RED NOTES

UNIT 6.- NETWORK LAYER

1.-INTRODUCTION

The **network layer** oversees transporting segments from sending to receiving hosts. On sending side encapsulates segments into datagrams. On receiving side, delivers segments to transport layer. The network layer protocols are in every host or router.

In order to carry packages through the network, the **IP protocol** is in charge of these problems:

- Identifying with addresses of the devices that intervene in the communication (IP addresses).
- Choosing a route in the network that allows you to reach the destination (routing).

The two key network layer functions are:

- **Forwarding**: moving packets from router's input to appropriate router output (router local action).
- **Routing**: determining the route taken by packets from source to destination (network wide process).

As usual, Internet's network layer provides **best-effort service**, that is:

- Timing between packets is not guaranteed to be preserved.
- Packets are not guaranteed to be received in the order in which they were sent.
- Eventual delivery of transmitted packets is not guaranteed.

2.-VIRTUAL CIRCUIT AND DATAGRAM NETWORKS

Datagram network provides network-layer **connectionless** service (like UDP).

Virtual circuit network provides network-layer **connection** service (like TCP).

Both are similar to the transport-layer services, although:

- **Service**: host-to-host.
- **No choice**: network provides one or the other.
- **Implementation**: in network core.

The virtual circuit model has three phases:

1. Connection establishment, circuit set up.
2. Data transfer, circuit is used.
3. Connection teardown, circuit is deleted.

Each packet carries VC identifier (not destination host address). Every router on source-destination path maintains the "state" for each passing connection.

A virtual circuit consists of:

- **Path** from source to destination.

- **VC numbers**, one number for each link along path, it can be changed on each link.
- **Entries in forwarding tables** in routers along path

Advantages:

- Less header overhead.

Disadvantages:

- At least 1 RTT delay before sending data.
- Routers must store status information about VCs
- If a link fails, the connection falls and it must be re-established.
- Buffer space reservation in routers to store packages if necessary.

Datagram VS Virtual circuits summary:

Issue	Datagrams	Virtual circuits
Setup phase	Not needed	Required
Router state	Per destination	Per connection
Addresses	Packet carries full address	Packet carries short labels
Routing	Per packet	Per circuit
Quality of service	Difficult to add	Easier to add

Longest prefix matching: when looking for forwarding table entry for given destination address, use longest address prefix that matches destination address.

3.-IP: INTERNET PROTOCOL

IPv4 datagram fields:

- Version number (4 bits).
- Header length (4 bits), expressed in words of 32 bits (min = 5).
- Datagram length (16 bits), measured in bytes.
- Type of service (8 bits), 3 bits for the priority (ignored), 4 bits for the type of service (only one bit to 1) and 1 bit to zero.
- Time-to-live, this field is decremented by one each time the datagram is processed by a router. It is dropped once 0 is reached.
- Protocol, it indicates the protocol of the datagram encapsulated: TCP (6), ICMP (1) and UDP (17).
- Header checksum, it must be recomputed and stored again at each router.
- Options.

IP address is 32-bit identifier for host, router interface.

An **interface** is a connection between host/router and physical link.

There is one IP address associated with each interface.

IP addresses v4 are represented as four decimal numbers obtained from the four bytes that make up the IP address. Each IP address has two fields: **Network identifier** and **Host identifier**.

Special IP Addresses:

- **Network IP Address**: Network identifier + All 0s
- **Loopback Address**: 127 + any value (localhost).
- **Host Address**: All 0s + All 0s (it is used when the host obtains its IP address automatically).
- **Directed Broadcast Addresses**: Network identifier + All 1s (to send to all host connected to this network).
- **Limited Broadcast Addresses**: All 1s + All 1s (to send to all computers on the network to which is connected the sending host).

There are two types of Internet addressing, depending on how it determines the length of the network prefix:

- **Classful IP addressing**: can take only the predefined number of bits 8, 16 or 24.
- **Classless IP addressing**: any number of bits can be assigned, but it requires a network mask.

Addresses within a private address space will only be unique within the private network. Routers don't route private addresses out into the Internet. The private address ranges are:

- 192.168.0.0/16
- 172.16.0.0/12
- 10.0.0.0/8

Subnet: give bits from the host to the network in order to divide this one.

Subnets can physically reach each other without intervening the router.

Route aggregation: use the common bits as netmask.

Hierarchical addressing allows efficient advertisement of routing information.

The **forwarding tables** contain information about possible destination networks and how to reach them. They should be compact and have only information about destination networks and the next router to reach them. The information in the forwarding tables is:

Destination network | Netmask | Route (next hop) | Output interface

4.-ROUTING ALGORITHMS

Classification of routing algorithms:

- **Global**: all routers have complete topology and link cost information.
- **Decentralized**: routers know physically-connected neighbours and link costs to neighbours. It is an iterative process of computation and exchange of information with neighbours.
- **Static**: routes change slowly over time.
- **Dynamic**: routes change more quickly.

Bellman-Ford equation:

Let:

$d_x(y)$ = cost of least-cost path from x to y.

Then:

$$d_x(y) = \min(c(x,v) + d_v(y))$$

From time-to-time, each node sends its own distance vector estimate to neighbours. When x receives a new distance vector estimate from neighbour, it updates its own distance vector using B-F equation.

Each node waits for a change in local link cost or a message from a neighbour, then recomputes the estimates and finally, if the distance vector to any destination has changed, it notifies its neighbours.

Considering cost changes:

- Good news travels fast.
- Bad news travels slow.

Solutions to a routing loop caused by a “count to infinity” problem:

- Limiting the diameter of the network.
- Poisoned reverse with Split horizon.

Split horizon: prohibiting a node from advertising a node back onto the interface from which it was learned.

Poisoned reverse: sets the number of cost to the unconnected node to a number that indicates “infinite”.

A Link-State routing algorithm: **Dijkstra’s Algorithm**.

```
Initialization:
    N' = {u}
    for all nodes v
        if v adjacent to u
            then $D(v) = c(u,v)$
            else $D(v) = \infty$
Loop
    find w not in N' such that D(w) is a minimum
    add w to N'
    update D(v) for all v adjacent to w and not in N’:
        $D(v) = \min( D(v), D(w) + c(w,v) )$
until all nodes in N'
```

Notation:

- c(x, y): link cost from node x to y.
- D(v): current value of cost of path from source to destination v.

- p(v): predecessor node along path from source to v.
- N’: set of nodes whose least cost path definitively known.

In order to have a hierarchical routing, we have to collect routers into regions, “autonomous systems” (AS). Each AS is within an ISP. The routers in the same AS run the same routing protocol, the “intra-AS” routing protocol.

Gateway router: it is a router at “edge” of its own AS that has a link to another router in another AS.

The forwarding table is configured by both intra and inter-AS routing algorithm:

- Intra-AS sets entries for internal destinations.
- Inter-AS and intra-AS sets entries for external destinations.

Hot potato routing: send packet towards closest of two routers.

5.-ROUTING IN THE INTERNET

The most common intra-AS routing protocols or **interior gateway protocols** (IGP) are:

- **RIP**: Routing Information Protocol.
- **OSPF**: Open Shortest Path First.
- **IGRP**: Interior Gateway Routing Protocol.

RIP uses UDP (port 520) and the implementation of the distance vector algorithm is:

- The distance is measured in hops (max = 15) and each link has cost 1.
- Distance vector is exchanged with neighbours every 30 seconds in response message (**advertisement**).
- Each advertisement lists up to 25 destination **subnets**.

If no advertisement is heard after 180 seconds, then the neighbour/link is declared dead, that starts these steps:

1. Routes via neighbour are invalidated.
2. New advertisements are sent to neighbours.
3. Neighbours in turn send out new advertisements if tables have changed.
4. Link failure information quickly propagates to entire net.
5. Poison reverse is used to prevent ping-pong loops (infinite distance = 16 hops).

OSPF uses link state algorithm. Its advertisements carry one entry per neighbour and are flooded to the entire AS (directly over IP). The network administrator decides the criteria to define the cost.

OSPF “advanced” features:

- **Security**: all OSPF messages are authenticated.
- **Multiple** same-cost **paths** allowed.
- For each link, there are multiple cost metrics for different ToS.
- Integrated **uni** and **multicast** support.
- **Hierarchical** OSPF in large domains.

The hierarchical OSPF is divided in two levels: **local area** and **backbone**. The link-state advertisements are only in the area. Each node has the detailed area topology, that is, only knows the shortest path to nets in other areas.

The **area border routers** summarize distances to nets in own area and advertise to other are border routers

The **backbone routers** run OSPF routing limited to the backbone.

The **boundary routers** connect to another AS's.

The Internet **inter-AS** routing **BGP** has different goals for different types of routing:

- Intra-AS: performance.
- Inter-AS: reachability.

BGP (Border Gateway Protocol) is the *de facto* inter-domain routing protocol. BGP provides each AS a mean to:

- Obtain subnet reachability information from neighbouring AS's.
- Propagate reachability information to all AS-internal routers.
- Determine "good" routes to other networks based on reachability information and policy.

It allows to subnets to advertise its existence to rest of Internet.

Basics of BGP:

- Uses TCP port 179.
- It is a path vector algorithm, similar to distance vector but with full paths. As it works with full paths, it prevents routing loops.
- Routers do not need to share a direct physical link.

6.-IPv6

IPv6 datagram has a fixed-length of 40 bytes header and the fragmentation is not allowed. This version was created as 32-bit addresses are not enough and the headers of this versions helps to speed the processing and forwarding.

The address is of 128 bits and is written in hexadecimal notation separated by ":". It includes a zero compression technique, then a sequence of zeros is replaced by a pair of ":" (only once). It uses CIDR notation (IPv6 Address / x).

Type of addresses:

- **Unicast**: address of a computer.
- **Multicast**: address of a group of computers (all).
- **Anycast**: address of a group of computers (anyone of the group).

The IPv6 datagram format adds this fields:

- **Priority**: identify priority among datagrams in flow.
- **Flow label**: identify datagrams in same flow.

- **Next header**: identify upper layer protocol for data.

And changes from IPv4:

- **Checksum**: removes entirely to reduce processing time at each loop.
- **Options**: allowed, but outside of header, indicated by “Next header” field.
- **ICMPv6**: new version of ICMP.

Not all routers can be upgraded to IPv6, thus the **tunnelling** technique is used. This technique is based on carry the IPv6 datagram as **payload** in IPv4 datagram among IPv4 routers.

UNIT 7.- LINK LAYER

1.-INTRODUCTION, SERVICES

Terminology:

- **Nodes**: hosts and routers.
- **Links**: communication channels that connect adjacent nodes along communication path (wired links, wireless links or LANs).
- **Frame**: layer packet, encapsulates datagram.

Data-link layer has the responsibility of transferring datagram from one node **to physically adjacent** node over a link.

Datagrams are transferred by different link protocols over different links. Each link protocol provides different services.

Link layer **services**:

- **Framing, link access**: encapsulate datagram into frame, adding header and trailer. “MAC” addresses are used in frame headers to identify source and destination.
- **Reliable delivery between adjacent nodes**. Wireless links have a high error rate.
- **Flow control**: pacing between adjacent sending and receiving nodes.
- **Error detection**: errors caused by signal attenuation or noise. Receiver detects presence of errors.
- **Error correction**: receiver identifies **and corrects** bit error(s) without resorting to retransmission.
- **Half-duplex and full-duplex**: with half duplex, nodes at both ends of link can transmit, but not at same time.

The link layer is implemented in each and every host as an “adaptor” or **network interface card**, or on a chip. It is a combination of hardware, software and firmware.

Adaptors communicating:

- Sending side encapsulates datagram in frame and adds error checking bits, rdt, flow control, etc.
- Receiving side looks for errors, rdt, flow control, etc. and extracts datagram and passes it to upper layers.

2.-ERROR DETECTION, CORRECTION

Error detection is not 100% reliable, protocol may miss some errors, but rarely. Larger Error Detections and Correction Bits field yields better detection and correction.

Parity checking: **single bit parity** detects single bit errors. The parity bit is a value added at the end that states if the numbers of 1’s send is even or odd of a given byte.

In **Internet Checksum**, the goal is to detect “errors” in transmitted packet:

- Sender treats segment contents as a sequence of 16-bit integers. The checksum is the addition in one's complement of segment contents. Sender puts checksum value into UDP checksum field.
- Receiver computes checksum of received segment and checks if that one equals the checksum of the field value.

Cyclic Redundancy Check (CRC) is a more powerful error-detection coding. It views data bits as a binary number (D). It chooses a r+1 bit pattern or generator (G). The goal is to choose r CRC bits (R), such that:

- <D,R> is exactly divisible by G (moduli 2).
- Receiver knows G, divides <D,r> by G. If non-zero remainder, then a error is detected.
- Can detect all burst errors less than r+1 bits.

The mathematical foundations of CRC are complex, but hardware implementation is simple. Simply with shift registers and XOR gates.

In order to correct the mistakes, you can use two strategies:

- **FEC (Forward Error Correction)**: adding enough information that the receiver can recover the correct information (detection + recovery). Two-dimensional bit parity.
- **ARQ (Automatic Repeat reQuest)**: the receiver asks the transmitter to forward the correct information (detection + forward). Acknowledgements.

3.-MULTIPLE ACCESS PROTOCOLS

There are two types of "links":

- **Point-to-point**.
- **Broadcast (shared wire or medium)**.

Multiple access protocols:

- Single shared broadcast channel.
- Two or more simultaneous transmissions by nodes. There is **collision** if a node receives two or more signals at the same time.

A **multiple access protocol** is a distributed algorithm that determines how nodes share channel and when a node can transmit. The communication about channel sharing must use the channel itself.

In a **frame collision**, all the frames involved are lost. The broadcast channel is wasted during the collision interval.

An ideal multiple access protocol, given a broadcast channel of rate R bps:

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

There are three broad classes of MAC protocols:

- **Channel partitioning**: divide the channel into smaller "pieces" and allocate piece to node for exclusive use.
- **Random access**: the channel is not divided, allows collisions (recovering) and nodes try to obtain the channel without any control.
- **Taking turns**: nodes take turns, but nodes with more to send can take longer turns.

Channel partitioning MAC protocols:

- **TDMA (Time Division Multiple Access)**: it shares the broadcast channel in time, the access to the channel is in "rounds" and each station gets fixed length slot in each round. Unused slots go idle.
- **FDMA (Frequency Division Multiple Access)**: the channel spectrum is divided into frequency bands and each station has assigned a fixed frequency band. Unused transmission time in frequency bands go idle.

Advantages:

- It eliminated collisions.
- It divides the bandwidth fairly among the N nodes.

Drawbacks:

- A node is limited to an average rate of R/N bps.
- A node must always wait for its turn in the transmission sequence.
- Both points happen even when a node is the only node with packets to transmit.

In **random access protocols**, a node's decision to transmit is made independently of the activity of other nodes attaches to the broadcast channel. When a node has a packet to send, it transmits at full channel data rate R and no a priori coordination among nodes. When two or more transmitting node, it occurs a collision. This protocol specifies:

- How to detect collisions.
- How to recover from collisions.

CSMA, listen before transmitting:

- If channel senses idle: transmit entire frame.
- If channel sensed busy: defer transmission.

CSMA/CD, carrier sensing, deferral as in CSMA. Collisions are detected within short time and colliding transmission are aborted, reducing channel wastage. Collision detection:

- Easy in wired LANs: measure signal strengths, compare transmitted, received signals.
- Difficult in wireless LANs: received signal strength overwhelmed by local transmission strength.

Collisions can still occur: propagation delay means two nodes may not hear each other's transmission. If there is collision, the entire packet transmission time is wasted.

Ethernet CSMA/CD algorithm:

1. NIC receives datagram from network layer, creates frame.

2. If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle then transmits.
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame.
4. If NIC detects another transmission while transmitting, aborts and sends jam signal
5. After aborting, NIC enters binary (exponential) backoff:
    - After nth collision, NIC chooses K at random form {0,1,2,…,2^{m-1}}. NIC waits K * 512 bit times, returns to Step 2. m = min(n, 10).
    - Longer backoff interval with more collisions.

CSMA/CD efficiency:

- T_{prop} = max prop delay between 2 nodes in LAN.
- T_{trans} = time to transmit max-size frame.

$$efficiency = \frac{1}{1 + 5 * t_{prop}/t_{trans}}$$

Channel partitioning MAC protocols:

- Share channel **efficiently** and **fairly** at **high load**.
- **Inefficient at low load**: delay in channel access, I/N bandwidth allocated even if only there is one active node.

Random access MAC protocols:

- **Efficient** at **low load**: single node can fully utilize channel.
- High load: **collision overhead**.

"**Taking turns**" MAC protocols:

- **Polling**: master node "invites" slave nodes to transmit in turn. Typically used with "dumb" slave services. Some concerns are polling overhead, latency and single point of failure (master).
- **Token passing**: control **token** passed from one node to next sequentially. Token message. Some concerns are token overhead, latency, single point of failure (token).

4.-LANS

Network classification:

- WAN: Wide Area Network.
- MAN: Metropolitan Area Network.
- LAN: Local Area Network.
- PAN: Personal Area Network.

LANs broadcasts data at high data transfers rates with very low error rates. The main LAN technologies are 802.3 Family, Ethernet, and 802.11, Wi-Fi.

MANs cover greater distances at higher data rates than LANs. They usually interconnect a number of LANs using a high-capacity backbone technology.

WANs cover a large geographical area. They often connect multiple smaller networks, such as LANs or MANs. The world's most popular WAN is the Internet.

A **collision domain** is a set of stations that are affected in a collision (whether they participate in it or not).

A **broadcast domain** is a set of stations that receive a broadcast made by any of them.

4.1.-INTERNETWORKING DEVICES

A **repeater** is an electronic device that regenerates the signal to reach farther. It interconnects two or more LAN segments. The repeater does not understand the format of the frame, or physical addresses.

Hubs are multiport repeaters.

Repeaters or hubs do not separate collision domain and cannot support multiple LAN technologies as they can't interconnect between different rates or formats.

A **bridge** interconnects segments of a single LAN and separates collision domains.

Switches are multiport bridges. The main function of a switch is to forward any frame whose source and destination are on different sides of the switch. They do not analyse the frame data, only the physical addresses. When a switch forwards a frame, it uses the original source address. The switch is called "transparent" because you can plug it and forget it. It is effective, and its actions are invisible to user.

How the switches learn where a station with a particular MAC address is located:

- The switch watches all the traffic at each of its ports.
- The switch notes the source MAC address of each frame and the port at which the frame was observed.
- The switch adds what it learns to a table called filtering table. Learned entries also are called dynamic entries.

The processing steps are:

- If frame's destination is in the filtering table and is reached through the arrival port, the switch discards the frame.
- If the frame's destination is in the filtering table and its exit port is different from the arrival port, the switch forwards the frame through the exit port.
- If the frame's destination is not in the filtering table, the switch forwards the frame through all ports other than the arrival port.

A switch makes possible to build mixed-speed LAN. It can also amplify the bandwidth available. The switch does not separate broadcast domains. Switches have to build a spanning tree topology because they forward packets according to MAC addresses which are not structured, and they do not detect frames that loop. The spanning tree algorithm reduces the active topology to a tree.

Routers traffic to and from LANs. It provides total flexibility in building a network topology, as they do not have to build a spanning tree since they forward packets according to IP addresses which are structured and eventually discard packets that loop. Routing decisions are taken based on IP addresses:

- IP network addresses that start with the same prefix belong to the same LAN.
- An IP system decides whether a destination is on its LAN by comparting its own address prefix with the destination's address prefix:
    - If the source and destination address prefix match, both systems are on the same LAN. The next step is to discover the destination's link layer MAC address.
    - An IP system discovers the MAC address of a destination on its LAN by broadcasting an Address Resolution Protocol (ARP) message that asks the owner of a specific IP address to respond.

Routers separate collision and broadcast domain. Each router port is a broadcast domain. They perform software processing of received packets:

- Modify IP header.
- Routers can generate ICMP packets.
- Routers run routing algorithms.
- Router generates a new frame and changes the source MAC address of the received frame by its own MAC address.

Switches and routers, both are store-and-forward:

- Routers: network-layer devices.
- Switches: link-layer devices.

Also, both have forwarding tables:

- Routers: compute tables using routing algorithms, IP addresses.
- Switches: learn forwarding table using flooding, learning, MAC addresses.

4.2.-ETHERNET

Ethernet (IEEE 802.3) is the "dominant" wired LAN technology:

- Cheap.
- First widely used LAN technology.
- Simpler.
- Kept up with speed race.

Physical topology:

- **Bus** (90s): all nodes in same collision domain can collide with each other.
- **Star** (today): active **switch** in centre and each "spoke" runs a Ethernet protocol (nodes do not collide with each other).

Sending adapter encapsulates IP datagram in **Ethernet frame**:

- **Preamble**: synchronization.
- **Type**: indicates the higher layer protocol.
- **CRC**: cyclic redundancy check.
- **Addresses**: 48-bit source and destination MAC addresses:

    - The source address is the unicast address of the station that sent the frame.
    - Receiver’s adaptor passes frame to network-level protocol.
    - Addresses are globally unique.
- **Data**: maximum, 1500 bytes, minimum, 46 bytes (+14 bytes header + 4 bytes trailer = 512 bits).

Ethernet characteristics:

- **Connectionless**: no handshaking between sending and receiving NICs.
- **Unreliable**: receiving NIC doesn’t send ACKs or NACKs to send NIC.
- Unslotted **CSMA/CD with binary backoff**.

4.3.-WIFI

Elements of a wireless network:

- **Wireless hosts**: may be stationary or mobile.
- **Base station**: typically connected to wired network. They are responsible for sending packets between wired network and wireless host(s) in its “area”.
- **Wireless link**: typically used to connect mobile(s) to base station. They are also used as backbone link. They offer multiple access protocol coordinates link access, various data rates and transmission distance.
- **Infrastructure mode**: base station connects mobiles into wired network. **Handoff**: mobile changes base station providing into wired network.
- **Ad hoc mode**: no base stations. Nodes can only transmit to other nodes within link coverage. Nodes organize themselves into a network: route among themselves.

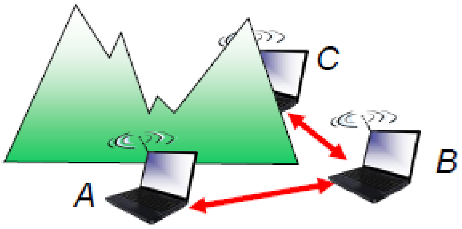
Wireless link characteristics have **important** differences from wired link:

- **Decreased signal strength**: radio signal attenuates as it propagates through matter (path loss).
- **Interference from other sources**: standardized wireless network frequencies shared by other devices. Devices (motors) interfere as well.
- **Multipath propagation**: radio signal reflects off objects ground, arriving ad destination at slightly different times.

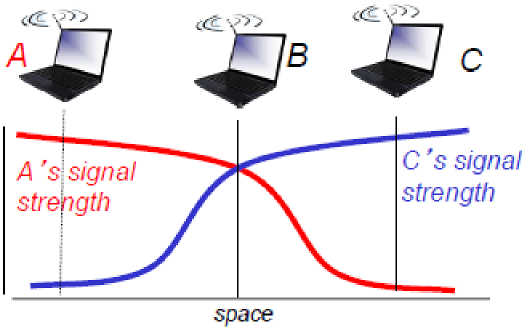
All these characteristics make communication across wireless link much more difficult.

Multiple wireless senders and receivers create additional problems:

- **Hidden terminal problem**.



- **Signal attenuation**.



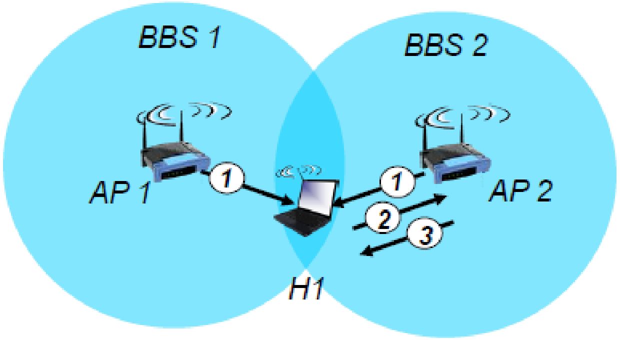
IEEE 802.11 Wireless LANs use CSMA/CA for multiple access. All have base-station and ad-hoc network versions.

802.11 LAN architecture:

- Wireless host communicates with base station (**access point**).
- **Basic Service Set (BSS)** in infrastructure mode contains:
  - Wireless hosts.
  - Access point (AP).
- **Host** must **associate** with an AP:
  - Scans channels, listening for **beacon frames** containing AP's name (SSID) and MAC address.
  - Selects AP to associate with.
  - May perform authentication.
  - Will typically run DHCP to get IP address in AP's subnet.

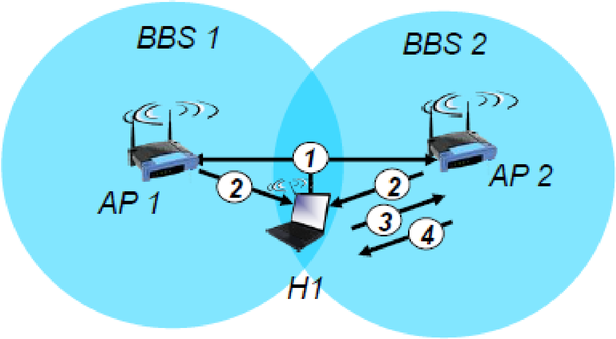
Passive scanning:

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



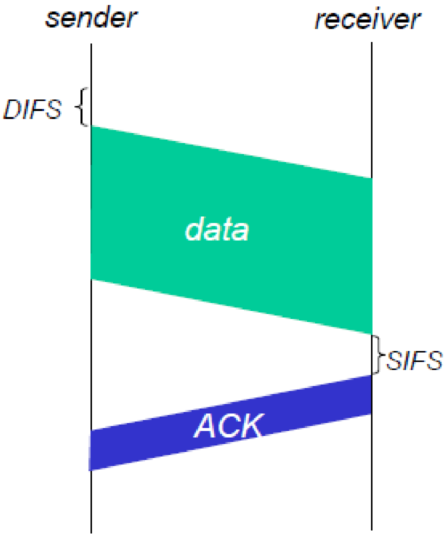
Active scanning:

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



CSMA/CA in IEEE 802.11:

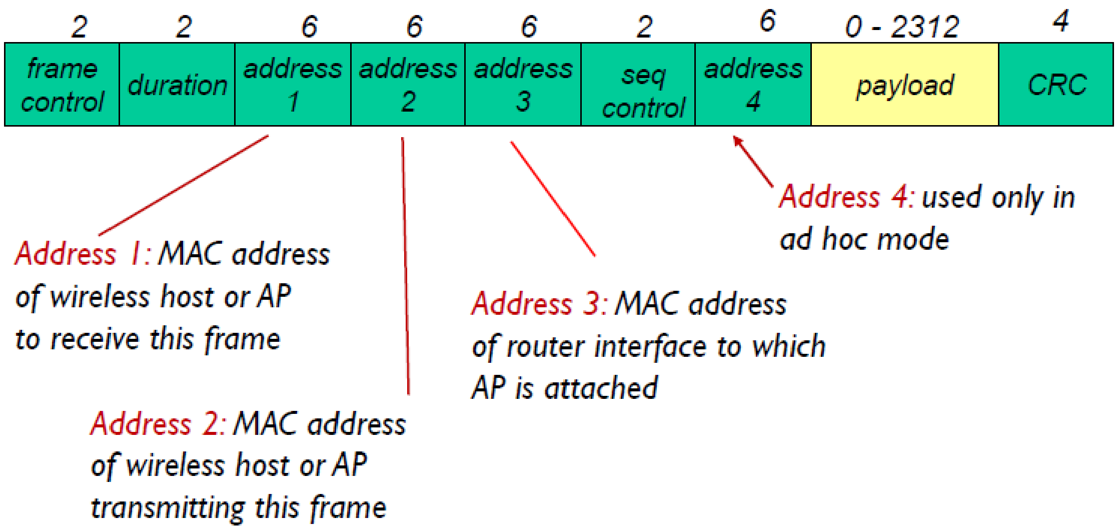
- Sender:
  - If sense channel idle for DIFS then transmit entire frame (no collision).
  - If sense channel busy, then:
    1. Start random backoff time.
    2. Timer counts down while channel idle.
    3. Transmit when timer expires.
    4. If no ACK, increase random backoff interval, repeat step 2.
- Receiver:
  - If frame received OK: return ACK after SIFS (ACK needed due to hidden terminal problem).



The idea for avoiding collisions is to allow sender to “reserve” the channel rather than making random accesses of data frames. This avoids collisions of long data frames:

- Sender first transmits **small** request-to-send (RTS) packets to BS using CSMA: RTSs may still collide with each other (but they are short).
- BS broadcasts clear-to-send (CTS) in response to RTS.
- CTS heard by all node:
  - Sender transmits data frame.
  - Other stations defer transmissions.

802.11 frame addressing:



2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

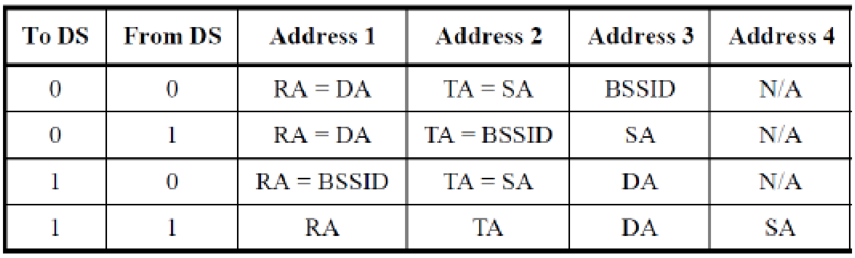
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

Addresses:



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

Types of frames:

- Control frames:
  - RTS/CTS/ACK.
  - CF-Poll/CF-End.
- Management frames:
  - **Beacons**: beacon frame announce the existence of a network, used in passive scanning.
  - **Probe Request/Response**: used in active scanning.
  - **Association Request/Response**.
  - **Dissociation/Reassociation**.
  - **Authentication/Deauthentication**.
- Data frames.

If a host remains in a same IP subnet, then the IP address can remain the same as the switch will see a frame from the host and "remember" which switch port can be used to reach the host.

5.-A DAY IN THE LIFE OF A WEB REQUEST

Scenario: student attaches laptop to campus network, request/receives www.google.com.

Connecting to the Internet:

1. Connecting laptop need to get its own IP address, address of first-hop router and address of DNS server: use **DHCP**.
2. DHCP request encapsulated in **UDP**, encapsulated in **IP**, encapsulated in **802.3 Ethernet**.
3. Ethernet frame **broadcast** on LAN, received at router running DHCP server.
4. Ethernet demuxed to IP demuxed, UDP demuxed to DHCP.
5. DHCP server formulates **DHCP ACK** containing client's IP address, IP address of first-hop router for client, name and IP address of DNS server.
6. Encapsulation at DHCP server, frame forwarded (switch learning) through LAN, demultiplexing at client.
7. DHCP client receives DHCP ACK reply.

ARP (before DNS, before HTTP):

1. Before sending **HTTP** request, need IP address of www.google.com: **DNS**.
2. DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Ethernet. To send frame to router, need MAC address of router interface: **ARP**.
3. **ARP query** broadcast, received by router, which replies with **ARP reply** giving MAC address of router interface.
4. Client now knows MAC address of first hop router, so can now send frame containing DNS query.

Using DNS:

1. IP datagram containing DNS query forwarded via LAN switch from client to 1º hop router.
2. IP datagram forwarded from campus network into comcast network, routed to DNS server.
3. Demuxed to DNS server.
4. DNS server replies to client with IP address of www.google.com.

TCP connection carrying HTTP:

1. To send HTTP request, client first opens **TCP socket** to web server.
2. TCP **SYN segment** inter-domain routed to web server.
3. Web server responds with **TCP SYNACK**.
4. TCP **connection established**.

HTTP request/reply:

1. **HTTP request** sent into TCP socket.
2. IP datagram containing HTTP request routed to www.google.com.
3. Web server responds with **HTTP reply**.
4. IP datagram containing HTTP reply routed back to client.