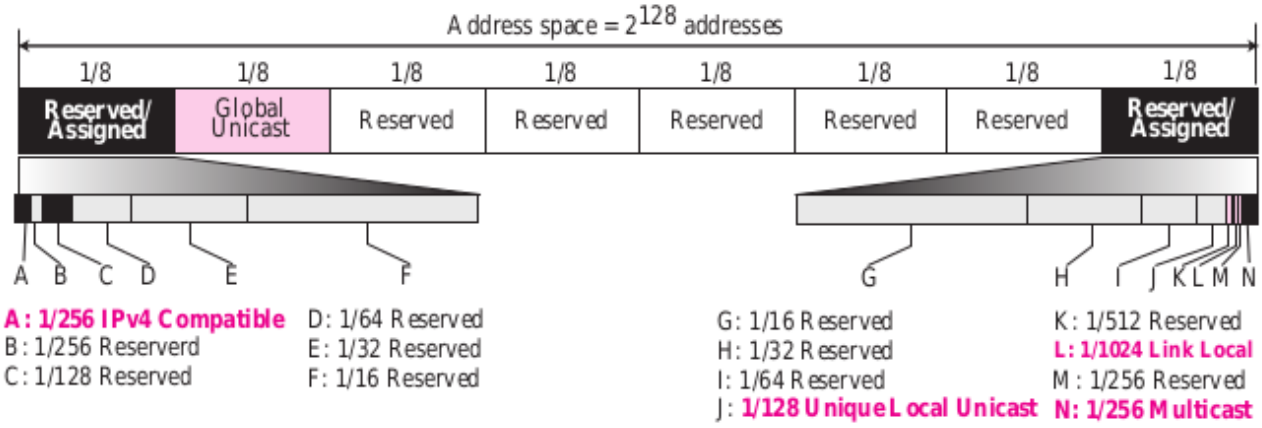


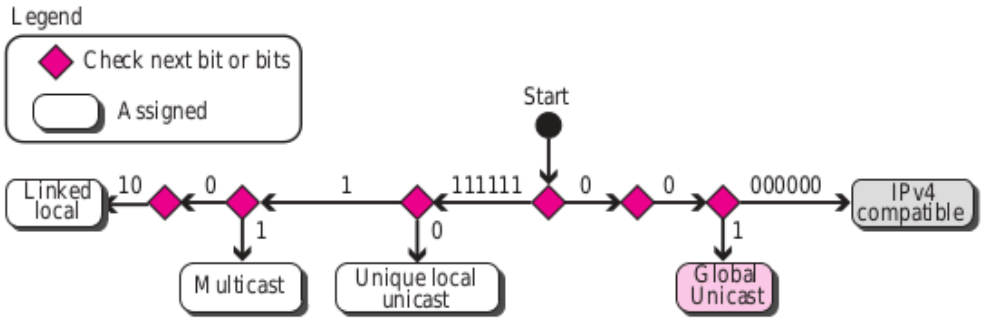
Table 26.1 Prefixes for IPv6 Addresses

	Block Prefix	CIDR	Block Assignment	Fraction
1	0000 0000	0000::/8	Reserved (IPv4 compatible)	1/256
	0000 0001	0100::/8	Reserved	1/256
	0000 001	0200::/7	Reserved	1/128
	0000 01	0400::/6	Reserved	1/64
	0000 1	0800::/5	Reserved	1/32
	0001	1000::/4	Reserved	1/16
2	**001**	**2000::/3**	**Global unicast**	**1/8**
3	010	4000::/3	Reserved	1/8
4	011	6000::/3	Reserved	1/8
5	100	8000::/3	Reserved	1/8
6	101	A000::/3	Reserved	1/8
7	110	C000::/3	Reserved	1/8
8	1110	E000::/4	Reserved	1/16
	1111 0	F000::/5	Reserved	1/32
	1111 10	F800::/6	Reserved	1/64
	1111 110	FC00::/7	Unique local unicast	1/128
	1111 1110 0	FE00::/9	Reserved	1/512
	1111 1110 10	FE80::/10	Link local addresses	1/1024
	1111 1110 11	FEC0::/10	Reserved	1/1024
	1111 1111	FF00::/8	Multicast addresses	1/256

Example 26.8

only a maximum of 10 bits to find the block of the address. Note that the reserved

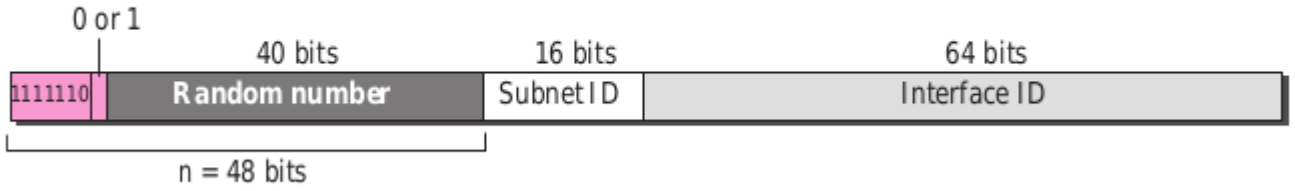
Figure 26.6 Algorithm for finding the allocated blocks



- global unicast prefix : 001 (/3)
- unique local unicast prefix is 1111 110 (/7)
- multicast prefix: 1111 1111 (/8)
- link local prefix : 1111 1110 10 (/10)
- ipv4 compatible adress : 0000::/8
- unspecified adress : ::/128
- loopback adress : ::1/128 (this is an address used by a host to test itself without going into the network. In this case, a message is created in the application layer, sent to the transport layer, and passed to the network layer. However, instead of going to the physical network, it returns to the transport layer and then passes to the application layer.)
- embedded ipv4
  - compatible adres : 96 bits of zero followed by 32 bits of IPv4 address, ::/96
    - is usedwhen a computer using IPv6 wants to send a message to another computer using IPv6. However, suppose the packet passes through a region where the networks are still using IPv4.
  - mapped adress :
    - comprises 80 bits of zero, followed by 16 bits of one, followed by the 32-bit IPv4 address.
    - The packet travels mostly through IPv6 networks but is finally delivered to a host that uses IPv4
- global unicast block : main block used for unicast communication between hosts in the Internet.
- Unique Local Unicast Blockblocks in the IPv4 address space were reserved for private addressing. IPv6 uses two large blocks for private addressing: one at the site level and one at the link level.

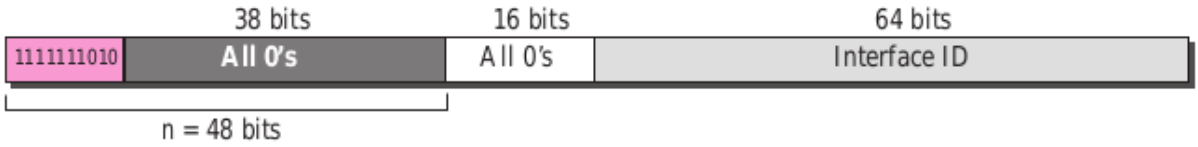
- site level unique local unicast block : block identifier 1111 110,next bit can be 0 or 1 , next 40 bits are selectd randomly by site.. they are not routable on public internet (only within site or organisation). meant for internal communication within sites network and meant to be globally unique can have subnet id

Figure 26.11 Unique local unicast block



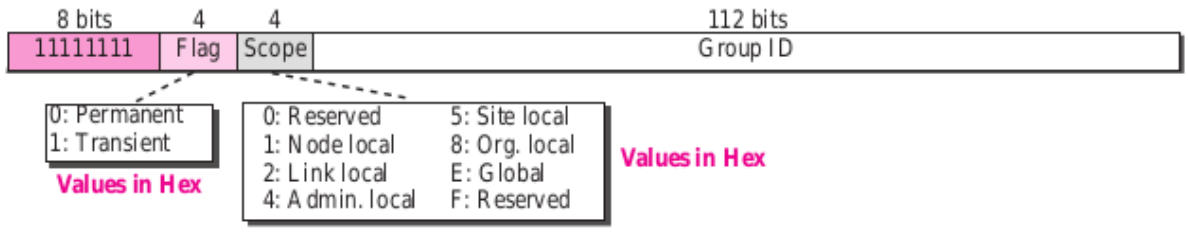
- link local block : has the block identifier 1111 1110 10. The next 54 bits are set to zero. The last 64 bits can be changed to define the interface for each computer.they have smaller scope and are limited to single network segment or link(not routable beyond local link). they dont hv subnet id as only within single local link

Figure 26.12 Link local address



- multicast block :used to define groups of hosts instead of one.permenant group means can be accessed all the time while transient is temporary

Figure 26.13 Multicast address



- global unicast :
  - CIDR : 2000::/3 (as prefix is 001)

Figure 26.14 Global unicast address

Recommended length of the different parts are shown in Table 26.2.

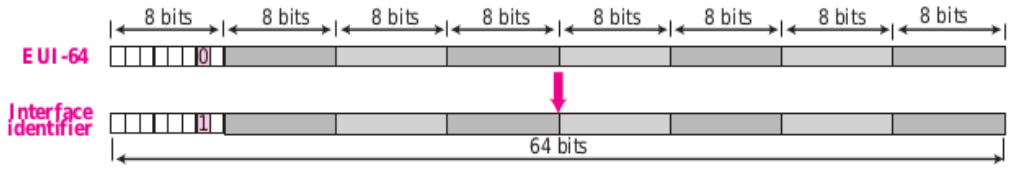
Table 26.2 Recommended Length of Different Parts in Unicast Addressing

Block Assignment	Length
Global routing prefix (n)	48 bits
Subnet identifier (128 – n – m)	16 bits
Interface identifier (m)	64 bits

-
- global routing prefix : used to route the packet through the Internet to the organization site such as ISP that owns the block , up to 2^45 (48-3)sites (ISP's or private organisation)
- subnet identifier : 2&16 subnets possible
- interace identifier :
  - defines interface.
  - physical adress is 48 bits while interface is 64 bits so physical address whose \ can be embedded as the whole or part of the interface identifier, eliminating the mapping process
  - two common physical adressing scheme : 64-bit extended unique identifier (EUI-64) defined by IEEE and the 48-bit physical address defined by Ethernet.

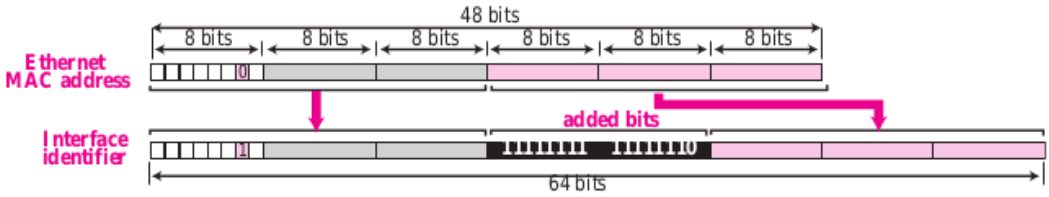
Mapping EUI-64 To map a 64-bit physical address, the global/local bit of this format needs to be changed from 0 to 1 (local to global) to define an interface address, as shown in Figure 26.15.

Figure 26.15 Mapping for EUI-64



Mapping Ethernet MAC Address Mapping a 48-bit Ethernet address into a 64-bit interface identifier is more involved. We need to change the local/global bit to 1 and insert an additional 16 bits. The additional 16 bits are defined as 15 ones followed by one zero, or $FFFE_{16}$. Figure 26.16 shows the mapping.

Figure 26.16 Mapping for Ethernet MAC



-
- mapping for eui 64 means to convert 64 bit physical adres to interface adress to be embeeded in ipv6 datagram
- mapping for ethernet mac means to convert 48 bit mac adress to 64 bit interface adress to be embedded inside ipv6 datagram

ipv6 protocol

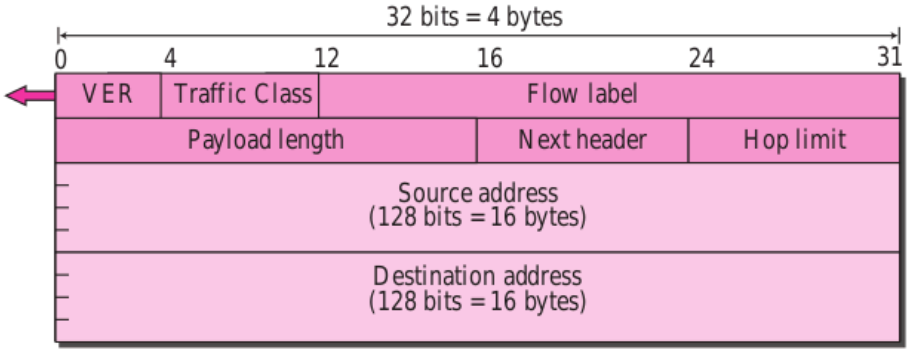
- advantages of ipv6 over ipv4
- The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information

IPv6 protocol responds to the above issues using the following main changes in the protocol:

- **Larger address space.** An IPv6 address is 128 bits long. Compared with the 32-bit address of IPv4, this is a huge (2^{96} times) increase in the address space.
- **Better header format.** IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- **New options.** IPv6 has new options to allow for additional functionalities.
- **Allowance for extension.** IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- **Support for resource allocation.** In IPv6, the type-of-service field has been removed, but two new fields, traffic class and flow label have been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
- **Support for more security.** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

- datagram
  ![](Pasted%20image%2020240501182642.png]]
- packet format

Figure 27.2 Format of the base header



- version indicates ipv4 or 6
- traffic class is similar to type of service in ipv4 (like realtime or non real time ,ECN)
- flow label :
  - 20 bit field, In its simplest form,
  - a flow label can be used to speed up the processing of a packet by a router. When a router receives a packet, instead of consulting the routing table and going through a routing algorithm to define the address of the next hop, it can easily look in a flow

label table(each entry defines the services required by the corresponding flow label) for the next hop.ex : flow label used for transmission of real time audio and video
    - the use of real-time data and the reservation of these resources require other protocols such as Real-Time Protocol (RTP) and Resource Reservation Protocol (RSVP) in addition to IPv6
    - 3 rules for flow labels :
    - The flow label is assigned to a packet by the source host. The label is a random number between 1 and 2 24 – 1. A source must not reuse a flow label for a new flow while the existing flow is still alive.
    - If a host does not support the flow label, it sets this field to zero. If a router does not support the flow label, it simply ignores it.
    - All packets belonging to the same flow have the same source, same destination,same priority, and same options.
- next header :defines header following base header . The next header is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP. Each extension header also contains this field
- hop limit : like ttl
- extension header(inside next header):

Figure 27.3 Extension header format

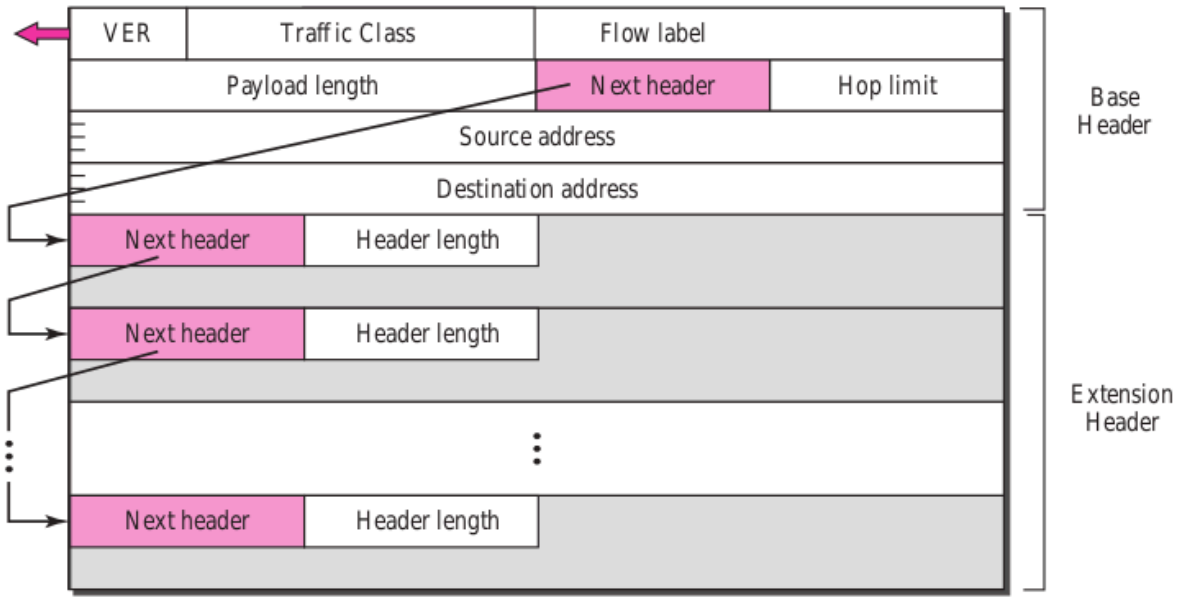
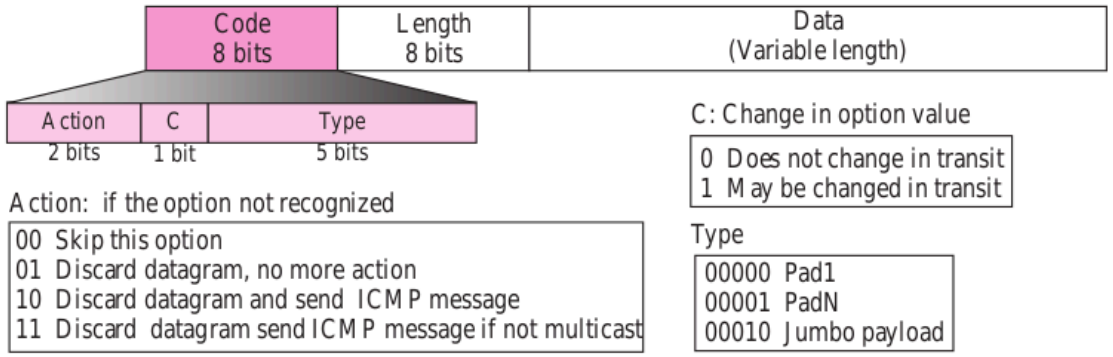


Figure 27.4 Extension header types

- hop by hop : used when the source needs to pass information to all routers visited by the datagram like debugging information, or if length > 65535 , routers must have this

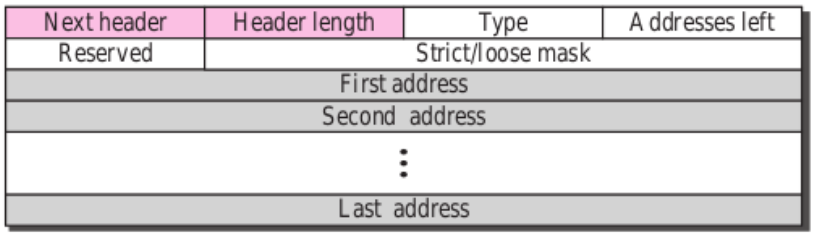
information
- 3 types of hop by hop options : - pad1,padN,jumbo payload
- pad1 : 1 byte long and used for alignment purpose , i.e some options need to start at specific bit of 32 bit word , so if option falls short of this alignment pad1 is added.((action is 00, the change bit is 0, and type is 00000)
- padn : The difference is that PadN is used when n or more bytes are needed for alignment (action is 00, the change bit is 0, and type is 00001)).option length contains number of padding bytes
- jumbo payload : the length of the payload in the IP datagram can be a maximum of 65,535 bytes. However, if for any reason a longer payload is required, we can use the jumbo payload option to define this longer length.it starts at 4n+2 byte always from beginning of extension header

Figure 27.6 The format of options in a hop-by-hop option header



- destination option : when source needs to pass information to destination.intermediate routers are not permitted to access it same format as hop by hop
- source routing :

Figure 27.10 Source routing



  - The type field defines loose or strict routing.
  - The addresses left field indicates the number of hops still needed to reach the destination.

- The strict/loose mask field determines the rigidity of routing. If set to strict, routing must follow exactly as indicated by the source. If, instead, the mask is loose, other routers may be visited in addition to those in the header

- fragmentation : in ipv4 , source or router could fragment here only source can fragment.A source must use a Path MTU Discovery technique to find the smallest MTU supported by any network on the path. If the source does not use a Path MTU Discovery technique, it fragments the datagram to a size of 1,280 bytes or smaller.

Figure 27.12 Fragmentation

- authentication field:used to check if sender is genuine and integrety / comprimisation of payload(if payload corrupted by hacker).The sender passes a 128-bit security key, the entire IP datagram, and the 128-bit security key again to the algorithm.reciever takes the secret key and the received datagram (again, with changeable fields set to zero) and passes them to the authentication algorithm. If the result matches that in the authentication data field, the IP datagram is authentic; otherwise, the datagram is discarded.

Figure 27.13 Authentication

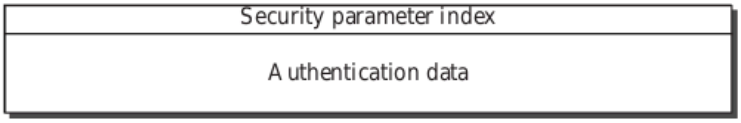
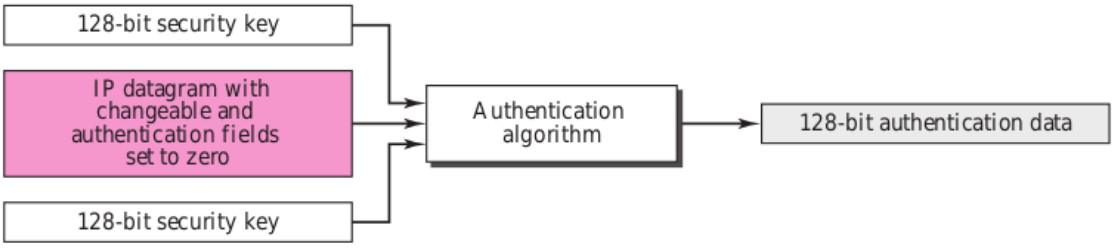
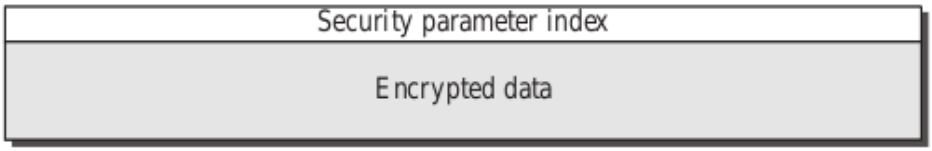


Figure 27.14 Calculation of authentication data



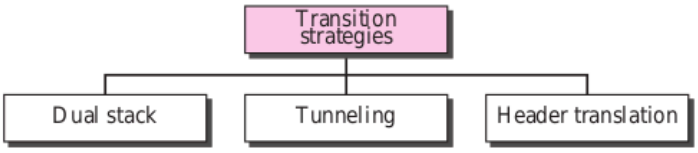
- enccypted securirty payload : The security parameter index field is a 32-bit word that defines the type of encryption/decryption used. The other field contains the encrypted data along with any extra parameters needed by the algorithm

Figure 27.15 Encrypted security payload



Transition from IPV4 to IPV6

Figure 27.16 Three transition strategies

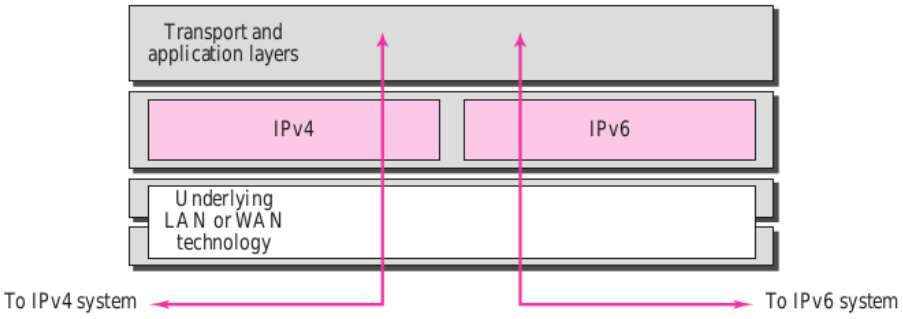


Dual Stack

- dual stack

It is recommended that all hosts, before migrating completely to version 6, have a **dual stack** of protocols. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6. See Figure 27.17 for the layout of a dual-stack configuration.

Figure 27.17 Dual stack



- tunneling : when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet

must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region

- header translation : he sender wants to use IPv6, but the receiver does not understand IPv6.tunneling cannot happen as header needs to be translated .rules for transforming ipv6 packet header to ipv4
    - The IPv6 mapped address is changed to an IPv4 address by extracting the right-most 32 bits
    - The value of the IPv6 priority field is discarded.
    - The type of service field in IPv4 is set to zero.
    - The checksum for IPv4 is calculated and inserted in the corresponding field.
    - The IPv6 flow label is ignored.
    - Compatible extension headers are converted to options and inserted in the IPv4 header. Some may have to be dropped.
    - The length of IPv4 header is calculated and inserted into the corresponding field.
    - The total length of the IPv4 packet is calculated and inserted in the corresponding field.

ICMP

- used for error reporting
- is often considered part of IP, but architecturally it lies just above IP, as ICMP messages are carried inside IP datagrams, i.e ICMP messages are carried as part of IP payload
- when host recieves IP datagram with ICMP packets it demultiplexes it into ICMP
- ICMP messages have a type and a code field, and contain the header and the first 8 bytes of the IP datagram that caused the ICMP message to be generated in the first place
- ping program sends an ICMP type 8 code 0 message to the specified host. The destination host, seeing the echo request, sends back a type 0 code 0 ICMP echo reply
- source quench message. This message is used to perform congestion control—to allow a congested router to send an ICMP source quench message to a host to force that host to reduce its transmission rate

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Figure 5.19 ICMP message types

-
- traceroute using ICMP : Traceroute in the source sends a series of ordinary IP datagrams to the destination.each datagram is udp segment with unlikely port number and each datagram have TTL of 1,2,.. and so on.when nth TTL of packet expires , nth router discards it and sends sends an ICMP warning message to the source (type 11 code 0). This warning message includes the name of the router and its IP address.This way we get intermediate router adress.at some point some datagram will reach destination but udp port number is unlikely (it sends) so it sends unreachable ICMP message (type 3 code 3) back to the source. When the source host receives this particular ICMP message, it knows it does not need to send additional probe packets.

ROUTING ALGORITHMS :

- graph is G(N,E) = Nodes, Edges
- For any edge (x, y) in E, we denote c(x, y) as the cost of the edge between nodes x and y
- if (x,y) doesnt belong to E , we set c(x,y) = ∞
- x1,x2, .. xp are nodes
- A centralized routing algorithm computes the least-cost path between a source and destination using complete, global knowledge about the network.algorithm has complete information about connectivity and link costs. Algorithms with global state information are

often referred to as link-state (LS) algorithms, since the algorithm must be aware of the cost of each link in the network

- in a decentralized routing algorithm , the calculation of the least-cost path is carried out in aniterative, distributed manner by the routers. No node has complete information about the costs of all network links. Instead, each node begins with only the knowledge of the costs of its own directly attached links. Then, through an iterative process of calculation and exchange of information with its neighboring nodes, a node gradually calculates the least-cost path to a destination or set of destinations.it is suited to control planes where routers interact with each other.This is distance vector algorithm
- In a load-sensitive algorithm, link costs vary dynamically to reflect the current level of congestion in the underlying link.
- 3 ways to classify {centralised,decentralised},{static,dynamic},{load sensitive}

Link state routing algorithm

- centralized routing algorithm
- Dijkstra's algorithm computes the least-cost path from one node (the source, which we will refer to as u) to all other nodes in the network. Dijkstra's algorithm is iterative and has the property thata fter the kth iteration of the algorithm, the least-cost paths are known to k destination nodes, and among the least-cost paths to all destination nodes, these k paths will have the k smallest costs.
- notations :
  - D(v): cost of the least-cost path from the source node to destination v as of this iteration of the algorithm.
  - p(v): previous node (neighbor of v) along the current least-cost path from the source to v.
  - N′: subset of nodes; v is in N′ if the least-cost path from the source to v is definitively known.
- based on D(v) = min(D(v), D(w)+ c(w,v))
- algorithm consists of initialisation step followed by a loop.number of times loop runs is the number of nodes

```
Initialization:
N’ = {u}
for all nodes v
        if v is a neighbor of u
                then D(v) = c(u, v)
        else D(v) = ∞
```

```
Loop
find w not in N’ such that D(w) is a minimum
add w to N’
update D(v) for each neighbor v of w and not in N’:
        D(v) = min(D(v), D(w)+ c(w, v) )

/* new cost to v is either old cost to v or known
least path cost to w plus cost from w to v */
15 until N’= N
```

- ex :

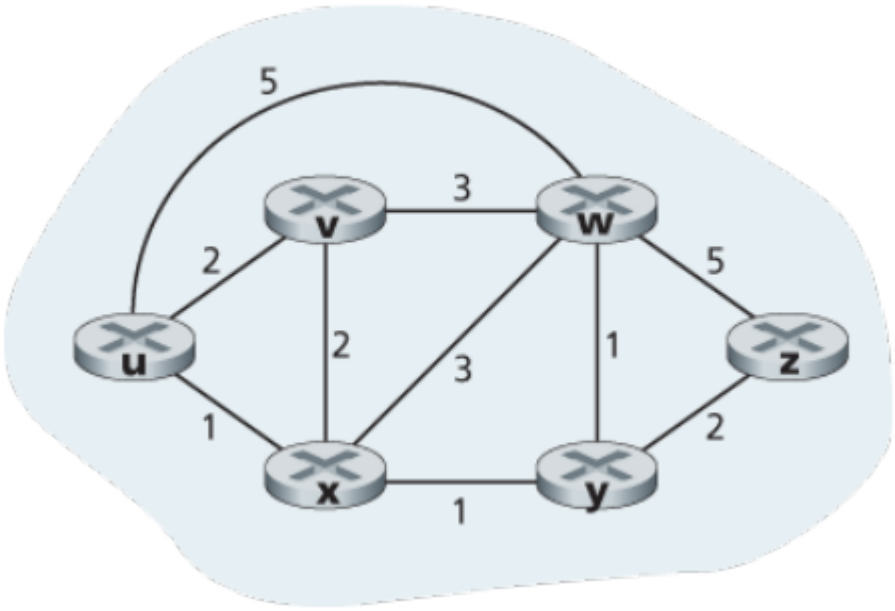


Table 5.1 Running the link-state algorithm on the network in Figure 5.3

step	N'	D (v), p (v)	D (w), p (w)	D (x), p (x)	D (y), p (y)	D (z), p (z)
0	u	2, u	5, u	1,u	∞	∞
1	ux	2, u	4, x		2, x	∞
2	uxy	2, u	3, y			4, y
3	uxyv		3, y			4, y
4	uxyvw					4, y
5	uxyvwz					

- In the first iteration, we need to search through all n nodes to determine the node, w, not in N′ that has the minimum cost. In the second iteration, we need to check n−1 nodes to determine the minimum cost; in the third iteration n−2 nodes, and so on. Overall, the total number of nodes we need to search through over all the iterations is n(n+1)/2, and thus we say that the preceding implementation of the LS algorithm has worst-case complexity of order n squared: O(n 2).
- Oscillations with congestion-sensitive routing
- a solution is to ensure that not all routers run the LS algorithm at the same time.

Distance Vector Routing algorithm

- it is decentralised
- each node receives some information from one or more of its directly attached neighbors, performs a calculation, and then distributes the results of its calculation back to its neighbors. It is iterative in that this process continues on until no more information is exchanged between neighbhours.
- x (y) be the cost of the least-cost path from node x to node y.
- dx(y)=minv{c(x,v)+dv(y)},
  read from 6.4

LINK LAYER

- the basic service of any link layer is to move a datagram from one node to an adjacent node(nodes like hosts,routers,switches) over a single communication link
- services provided by link layer are

1. Framing : Almost all link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link. A frame consists of a data field, in which the network-layer datagram is inserted, and a number of header fields
2. Link access : A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link.For point-to-point links that have a single sender and receiver the MAC protocol is simple (or nonexistent),sender sends whenever link is idle.for when multiple nodes share single broadcast link, (multiple access control problem), MAC protocol serves to coordinate the frame transmissions of the many nodes
3. Reliable delivery : link-layer reliable delivery service is often used for links that are prone to high error rates, such as a wireless link.link-layer reliable delivery can be considered an unnecessary overhead for low bit-error links, including fiber, coax, and many twisted-pair copper links. For this reason, many wired link-layer protocols do not provide a reliable delivery service.
4. Error detection and correction : sometimes bit errors are introduced in a link layer frame by factors like signal attenuation and electromagnetic noise.To detect such bit errors transmitting node include error-detection bits in the frame, and having the receiving node perform an error check

- for the most part the link layer is implemented in a network adapter, also sometimes known as a network interface card (NIC), while for a router it is implemented in router’s line card.much of the link layer functionality is impemented in hardware
- intels 710 adapter implements ethernet protocol, Atheros AR5006 implements 802.11 WiFi protocol
- network adapters are being integrated onto the host’s motherboar- a so-called LAN-on-motherboard configuration.

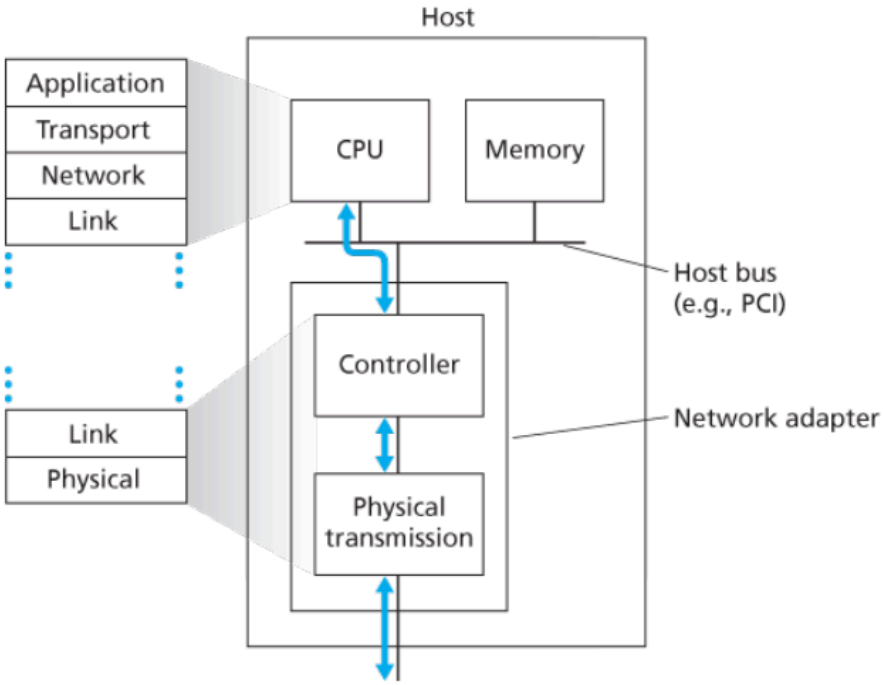


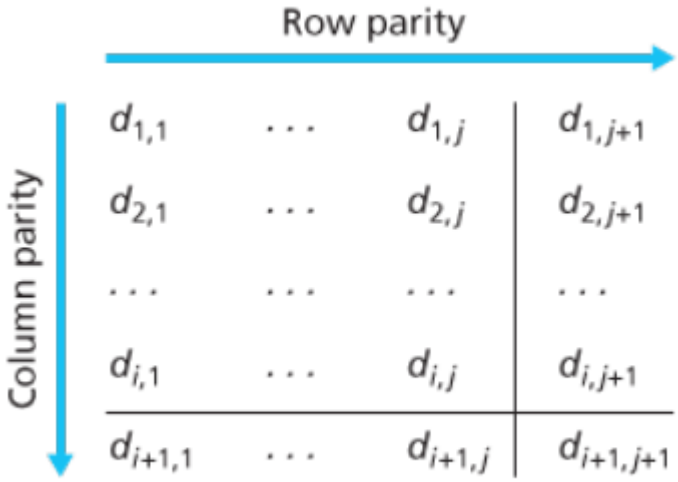
Figure 6.2 Network adapter: Its relationship to other host components and to protocol stack functionality

- while most of link layer is in hardware, the software component of link layer implement higher-level link-layer functionality such as assembling link-layer addressing information and activating the controller hardware while on receiving side, link-layer software responds to cotroller interrupts (e.g., due to the receipt of one or more frames), handling error conditions and passing a datagram up to the network layer.

Error correction and detection techniques

- three methods : parity checks (to illustrate the basic ideas behind error detection and correction), checksumming methods (which are more typically used in the transport layer), and cyclic redundancy checks (which are more typically used in the link layer in an adapter).
- parity check :
  - single dimensional parity : check if a row of bits has even number of 1's, if so parity bit is set to 0 else set to 1 (to preserve even parity). to detect erros check if that data + parity has even no of 1's , if it does no error else error.Note that if even number of bit erros occurs it goes undetected
  - two dimensional parity : here parity bit is generated both row wise and column wise in a similar manner as single dimensional parity(add row parity bit = 1 if row has odd no of 1,s and add column parity =1 if column has odd no of 1's to preserve even number of 1's) . In this case receiver can thus not only detect the fact that a single bit error

has occurred, but can use the column and row indices of the column and row with parity errors to actually identify the bit that was corrupted and correct that error



  - The ability of the receiver to both detect and correct errors is known as forward error correction (FEC).FEC techniques are valuable because they can decrease the number of sender retransmissions require.In network they can be used by themselves or in conjunction with ARQ (automatic repeat request like stop and wait or go back N ARQ) in data link layer
- checksumming :
  - bytes of data are treated as 16 bit integers and summed . The 1s complement of this sum then forms the Internet checksum that is carried in the segment header.The receiver checks the checksum by taking the 1s complement of the sum of the received data (including the checksum) and checking whether the result is all 1 bits.
  - In the TCP and UDP protocols, the Internet checksum is computed over all fields (header and data fields included)
  - In IP the checksum is computed over the IP header (since the UDP or TCP segment has its own checksum)
  - other protocol like XTP, one checksum is computed over the header and another checksum is computed over the entire packet.
  - Because transport-layer error detection is implemented in software, it is important to have a simple and fast error-detection scheme such as checksumming. On the other hand, error detection at the link layer is implemented in dedicated hardware in adapters, which can rapidly perform the more complex CRC operations
- cyclic redudancy check (CRC) :

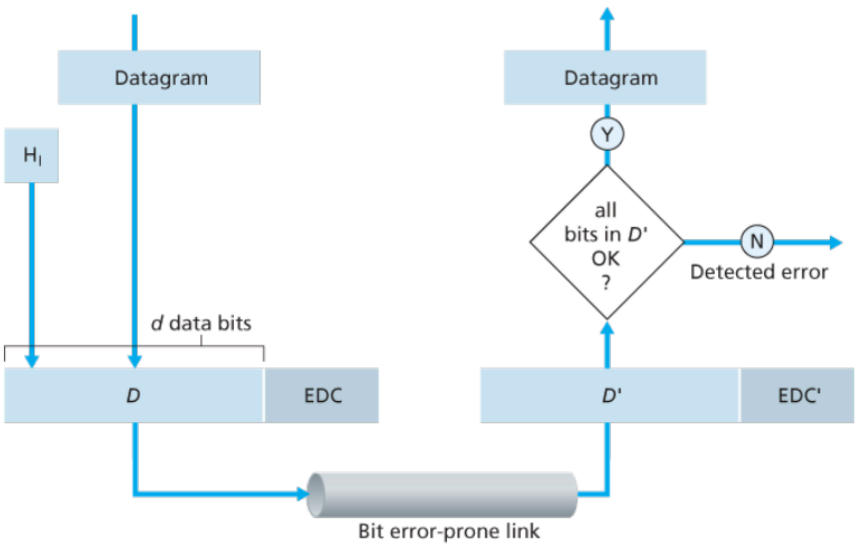


Figure 6.3 Error-detection and -correction scenario

- CRC codes are also known as polynomial codes, since it is possible to view the bit string to be sent as a polynomial whose coefficients are the 0 and 1 values in the bit string
- say that sending node wants to send D bit data to the receiving node.The sender and reciever first agree on an r+1 bit pattern, known as a generator , which we will denote as G.For a given piece of data, D, the sender will choose r additional bits, R, and append them to D such that the resulting D+R bit pattern (interpreted as a binary number) is exactly divisible by G (i.e., has no remainder) using modulo-2 arithmetic.
- The process of error checking with CRCs is thus simple: The receiver divides the D+R received bits by G. If the remainder is nonzero, the receiver knows that an error has occurred; otherwise the data is accepted as being correct.
- R can be generated on sender side by dividng (D bits + (r bits of 0s appended to D)) by G .The remainder of this operation is R. **R = (D * 2^r) % G** (note that multipling by 2^r means left shifting by r bits so r bits of 0 appended to D)
- All CRC calculations are done in modulo-2 arithmetic without carries in addition or borrows in subtraction. This means that addition and subtraction are identical, and both are equivalent to the bitwise exclusive-or (XOR) of the operands.module 2 arithmetic is like this ((2+3)%2=1,(3+3)%2=0)
- Multiplication and division are the same as in base-2 arithmetic,
- Each of the CRC standards can detect burst errors of fewer than r+1 bits. (This means that all consecutive bit errors of r bits or fewer will be detected.)
- a burst length greater than r+1 is detected with probability 1-0.5r
- each of the CRC standards (8,12,16 and 32 bit generators) can detect any odd number of bit errors

- The CRC-32 32-bit standard, which has been adopted in a number of link-leve IEEE protocols, uses a generator of GCRC-32=100000100110000010001110110110111

MULTIPLE ACCESS LINKS AND PROTOCOLS

- two types of links point to ppoint links (fr 1 sender-reciever ex : point to point protocol, high-level data link control (HDLC)) and broadcast link
- in case of broadcast link need to coordinate the access of multiple sending and receiving nodes to a shared broadcastchannel—the multiple access problem.(as frames can collide if multiple sender at same time wasting the broadcast channel)
- multiple access protocol as belonging to one of three categories: channel partitioning protocols, random access protocols, and taking-turns protocols.
- multiple access protocol must have the following desirable characteristics :
  - when one node sending throughtput is R bps , when M nodes sending each node must have R/M bps
  - protocol needs to be decentralised (no master node)
  - simple and inexpensive to implement

Channel partitioning protocols

- TDMA(time division multiple access)
  - total time is divided into time frames and further divides each time frame into N time slots.Each time slot is then assigned to one of the N node .slot sizes are chosen so that a single packet can be transmitted during a slot time
  - while each node can transmit upto R bps during its assigned time slot, it only gets a dedicated slot for a fraction of the total frame time (1/N), the average transmission rate is reduced to R/N bps of each node during each frame time.
  - drawbacks
    - node is limited to an average rate of R/N bps even when it is the only node with packets to send
    - node must always wait for its turn in the transmission sequence
- FDM(frequency division multiplE access) :
  - divides the R bps channel into different frequencies (each with a bandwidth of R/N) and assigns each frequency to one of the N nodes
  - drawback : a node is limited to a bandwidth of R/N, even when it is the only node with packets to send.
  - both fdm and tdm avoids collisions and divides the bandwidth fairly among the N

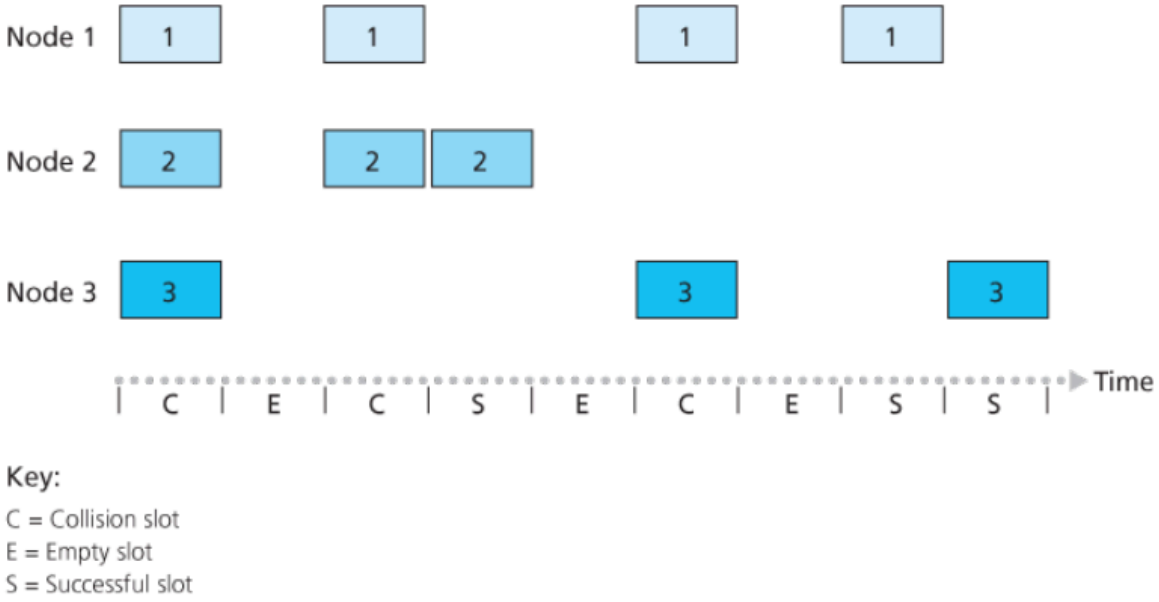
nodes

- CDMA (code division multiple access) :
  - at sending site, assigns a different code to each node. Each node then uses its unique code to encode the data bits it sends.
  - At the receiving end, a decoder separates the encoded signals based on their unique codes, filtering out the "noise" from other users
  - in this way different nodes can transmit simultaneously and yet have their respective receivers correctly receive a sender’s encoded data bits in spite of interfering transmissions by other nodes
  - mainly used for wireless channels,cellular telephony and military networks

Random access protocols

- transmitting node always transmits at the full rate of the channel, namely, R bps.
- When there is a collision, each node involved in the collision repeatedly retransmits its frame until its frame gets through without a collision.
- But when a node experiences a collision, it waits a random delay before retransmitting the frame. Each node involved in a collision chooses independent random delays so it is possible that one of the nodes will pick a delay that is sufficiently less than the delays of the other colliding nodes and will therefore be able to sneak its frame into the channel without a collision.
- ex: ALOHA,CSMA(ethernet is CSMA)
- slotted ALOHA(Advocates of Linux Open-source Hawaii Association) :
  - All frames consist of exactly L bits.
  - Time is divided into slots of size L/R seconds (that is, a slot equals the time to transmit one frame).
  - Nodes start to transmit frames only at the beginnings of slots.
  - The nodes are synchronized so that each node knows when the slots begin.
  - If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends.
  - When the node has a fresh frame to send, it waits until the beginning of the next slot and transmits the entire frame in the slot.
  - If there isn’t a collision, the node has successfully transmitted its frame and thus need not consider retransmitting the frame.
  - If there is a collision, the node detects the collision before the end of the slot. The node retransmits its frame in each subsequent slot with probability p until the frame is transmitted without a collision.
  - By retransmitting with probability p, we mean that the node effectively tosses a biased coin; the event heads corresponds to “retransmit,” which occurs with probability p, while

event of skipping and tossing coin in next slot occurs with probability 1-p
- a certain fraction of the slots will have collisions and will therefore be “wasted.”.the unwasted slots where exactly one node transmits is called successful slot.efficiency of slotted aloha is given by long run fraction of successful slots
- if say 1 node transmits (prob is p), N-1 dont transmit (1-p probablity for not transmit for each node).Therefore probabiliity one node has success is is 1x(p) x (N-1)(1−p) .probability that any one of the N nodes has a success is Np(1−p)N−1 .
- By finding p that maximises the equation we ll find that max efficiency is 0.37(1/e)
- That is, when a large number of nodes have many frames to transmit,then (at best) only 37 percent of the slots do useful work. Thus the effective transmission rate of the channel is not R bps but only 0.37 R bps



- ALOHA
  - this is exactly same as slotted ALOHA except the fact that it is unsloted.Here If a transmitted frame experiences a collision the node will then immediately retransmit the frame with probability p, otherwise waits for a frame transmission time
  - only difference between this and slotted aloha is that it doesnt hv slots to synchronise nodes
  - here maximum efficiency of the pure ALOHA protocol is only 1/(2e)—exactly half that of slotted ALOHA
- CSMA (Carrier Sense Multiple Access)
  - carrier sensing—a node listens to the channel before transmitting.If a frame from another node is currently being transmitted into the channel, a node then waits until it detects no transmissions for a short amount of time and then begins transmission.
  - collision detection—a transmitting node listens to the channel while it is transmitting. If it detects that another node is transmitting an interfering frame, it stops transmitting

and waits a random amount of time before repeating the sense-and-transmit-when-idle cycle.
    - if end-to-end channel propagation delay of a broadcast channel—the time it takes for a signal to propagate from one of the nodes to another— is high , then larger is the chance that carrier-sensing node is not yet able to sense a transmission that has already begun at another node in the network which will result in collision
- CSMA/CD(Carrier Sense Multiple Access with Collision Dection)
    - While transmitting, the adapter monitors for the presence of signal energy coming from other adapters using the broadcast channel(collision detection)
    - When a node performs collision detection, itc eases transmission as soon as it detects a collision
    - wait time must be optimal(f the interval is large and the number of colliding nodes is small, nodes are likely to wait a large amount of time (with the channel remaining idle) before repeating the sense-and-transmit-when-idle)
    - wait time given by binary exponential back off algorithm - when transmitting a frame that has already experienced n collisions, a node chooses the value of K at random from { 0,1,2,…2n−1}. Thus, the more collisions experienced by a frame, the larger the interval from which K ischosen.
    - For Ethernet, the actual amount of time a node waits is K·512 bit times (i.e., K times the amount of time needed to send 512 bits into the Ethernet) and the maximum value that n can take is capped at 10.
    - Efficiency=1/(1+(5dprop/dtrans))
    - where d prop denote the maximum time it takes signal energy to propagate between any two adapters.
    - Let d trans be the time to transmit a maximum-size frame

taking turns protocol

- polling protocol :
    - requires one node to be master node
    - master node polls each of the nodes in a round-robin fashion.ex : it sends message to node 1, saying it can transmit upto certain number of frames,after node 1 transmits , its sends message to node 2 , and the process goes on in a cyclic manner
    - drawback :
        - polling delay(time to notify a node that it can transmit).if only one node is active, then the node will transmit at a rate less than R bps, as the master node must poll each of the inactive nodes in turn each time the active node has sent its maximum number of frames

        - if master node fails entire channel is inoperative
    - ex : 802.15 protocol and the Bluetooth protocol
- token passing protocol :
    - no master node
    - a token is exchanged among the nodes in some fixed order.
    - If a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node
    - drawback :
        - failure of one node can crash the channel
        - if a node accidentally neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation
    - ex : fiber distributed data interface (FDDI) protocol, and IEEE 802.5 token ring protocol

DOCSIS: The Link-Layer Protocol for Cable Internet Access

- cable access network typically connects several thousand residential cable modems to a cable modem termination system (CMTS) at the cable network headend.
- DOCSIS - Data- Over-Cable Service Interface Specifications
- uses FDM to divide the downstream (CMTS to modem) and upstream (modem to CMTS) network segments.both are broadcast links
- downstream channel - 6MHz,40mbps , upstream channel - 6.4MHz,30Mbps
- each upstream channel is divided into intervals of time (TDM-like), each containing a sequence of mini-slots during which cable modems can transmit to the CMTS.
- The CMTS explicitly grants permission to individual cable modems to transmit during specific mini-slots by sending a control message known as a MAP message on a downstream channel to specify which cable modem (with data to send) can transmit during which mini-slot
- CMTS know which cable modems have data to send in the first place by having cable modems send mini-slot-request frames to the CMTS during a special set of interval mini-slots that are dedicated for this purpose
- these mini-slot- request frames are transmitted in a random access manner and so may collide with each other
- modem infers that its mini-slot-request frame experienced a collision if it does not receive a response to the requested allocation in the next downstream control message
- When a collision is inferred, a cable modem uses binary exponential backoff to defer the retransmission of its mini-slot-request frame to a future time slot.

SWITCHED LANS

- MAC adress is fixed and unique
- IEEE manages the MAC address space. In particular, when a company wants to manufacture adapters, it purchases a chunk of the address space
- it is 6 bytesn order for the layers to be largely independent building blocks in a network architecture, different layers need to have their own addressing scheme. We have now seen three types of addresses: host names for the application layer, IP addresses for the network layer, and MAC addresses for the link layer.
- ARP (Adress resolution protocol)
  - used to resolve IP adresses into MAC adresses
  - sender passes an ARP query packet to the adapter along with an indication that the adapter should send the packet to the MAC broadcast address, namely, FF-FF-FF-FF-FF-FF. The adapter encapsulates the ARP packet in a link-layer frame, uses the broadcast address for the frame's destination address, and transmits the frame into the subnet
  - The frame containing the ARP query is received by all the other adapters on the subnet, and (because of the broadcast address) each adapter passes the ARP packet within the frame up to its ARP module.
  - Each of these ARP modules checks to see if its IP address matches the destination IP address in the ARP packet. The one with a match sends back to the querying host a response ARP packet with the desired mapping.
  - The querying host can then update its ARP table and send its IP datagram,
  - this is used for sending datagrams within same subnet.
  - for sending datagram to sender in a diferent subnet , usually datagram is sent to the first hop router , the ip adress of which is given by DNS, given this ip adress , ARP is used to get the MAC adreess so that datagram can be sent to the router.the router adapter when it recieves this frame sees that the link-layer frame is addressed to it, and therefore passes the ip datagram extracted from the frame to the network layer of the router, where it consults the fowarding table to determine the correct interface on which the datagram is to be forwarded
  - . This interface then passes the datagram to its adapter, which encapsulates the datagram in a new frame and sends the frame into other subnet
  - note : ARP packet is encapsulated within a link-layer frame and thus lies architecturally above the link layer.However, an ARP packet has fields containing link-layer addresses and thus is arguably a link-layer protocol, but it also contains network-layer addresses and thus is also arguably a network-layer protocol.
  - conclusion : ARP is probably best considered a protocol that straddles the boundary between the link and network layers—not fitting neatly into the simple layered

protocol stack

Ethernet 802.3

- sending adapter encapsulates the IP datagram within an Ethernet frame andpasses the frame to the physical layer.
- The receiving adapter receives the frame from the physical layer, extracts the IP datagram, and passes the IP datagram to the network layer
- hub is a physical-layer device that acts on individual bits rather than frames. When a bit, representing a zero or a one, arrives from one interface, the hub simply re- creates the bit, boosts its energy strength, and transmits the bit onto all the other interfaces.Ethernet with a hub-based star topology is also a broadcast LAN
- ethernet was original;y bus-topology designs using coaxial cable

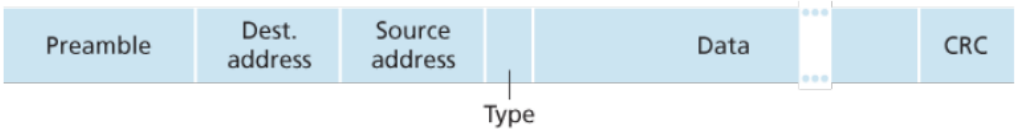


Figure 6.20 Ethernet frame structure

-
- 6 fields of ethernet are
  - data field : MTU of ethernet is 1500 bytes f the IP datagram exceeds 1,500 bytes, then the host has to fragment the datagram. the minimum size of the data field is 46 bytes. This means that if the IP datagram is less than 46 bytes, the data field has to be “stuffed” to fill it out to 46 bytes.network layer uses the length field in the IP datagram header to remove the stuffing.
  - destination MAC address : when receiving adapter received ethernet frame where destination MAC address matches itself, it passes to upper layer (i.e network layer) otherwise it discards it
  - source MAC address(6 bytes)
  - type field : permits Ethernet to multiplex network-layer protocols.type field is analogous to the protocol field in the network-layer datagram and the port-number fields in the transport-layer segment;each protocol has its standardised protocol number used for multiplexing (while sending) and demultiplexing (while receiving) .ex : if the arriving frame contains an ARP packet (i.e., has a type field of 0\x0806 hex), the ARP packet will be demultiplexed up to the ARP protocol
  - CRC (4bytes)
  - Preamble 8 bytes : consists of 7 bytes of 10101010 followed by 1 byte of 10101011.he first 7 bytes of the preamble serve to “wake up” the receiving adapters and to synchronize their clocks to that of the sender’s clock.A receiving adapter can

lock onto adapter A's clock simply by locking onto the bits in the first 7 bytes of the preamble. The last 2 bits of the eighth byte of the preamble (11)alert adapter that the "important stuff" is about to come.

- provide connectionless service to the network layer as no handshaking before sending.If a frame fails CRC check adapter discards the frame.reliability is determined by upper layer protocol like tcp or udp
- etherent comes in flavours like 10BASE-T, 10BASE-2, 100BASE-T, 1000BASE-LX, 10GBASE-T and 40GBASE-T.The first part represents speed like 10,20,100 gbps."BASE" refers to baseband Ethernet, meaning that the physical media only carries Ethernet traffic;the final part of the acronym refers to the physical media itself for ex a "T" refers to twisted-pair copper wires
- multiple access solved by CSMA\CD
- in a switch-based Ethernet LAN there are no collisions and, therefore, there is no need for a MAC protocol as switch coordinates its transmissions and never forwards more than one frame onto the same interface at any time

link layer switches :

- eliminate the need for multiple access protocols
- Filtering is the switch function that determines whether a frame should be forwarded to some interfaceor should just be dropped.
- Forwarding is the switch function that determines the interfaces to which a frame should be directed, and then moves the frame to those interfaces.
- Switch filtering and forwarding are done with a switch table.
- suppose a frame with destination address DD-DD-DD-DD-DD-DD arrives at the switch on interface x. The switch indexes its table with the MAC address DD-DD-DD-DD-DD-DD. There are three possible cases:
    - There is no entry in the table for DD-DD-DD-DD-DD-DD. In this case, the switch forwards copies of the frame to the output buffers preceding all interfaces except for interface x. In other words, if there s no entry for the destination address, the switch broadcasts the frame.
    - There is an entry in the table, associating DD-DD-DD-DD-DD-DD with interface x. In this case, the frame is coming from a LAN segment that contains adapter DD-DD-DD-DD-DD-DD. There being no need to forward the frame to any of the other interfaces, the switch performs the filtering function by discarding the frame. its discards the frame to prevent unnecessary traffic flow. This prevents the data from continuously looping back within the switch. (note that in this case at layer 2 it suspects theres loop so imeddiately doesnt discard,it finds the ip, confirms its loopback, then discards and prepares separate packet to send back to source)

    - There is an entry in the table, associating DD-DD-DD-DD-DD-DD with interface y≠x. In this case, the frame needs to be forwarded to the LAN segment attached to interface y. The switch performs its forwarding function by putting the frame in an output buffer that precedes interface y.
    - The switch deletes an address in the table if no frames are received with that address as the source address after some period of time (the aging time)
- advantages :
    - elimination of collisions: switches buffer frames and never transmit more than one frame on a segment at any one time .better performance than broadcast link
    - heterogenous links : switch isolates one link from another so different links can have different speeds.so it can mix ideal and legacy equipment
    - management: if an adapter malfunctions and continually sends Ethernet frames (called a jabbering adapter), a switch can detect the problem and internally disconnect the malfunctioning adapter.
- switch poisioning : an attack against a switch, where tons of packets sent to the switch with many different bogus source MAC addresses, thereby filling the switch table with bogus entries and leaving no room for the MAC addresses of the legitimate hosts. This causes the switch to broadcast most frames, which can then be picked up by the sniffer
- routers provide a more robust isolation of traffic, control broadcast storms, and use more “intelligent” routes among the hosts in the network as compared to switches but have larger per-packet processing time than switches, because they have to process up through the layer-3 fields and are not plug and play

VLAN (Virtual local area network)

- this is how typical hierarchical network looks like

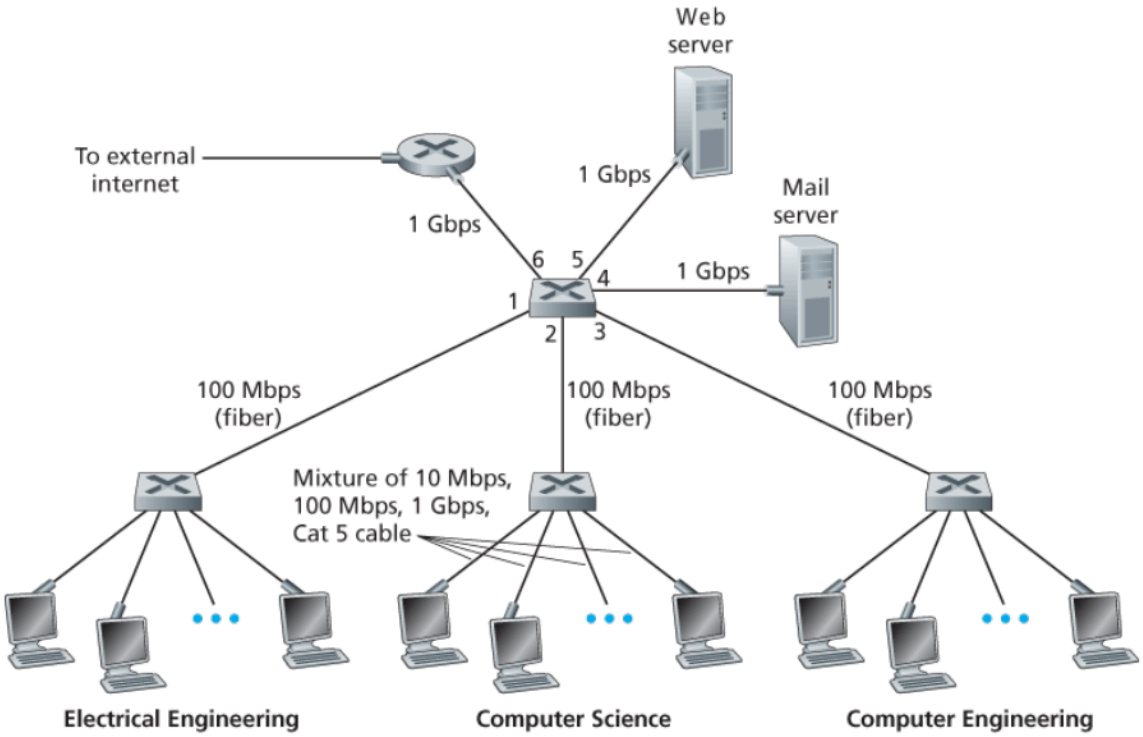


Figure 6.15 An institutional network connected together by four switches

- disadvantages of the above are :
  - lack of traffic isolation : Although the hierarchy localizes group traffic to within a single switch, broadcast traffic must still traverse the entire institutional network.This is undesirable for privacy reasons , ex : if one group has companys exec management team n and other group are employees running snifferes , then it is not desirable for executives' traffic to reach employee network
  - inneficient use of switches
  - managing users : an employee moves between groups, the physical cabling must be changed to connect the employee to a different switch
- instead of hierarchical networking we can use VLAN where port-based VLAN, the switch’s ports (interfaces) are divided into groups by the network manager. Each group constitutes a VLAN, with the ports in each VLAN forming a broadcast domain (i.e., broadcast traffic from one port can only reach other ports in the group).4
- =if one user wants to switch from one department to another dept then network operator simply reconfigures the VLAN software to reassign the port no

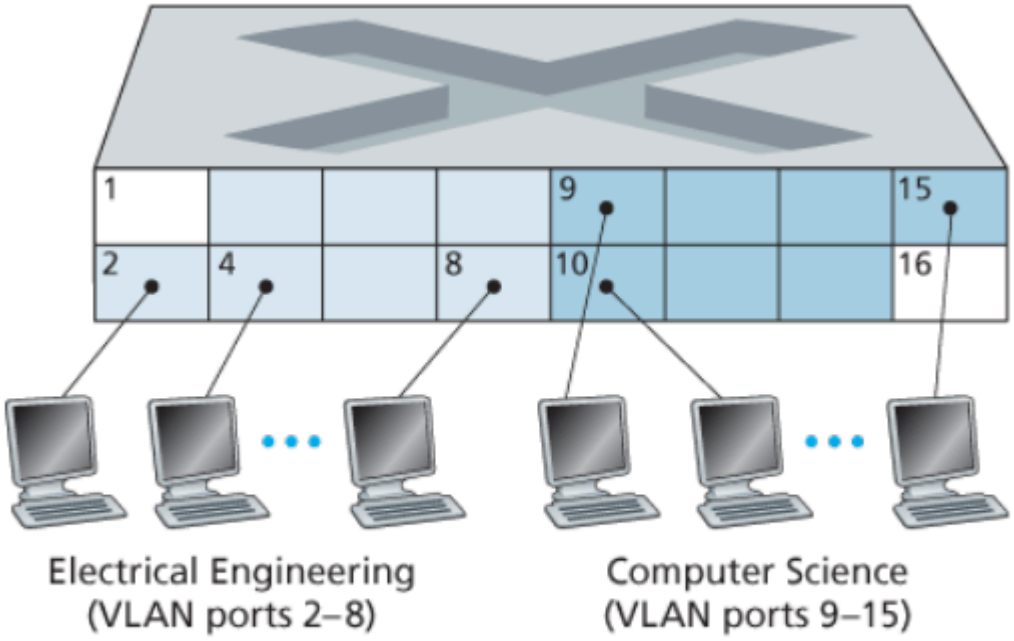


Figure 6.25 A single switch with two configured VLANs

- a more scalable way to interconnect VLAN switches is called VLAN trunking.a special port on each switch is configured as a trunk port to interconnect the two VLAN switches. The trunk port belongs to all VLANs, and frames sent to any VLAN are forwarded over the trunk link to the other switch
- The IEEE has defined an extended Ethernet frame format, 802.1Q, for frames crossing a VLAN trunk with a four-byte VLAN tag added into the header that carries the identity of the VLAN to which the frame belongs
- VLAN tag is added into a frame by the switch at the sending side of a VLAN trunk, parsed, and removed by the switch at the receiving side of the trunk.
- VLAN tag itself consists of a 2-byte Tag Protocol Identifier (TPID) field (with a fixed hexadecimal value of 81-00), a 2-byte Tag Control Information field that contains a 12-bit VLAN identifier field, and a 3-bit priority field that is similar in intent to the IP datagram TOS field.

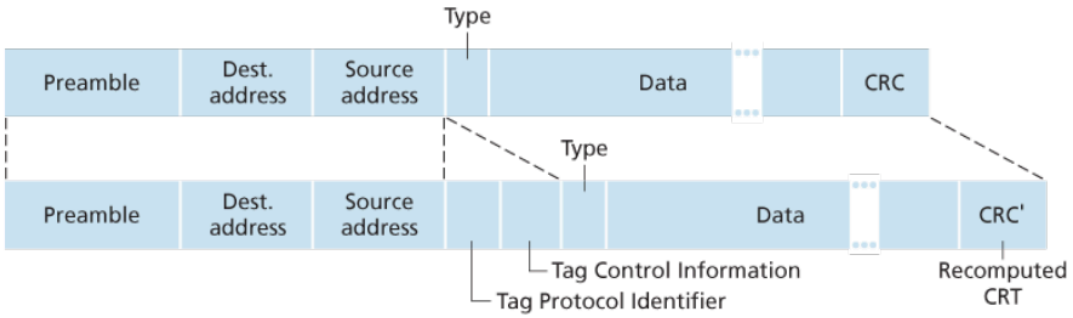


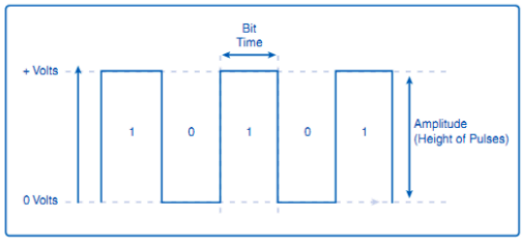
Figure 6.27 Original Ethernet frame (top), 802.1Q-tagged Ethernet VLAN frame (below)

```
note : BGP(Border Gateway Protocol) is an exterior gateway protocol,
meaning it operates between different autonomous systems. It's
responsible for exchanging routing information and establishing paths
for data packets to flow between these independent networks.
```

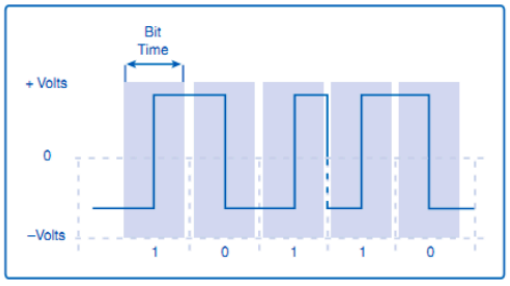
section 6.7 day in life of web page request is omited as we know it

COMPUTER NETWORKS

Signalling Methods



NRZ (Non Return to Zero) Encoding – A low voltage being 0 and a higher voltage representing a 1.



Manchester Encoding

- A voltage change from low to high within the bit time represents a 1.
- A voltage drop within the bit time from a high to a low voltage represents a 0.

WiFi: 802.11 Wireless LANs

- IEEE 802.11 wireless LAN, also known as WiFi , all use the same medium access

protocol, CSMA/CA

- operates at two different frequency ranges 2.4GHz(unlicensed,may compete with phones nd microwave ovens) and 5GHz(shorter transmn distance,suffer from multipath propagation)
- 802.11n and 802.11ac uses multiple input multiple-output (MIMO) antennas; i.e., two or more antennas on the sending side and two or more antennas on the receiving side that are transmitting/receiving different signals
- 802.11ac may use may transmit to multiple stations simultaneously, and use “smart” antennas to adaptively beamform to target transmissions in the direction of a receiver. This decreases interference and increases the distance reached at a given data rate

802.11 Architecture

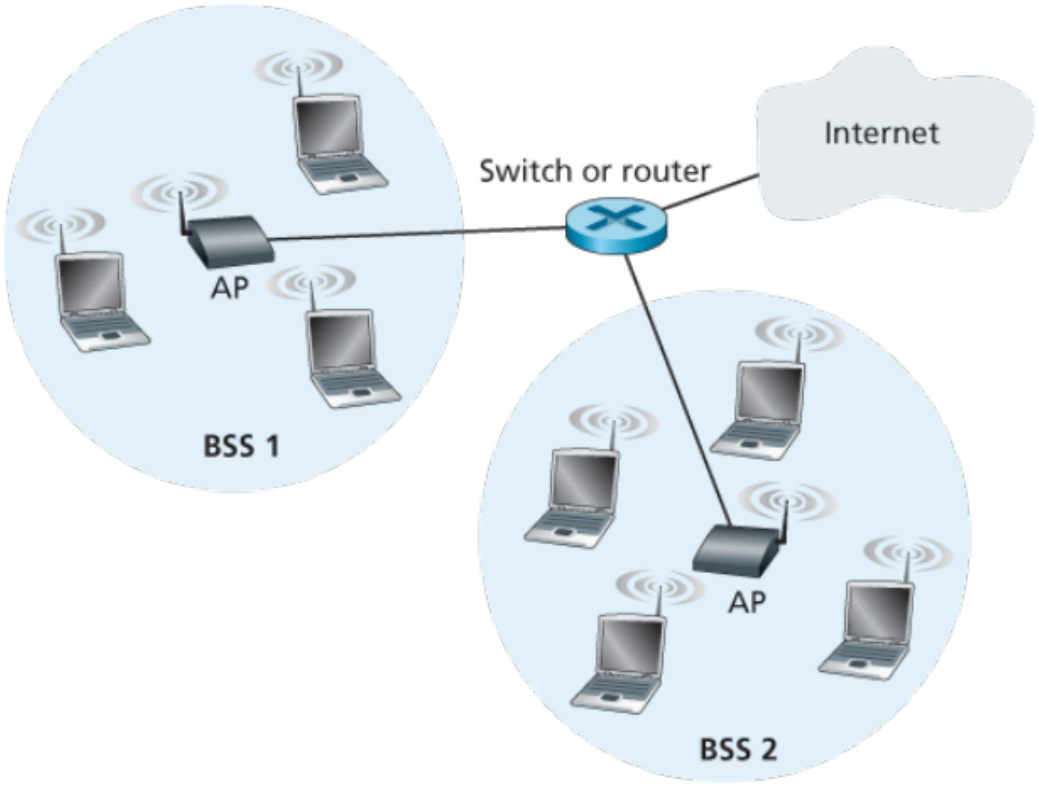
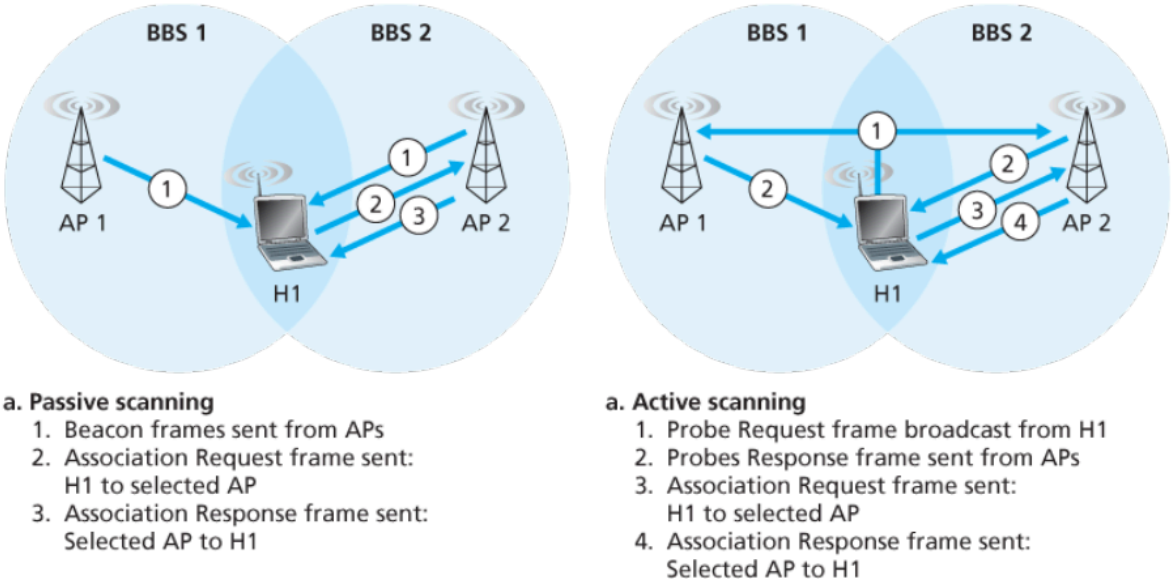


Figure 7.7 IEEE 802.11 LAN architecture

- above picture is an infrastruction network, as opposed to ad hoc networks which only connect to each other and dont have an access point
- fundamental block is basic service set (BSS). A BSS contains one or more wireless stations and a central base station, known as an access point (AP)
- note : Acess point is link layer device , so it only understands MAC address and not IP address

- station is wireless device like laptop which connects to a access point
- Each AP also has a MAC address for its wireless interface.each wireless station has MACC adress stored in firmware of stations adapter
- ad hoc network : a network with no central control and with no connections to the “outside world.”by mobile devices that have found themselves in proximity to each other, that have a need to communicate
- In 802.11, each wireless station needs to associate with an AP before it can send or receive network- layer data
- When a network administrator installs an AP, the administrator assigns a one- or two-word Service Set Identifier (SSID) to the access point and a channel number to the AP
- to understand channel numbers, recall that 802.11 operates in the frequency range of 2.4 GHz to 2.4835 GHz. Within this 85 MHz band, 802.11 defines 11 partially overlapping channels
- any two channels are non-overlapping if and only if they are separated by four or more channels.ex : This means that an administrator could create a wireless LAN with an aggregate maximum transmission rate of 33 Mbps by installing three 802.11b APs at the same physical location, assigning channels 1, 6, and 11 to the APs, and interconnecting each of the APs with a switch.
- A WiFi jungle is any physical location where a wireless station receives a sufficiently strong signal from two or more APs.To gain Internet access, wireless device needs to join exactly one of the subnets and hence needs to associate with exactly one of the APs
- The 802.11 standard requires that an AP periodically send beacon frames, each of which includes theAP’s SSID and MAC address. Your wireless device, knowing that APs are sending out beacon frames, scans the 11 channels, seeking beacon frames from any APs that may be out there.this is called passive scanning
- A wireless device can also perform active scanning , by broadcasting a probe frame that will be received by all APs within the wireless device’s range,device choses AP to associate with ,sends an association request frame to the AP, and the AP responds with an association response frame.
- authentication done on separate server



a. Passive scanning

1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1

a. Active scanning

1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

Figure 7.9 Active and passive scanning for access points

802.11 MAC PROTOCOL

- Once a wireless device is associated with an AP, it can start sending and receiving data frames to and from the access point. But because multiple wireless devices, or the AP itself may want to transmit data frames at the same time over the same channel, a multiple access protocol is needed to coordinate the transmissions
- unlike IEEE 802.3 ethernet which uses CSMA\CD, 802.11 uses CSMA\CA, and becaause of high bit error rates of wireless channels,802.11 (unlike Ethernet) uses a link-layer acknowledgment/retransmission (ARQ) scheme
- 802.11 doesnt implement collision detection for 2 reasons
  - because strength of the received signal is typically very small compared to the strength of the transmitted signal at the 802.11 adapter, it is costly to build hardware that can detect a collision.
  - adapter would still not be able to detect all collisions, due to the hidden terminal problem and fading.
    - hidden terminal problem : 2 devices are outside each other's range but can both communicate with a central access point (AP)..ex dev A is outside B but can communicate with AP, B is outside A but can communciate with access point. so Device A starts transmitting data to the AP, Device B won't be able to detect this transmission because they are not in each other's range.As a result, Device B might also try to transmit data to the AP at the same time, causing a collision at the AP where the signals from both devices overlap and become garbled.

        - fading problem **:** Wireless signals can be unpredictable due to various environmental factors like walls, buildings, and distance.
- Because 802.11wireless LANs do not use collision detection, once a station begins to transmit a frame, it transmits the frame in its entirety; that is, once a station gets started, there is no turning back
- when a station in a wireless LAN sends a frame, the frame may not reach the destination station intact for a variety of reasons. To deal with this non-negligible chance of failure, the 802.11 MAC protocol uses link-layer acknowledgments
- when the destination station receives a frame that passes the CRC, it waits a shortperiod of time known as the Short Inter-frame Spacing (SIFS) and then sends ACK frame.if transmitting staation doesnt recieve ACK , it assumes error occured and retrasmits frame usin CSMA\CA to access the channel.if ACK is not recieved after fixed number of transmissions frame is discarded
- 802.11 CSMA\CA
    - If initially the station senses the channel idle, it transmits its frame after a short period of time known as the Distributed Inter-frame Space (DIFS)
    - If the station detects a busy channel during the initial check or while waiting for DIFS, it enters the backoff phase.station chooses a random backoff value using binary exponential backoff and counts down this value after DIFS when the channel is sensed idle.While the channel is sensed busy, the counter value remains frozen.
    - When the counter reaches zero (note that this can only occur while the channel is sensed idle), the station transmits the entire frame and then waits for an acknowledgment.
    - if ACK received then send new frames starting from step 1 , if ACK isnt recieved reenter back off phase in step 2 and retransmit accordingly
    - Because 802.11 does not detect a collision and abort transmission, a frame suffering a collision will be transmitted in its entirety.thus to avoid collision whenever possible counter used even when channe idle (in CSMA\CD,two stations would each transmit as soon as they detect that the third station has finished transmitting, but in CD collision detection so frames aborted but remember this cant happen in CA as we dont detect collisions)
- in order to avoid hidden terminal problem , IEEE 802.11 uses a short Request to Send (RTS) control frame and a short Clear to Send (CTS) control frame to reserve access to the channel
    - when a sender wants to send a DATA it can first send an RTS frame to the AP, indicating the total time required to transmit the DATA frame and the acknowledgment (ACK) frame.(RTS frames are also usually broadcasted so that it can be heard by all stations in the frame)

- When the AP receives the RTS frame, it responds by broadcasting a CTS frame. This CTS frame serves two purposes: It gives the sender explicit permission to send and also instructs the other stations not to send for the reserved duration.this refrains other stations from sending data
- Although the RTS/CTS exchange can help reduce collisions, it also introduces delay and consumes channel resources. For this reason, the RTS/CTS exchange is only used (if at all) to reserve the channel for the transmission of a long DATA frame.
- In practice, each wireless station can set an RTS threshold such that the RTS/CTS sequence is used only when the frame is longer than the thresh

IEEE 802.11 FRAME

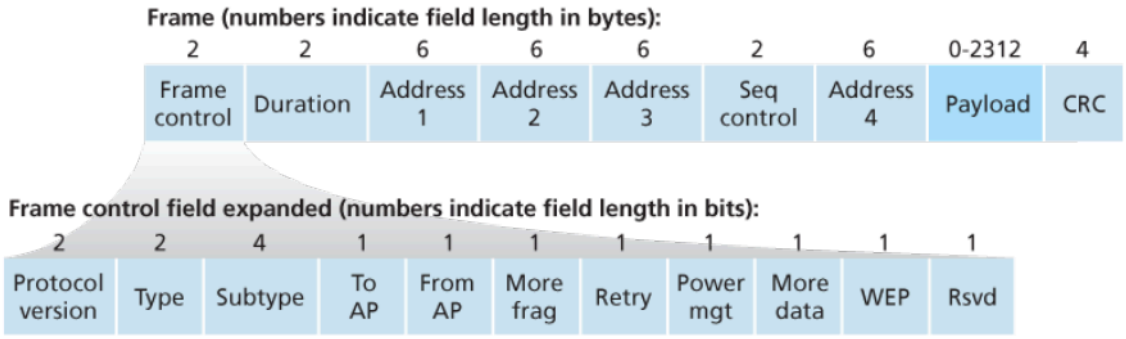


Figure 7.13 The 802.11 frame

- payload and CRC : payload, which typically consists of an IP datagram or an ARP packet. Although the field is permitted to be as long as 2,312 bytes, it is typically fewer than 1,500 bytes . 802.11 frame includes 32 bit CRC
- Adress fields :
  - address 2 : MAC address of the station that transmits the frame
  - address 1 : MAC address of the wireless station that is to receive the frame
  - address 3 : Address 3 contains the MAC address of this router interface which connects the BSS to other subnetss
  - address 4 : used when APs forward frames to each other in ad hoc mode
  - using the first picture under 802.11 architecture as reference consider the below ex where router R1 sends packet to H1
  - the router, which knows the IP address of H1 (from the destination address of the datagram), uses ARP to determine the MAC address of H1, just as in an ordinary Ethernet LAN. After obtaining H1’s MAC address, router interface R1 encapsulates the datagram within an Ethernet frame. The source address field of this frame contains R1’s MAC address, and the destination address field contains H1’s MAC addresss

    - When the Ethernet frame arrives at the AP, the AP converts the 802.3 Ethernet frame to an 802.11 frame before transmitting the frame into the wireless channel. The AP fills in address 1 and address 2 with H1’s MAC address and its own MAC address, respectively, as described above. For address3, the AP inserts the MAC address of R1. In this manner, H1 can determine (from address 3) theMAC address of the router interface that sent the datagram into the subnet.
- sequence control : use of sequence numbers allows the receiver to distinguish between a newly transmitted frame and the retransmission of a previous frame.
- duration : 802.11 protocol allows a transmitting station to reserve the channel for a period of time that includes the time to transmit its data frame and the time to transmit an acknowledgment, this is included in duration field
- frame control :
    - type, subtype : used to distinguish the association, RTS, CTS, ACK, and data frames
    - The to and from fields :used to define the meanings of the different address fields(meaning of adress field varies in infrastructure mode and ad hoc mode)
    - WEP : whether WEP encryption is used or not
        - WEP is wired equivalent privacy.it uses a shared key (either 40-bit or 104-bit) to encrypt data packets transmitted over the wireless network.but this key was static which means same key was used to encrypt all communication on the network.this is vulenrable
        - modern Wi-Fi networks should use WPA2 or the latest standard, WPA3, for secure communication.WPA replaced WEP's weak encryption algorithms with TKIP (Temporal Key Integrity Protocol) which introduces dynamic key generation making it much harder to crack the code compared to WEP's static key.
- mobitlity within same subnet : when H1 Moves from BSS1 to BSS2 (assumning BSS1 and 2 are interconnected via switch so part of same subnet , dont need to change IP) As H1 wanders away from AP1, H1 detects a weakening signal from AP1 and starts to scan for a stronger signal. H1 receives beacon frames from AP2 . H1 then disassociates with AP1 and associates with AP2, while keeping its IP address and maintaining its ongoing TCP sessions.switches are self learning so fowarding tables are accordingly updated