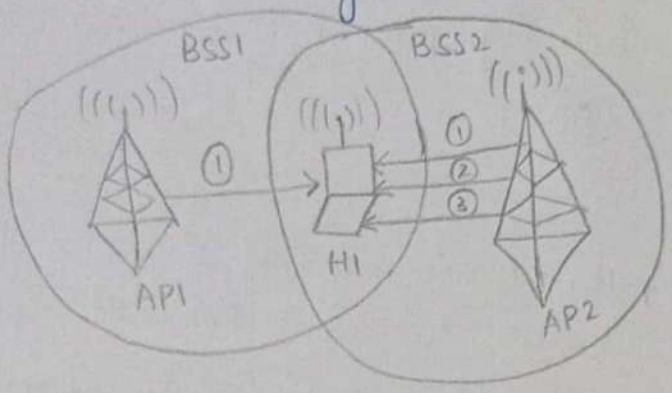
Passive Scanning

* A passive scan takes more time since the client must listen and wait for a beacon.
* If the client does not wait long enough on a channel, then the client may miss an AP beacon
* It is low cost and provides accurate and up-to-date information as soon as a system appears and starts communication
* Passive scanners identify operating systems, applications and ports throughout a network, monitoring activity to determine the networks' vulnerability

Active Scanning

* It takes less time since it actively probes to find an AP
* There is no missing situation of beacon. the client transmits a probe request and listens to a probe response
* It can have high cost and far-reaching effects on system uptime and reliability
* Active scanners send transmissions to the network nodes, examining the responses they recieve to evaluate whether a specific node represents weak point within network

Passive Scanning



* During a passive scanning, the client radio listens on each channel for beacons sent periodically by an AP

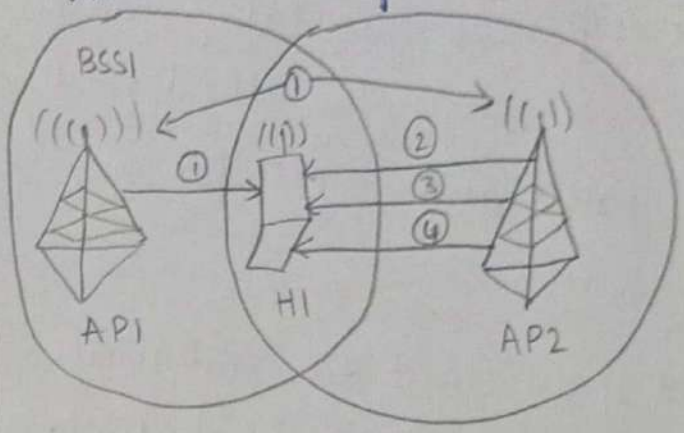
* The connections shown in the above figure can be explained as:-

1) Beacon frame sent from APs.

2) Association request frame sent: H1 to selected AP

3) Association response frame sent from selected AP to H1.

Active Scanning



* During an active scanning, the client radio transmits a probe request and listens for a probe response from an AP.

* The connections shown in above figure can be explained as:-

1) Probe request frame broadcast from H1

2) Probe response frame sent from APs.

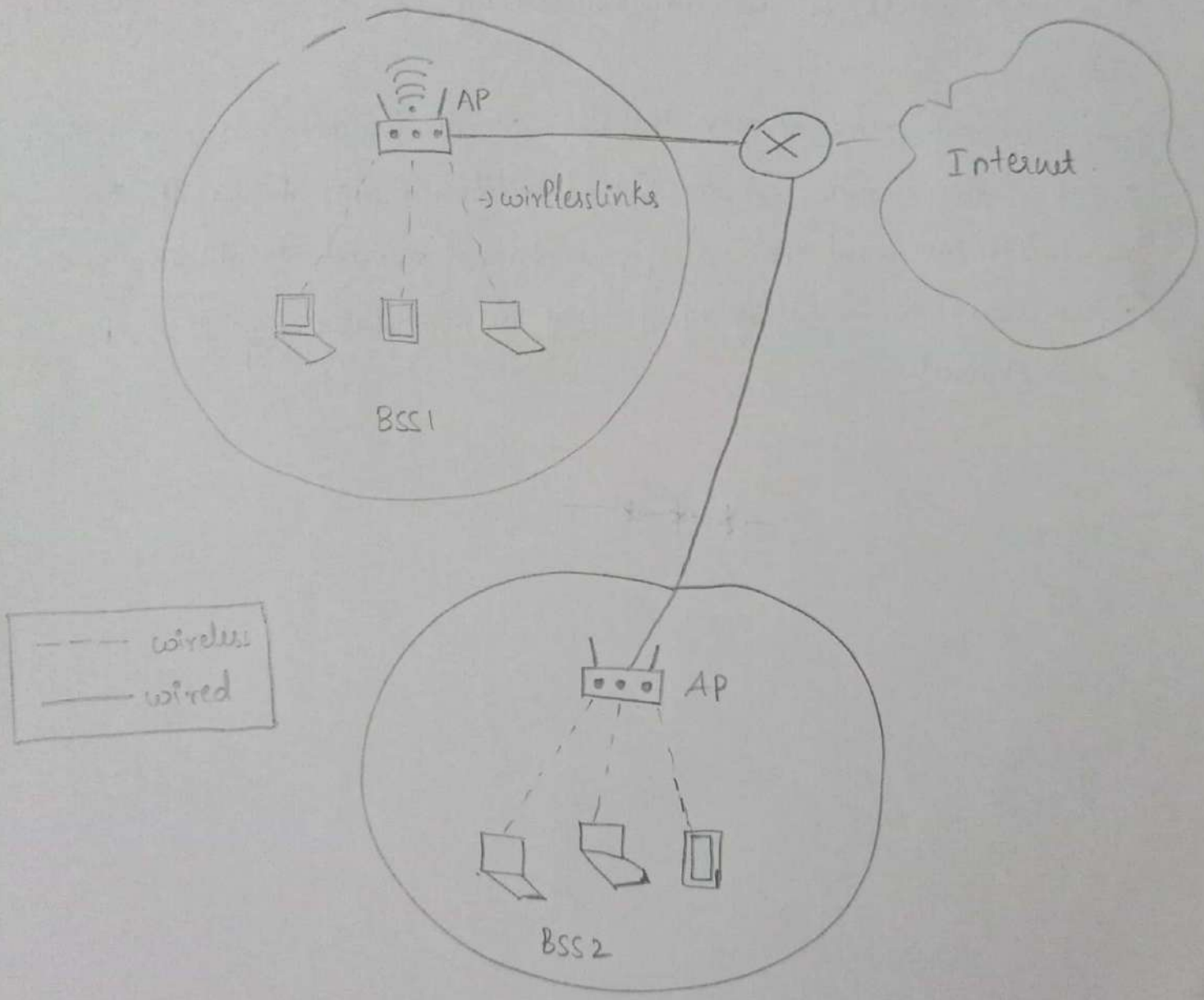
3) Association request frame sent :- H1 to selected AP.

4) Association response frame sent : selected AP to H1

Pg No:

Architecture of 802.11

The fundamental building block of the 802.11 architecture is the Basic Service set (BSS). A BSS contains one or more wireless stations and a central base station that is always connected to Internet, known as Access Point (AP) in 802.11 paralance.



The figure above shows the AP in each of 2 BSS's connecting to a microcontroller device/switch/router/which further connects to Internet

In a typical home network, there is one AP and one router that connects the BSS to the Internet.

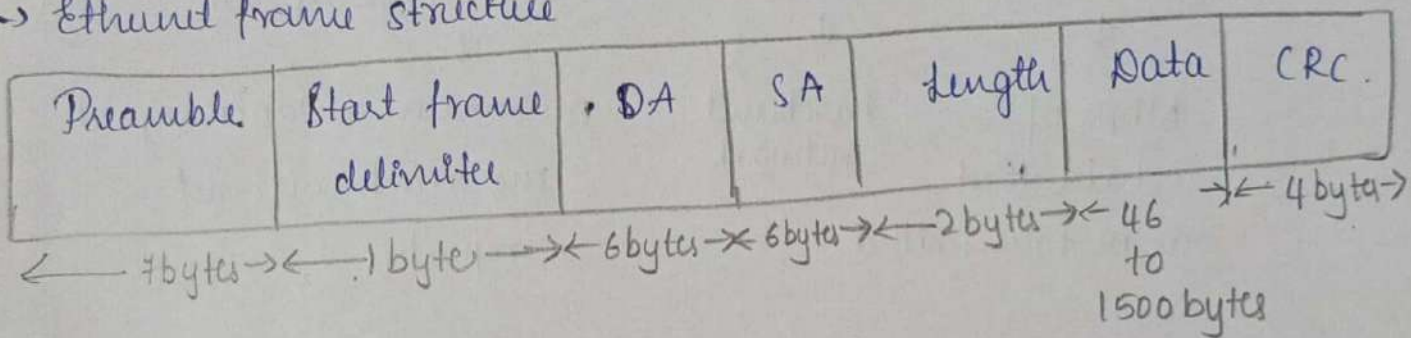
→ Each 802.11 wireless station has a 6 byte MAC address that is stored in the firmware of the station adapter.
Each AP also has a MAC address for it's wireless interface
These MAC addresses are adminstered by IEEE and are globally unique.

→ When network administrator installs an AP, the administrator assigns a one or two word Service Set Identifier (SSID) to the AP. the administrator must also assign a channel number for AP. Any two channels are non-overlapping if they are separated by four or more channels.

Ethernet.

→ Ethernet is widely used in Wired LAN's
→ Link-layer-protocol
→ Used CSCMA/CD protocol
→ It achieves:
(i) Higher data rate, data speed
(ii) Inexpensive. (iii) Helps in switched LAN's

→ Ethernet frame structure



(i) Preamble: It is 10101010 ie 1's and 0's alternatively in 7 bytes. Used for synchronization purposes. It helps in time & speed synchronization between two network adapters. It is "wakeup" to adapters.

(ii) Start frame delimiter: The value is 1. It is in one byte. So that after preamble ends at 1. There are two consecutive ones that activates the adapter that message is there/important stuff to come. SFD and preamble is added by physical layer.

(iii) DA - distination address. It is distinations 48-bit MAC (media access control) address. Hence 6-bytes long. Similarly SA - source MAC address and is 6 bytes / 48 bits long.

(iv) length → 2 bytes. length of IP datagram encapsulated

(v) Data → Payload / actual data. Minimum 46 is required for collision detection to happen. So if it's lesser than that it stuffs / pads zeroes. If it's greater than fragments it's and transfers.

(vi) CRC → It helps in error detection and correction

Ethernet uses baseband transmission which increases its speed as adapter directly sends digital signals into the broadcast channel. It also uses Manchester encoding.

Technology:

format: Number — base — distance / type of cable

- Number → Mbps of data that can be transmitted
- base → baseband network
- distance / type of cable → maximum distance signal can reach without repeaters.

Ex: 10-BASE-T

- 10 → 10 Mbps
- BASE → BASE
- T → Twisted Cu Cable

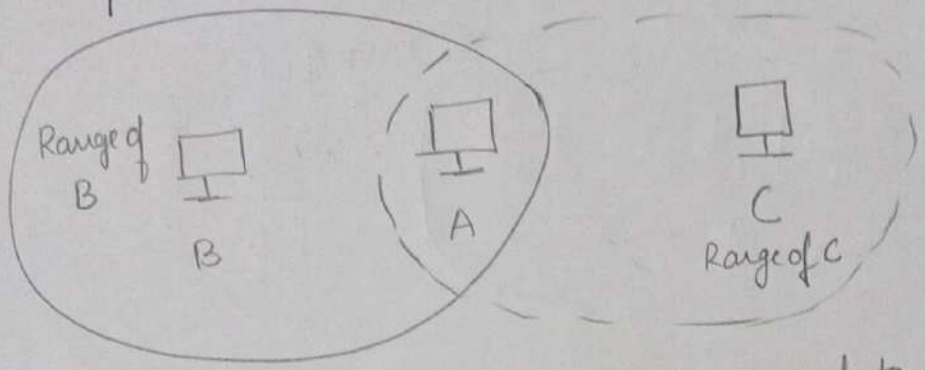
100-BASE-FX

- 100 → 100 Mbps
- FX → fibre cable

LX – Long wavelength
SX – short wavelength.

Pg No.

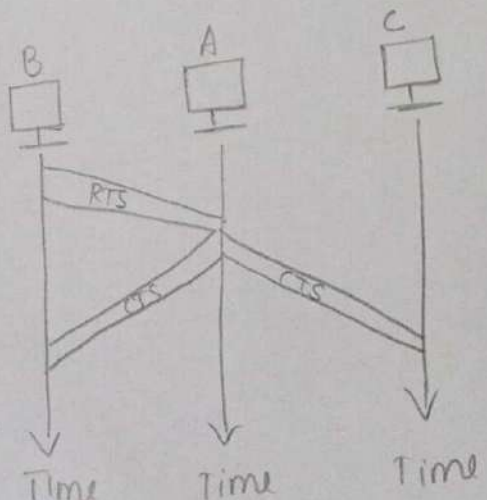
Hidden Station

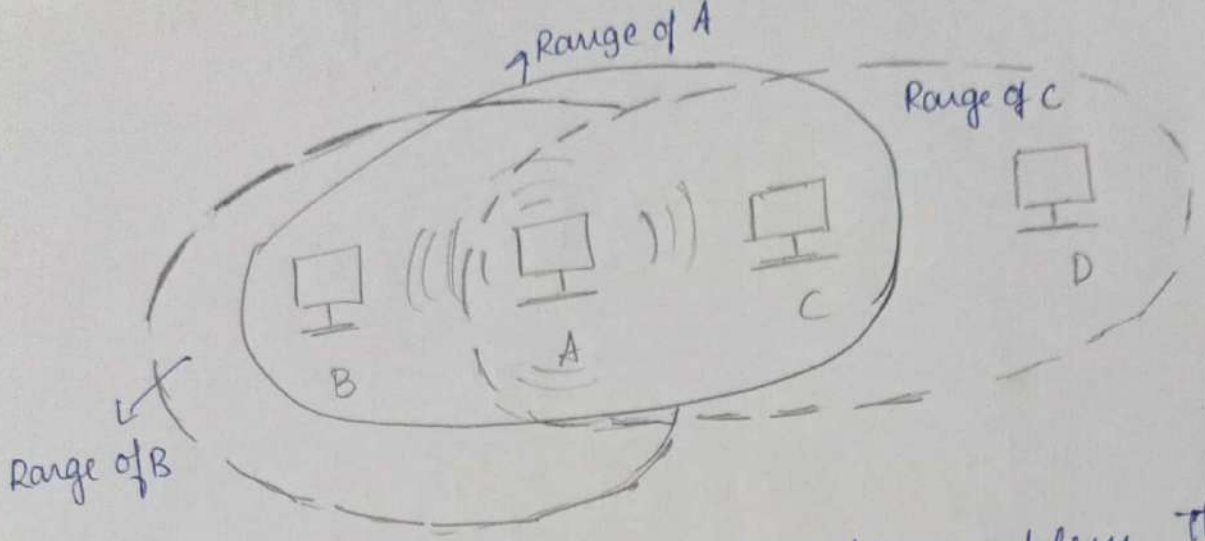


B and C are hidden with respect to A

All nodes in a range can sense transmissions of other nodes. C is not in B's range and B is not in C's range. Range of B is represented in oval. Range of C is represented in dashed oval. Assume if B is sending data and to station A. In the middle of this transmission if station C also has data to send to station A. But station C is out of range of B and transmissions from B can't reach C. ∴ C thinks medium is free and sends its data to A, which results in collision at A. Hidden stations can reduce the capacity of network because of the possibility of collision. Here neither B's nor C's data reach A.

→ the solution to hidden station / terminal problem is the use of handshake frames RTS (Ready TO Send) and CTS (Clear TO Send). The RTS message from B reaches A, but not C. Because, both B and C are within range of A, the CTS message, which contains the duration of data transmission from B to A reaches C and it knows some hidden station is using the channel and refrains from transmission until duration is over





This problem is inverse of exposed station problem. The station refrains from using the channel when it's actually available. Station A is transmitting to station B. Station C has some data to send to station D, however which can be sent without interfering with transmission from A to B. As A's transmission is broadcast in nature (Wifi) C is exposed to A's transmision C hears what A is sending and thus refrains from sending.

C is too conservative or conscious and wastes the capacity of channel.

Exposed Station Problem.