WIRELESS NETWORKS

UNIT-3

Wireless LAN
&
Mobile Network Layer

Syllabus

UNIT - III

- **Wireless LAN:** Infrared Vs. Radio Transmission, Infrastructure and Ad-hoc Networks,
- **IEEE 802.11:** System Architecture, Protocol Architecture, Physical Layer, MAC Layer, and MAC Management.
- **Mobile Network Layer: Mobile IP**: Entities and Terminology, IP packet delivery, Agent discovery, Registration, and Tunneling and Encapsulation,
- **Dynamic Host Configuration Protocol**
- **Ad Hoc Networks.**

Wireless LAN: Introduction

- WLAN constitutes a fast-growing market introducing the **flexibility of wireless access into office, home, or production environments.**
- WLANs are typically **restricted in their diameter** to buildings, a campus, single rooms etc. and are operated by individuals, not by large-scale network providers.
- The global goal of WLANs is **to replace office cabling, to enable tether less access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings.**

Wireless LAN: Introduction

- Some **advantages of WLANs are:**

(1)Flexibility: With in **radio coverage nodes can communicate without further restriction.**

(2)Planning: Wireless ad hoc network **allow communication without planning** whereas wired network needs wiring plans.

(3)Design: Wireless Network can survive disaster. If the wireless devices survive people can communicate.

(4)Cost: After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a **wireless network will not increase the cost.** With fixed network addition of an user will lead into unplugging and plugging. Wireless connections do not wear out.

Wireless LAN: Introduction

WLANs also have several **disadvantages:**

- **Quality of service:** offers Low quality than wires because of Lower bandwidth, High error rate and Higher delay variation due to extensive **error correction and detection mechanisms.**
- **Proprietary solutions:** Many companies have come up with proprietary solutions offering standardized functionality. This is due to **slow standardization procedures.**
- **Restrictions:** The wireless products need to comply with national regulations.
- **Safety and security: Using radio waves** for data transmission **might interfere** with other high-tech equipment in, e.g., hospitals. Senders and receivers are operated by laymen and, radiation has to be low. Precautions have to be taken to prevent safety hazards.

Wireless LAN: Introduction

- Many different, and sometimes competing, design goals have to be taken into account for WLANs to ensure their commercial success:

➢ **Global operation**

➢ **Low power**

➢ **License-free operation(2.4 GHz ISM band)**

➢ **Robust transmission technology**

➢ **Simplified spontaneous cooperation in Adhoc Meets**

➢ **Easy to use**

➢ **Protection of investment**

➢ **Safety and security**

➢ **Transparency for applications**

Infrared vs Radio Transmission

- Today, two different basic transmission technologies can be used to set up WLANs.
- One technology is based on the **transmission of infra red light (e.g., at 900 nm wavelength),** the other one, which is much more popular, uses **radio transmission in the GHz range (e.g., 2.4 GHz in the license-free ISM band).**
- Both technologies can be used to set up ad-hoc connections for work groups, to connect, e.g., a **desktop with a printer without a wire, or to support mobility within a small area.**

Infrared vs Radio Transmission

Infrared:

1. This technology uses diffuse light reflected at walls, etc (or) directed light if line of sight exists between sender and receiver.
2. Sender can be **LED or LASER diodes** and Receivers can be **Photo diodes.**

Advantages:

- Simple and cheap because of LED/ Diodes(crystal rectifier).
- No license needed-uses only infra-red.
- Shielding is very simple.
- No interferences form/ with electrical devices.

Disadvantages:

- Low bandwidth. The infra-red can be easily shielded.
- Infra-red cannot penetrate walls.LOS is needed.
- Infrared is used when Good transmission quality and High data rates.

Infrared vs Radio Transmission

- **Radio waves for data transmission,** e.g., GSM at 900, 1,800, and 1,900 MHz, DECT at 1,880 MHz etc.

Advantages:

- Long term for WAN.
- Coverage is larger.
- Can penetrate walls, furniture's etc.
- Additional coverage is by reflection.
- Does not need LOS.
- Higher transmission rates above 100 Mb/s.

Disadvantages:

- Shielding is not simple. Interference is possible.
- Radio transmission is permitted in certain frequency bands only.
- Limited range of license free hands are available world wide and are not available same in all countries.

Infrared vs Radio Transmission

- One (**IEEE 802.11**) standardized infra red transmission in addition to radio transmission.
- The other two (**HIPERLAN and Bluetooth**) rely on radio.
- WLANs should, e.g., **cover a whole floor of a building and not just the one room where LOSs exist.**
- Future **mobile devices may have to communicate while still in a pocket or a suitcase so cannot rely on infra red.**
- The big advantage of radio transmission in everyday use is indeed the **ability to penetrate certain materials and that a LOS is not required.**

Infrastructure and ad-hoc networks

Infrastructure Networks:

- Many WLANs of today need an **infrastructure network.**
- **Infrastructure networks** not only provide access to other networks, but also include forwarding functions, medium access control etc.
- In these infrastructure-based wireless networks, **communication typically takes place only between the wireless nodes and the access point (see Figure 7.1), but not directly between the wireless nodes.**

Infrastructure and ad-hoc networks

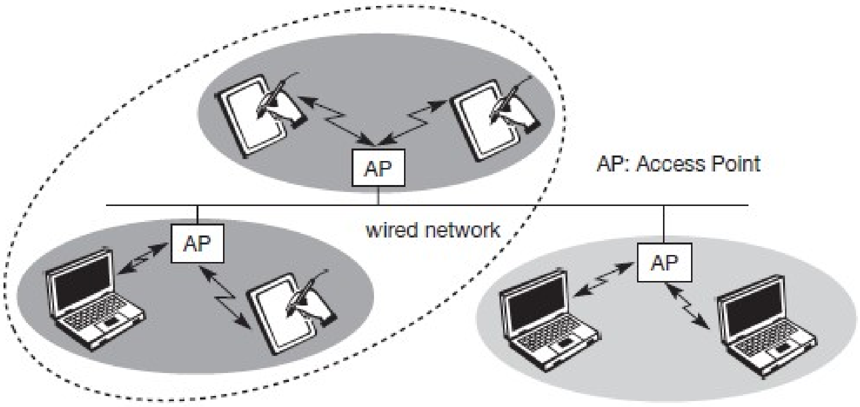
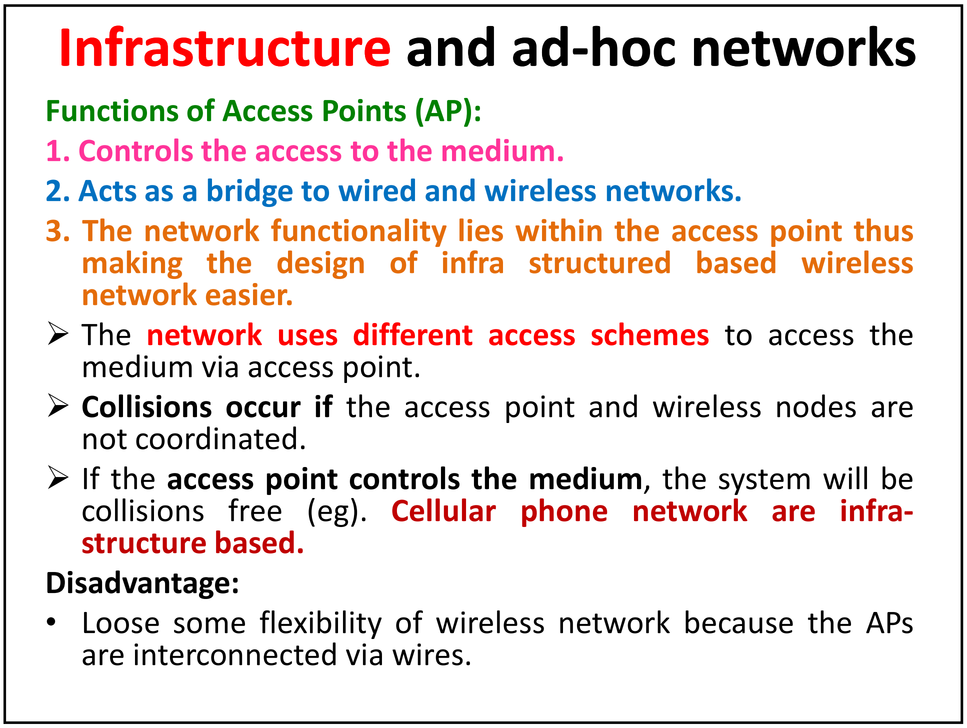


Figure 7.1 Example of three infrastructure-based wireless networks



Infrastructure and ad-hoc networks

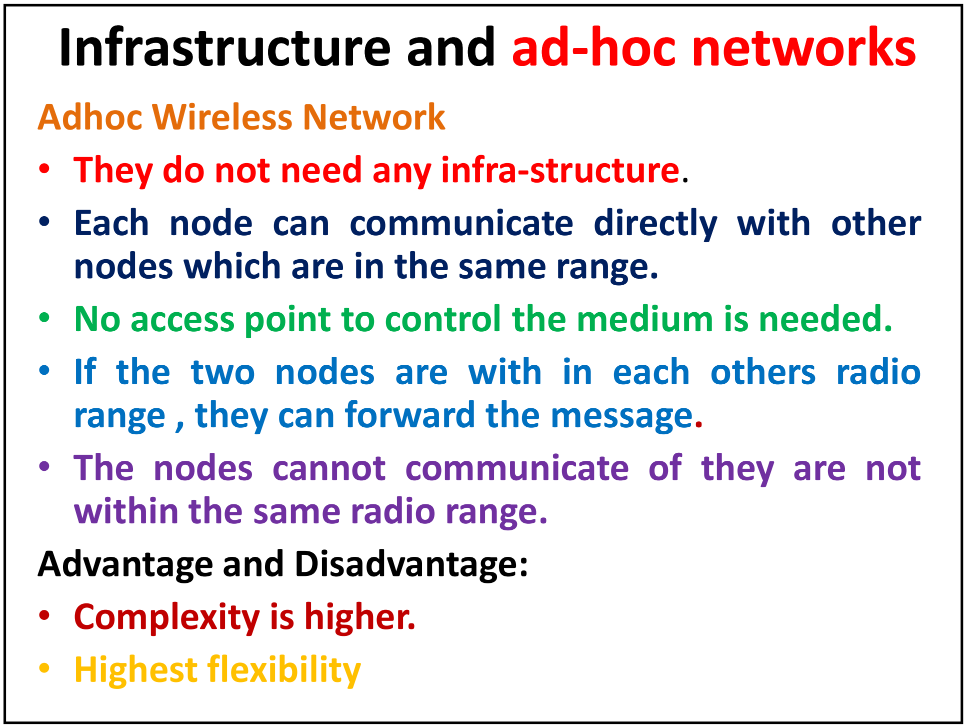
Functions of Access Points (AP):

1. **Controls the access to the medium.**
2. **Acts as a bridge to wired and wireless networks.**
3. **The network functionality lies within the access point thus making the design of infra structured based wireless network easier.**

- ➢ The **network uses different access schemes** to access the medium via access point.
- ➢ **Collisions occur if** the access point and wireless nodes are not coordinated.
- ➢ If the **access point controls the medium**, the system will be collisions free (eg). **Cellular phone network are infra-structure based.**

Disadvantage:

- Loose some flexibility of wireless network because the APs are interconnected via wires.



Infrastructure and ad-hoc networks

Adhoc Wireless Network

- **They do not need any infra-structure**.
- **Each node can communicate directly with other nodes which are in the same range.**
- **No access point to control the medium is needed.**
- **If the two nodes are with in each others radio range , they can forward the message.**
- **The nodes cannot communicate of they are not within the same radio range.**

Advantage and Disadvantage:

- **Complexity is higher.**
- **Highest flexibility**

Infrastructure and ad-hoc networks

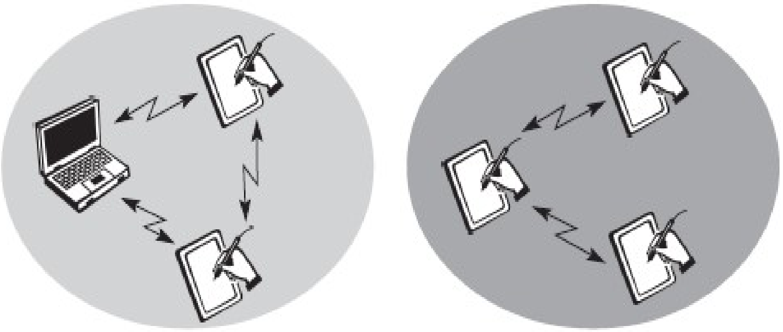


Figure 7.2 Example of two ad-hoc wireless networks

WLAN Technologies

- Wireless LAN Standards that are currently being explored in the field of communications technology are:

  1. IEEE 802.11.

     a.802.11a b.802.11b c.802.11g

  2. BRAN

     a.HiperLAN1/2 b. Hiper access c. Hiper man

  3. Bluetooth

- **Wireless LAN Standards**: There are several wireless LAN solutions available today, With varying levels of standardization and industry are, **HomeRF and Wi-Fi (IEEE 802.11b).**
- Of these two, 802.11 technologies enjoy wider industry support and are **targeted to solve Enterprise, home and even public hot spot.**

IEEE 802.11 WLAN

- The IEEE finalized the initial standard for wireless LANs, IEEE 802.11 in June 1997.
- This initial standard specifies a **2.4 GHz** operating frequency with data rates of **1 and 2 Mbps.**
- With this standard, one could choose to use either **frequency hopping or direct sequence**(two non compatible forms of spread spectrum modulation).
- **The primary goal of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services.**
- In late 1999, the IEEE published two supplements to the initial **802.11a and 802.11b (Wi-fi*).**
- Additional features of the WLAN should include the **support of power management to save battery power, the handling of hidden nodes, and the ability to operate worldwide.**

IEEE 802.11 System Architecture

System Architecture

- Wireless networks can be of either of 2 basic architectures.

(1) Infra structure based

(2) Ad hoc based.

IEEE 802.11- Infrastructure based Architecture

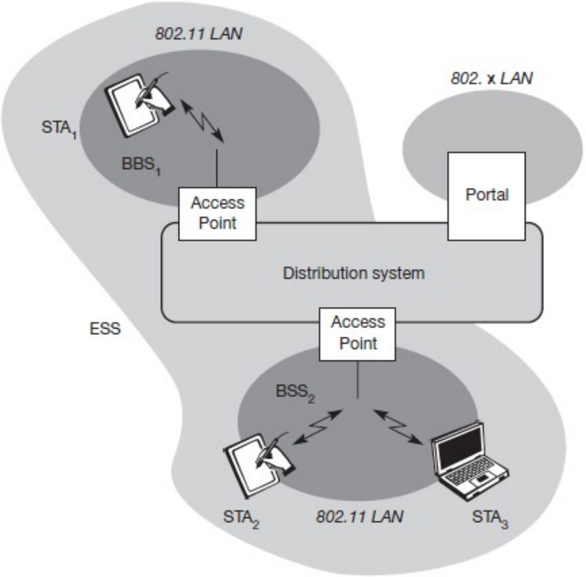


Figure 7.3 Architecture of an Infrastructure-based IEEE 802.11

IEEE 802.11- Infrastructure based Architecture

- **Portal is a bridge to other wired network.**
- Wireless nodes are called as **station represented** as **STA.**
- These station are connected to the **Access Point (AP).**
- The stations and the AP which are within the **same radio coverage** is form **Basic Service Set (BSS$_i$).**
- The **BSS are interconnected via a distribution system**.
- **The distribution system connects several BSS via AP to form a single network. This network is called Extended Service Set(ESS).**
- This **ESS** has its own identifier **ESSID**. The **ESSID is the name of the network and is used to separate different network.**

IEEE 802.11- Infrastructure based Architecture

Distribution System:

- **The distribution system connects the wireless network via the AP with a portal by which other LANs can also be connected.**
- **The distribution system consists of bridged IEEE LAN, Wireless Lines or any other network.**
- **Handles data transfer between AP‟s.**

Function of Access Point:

1. **Support roaming**
2. **Period synchronization with in BSS**
3. **Support power management.**
4. **Control medium access.**

IEEE 802.11- Adhoc based Architecture

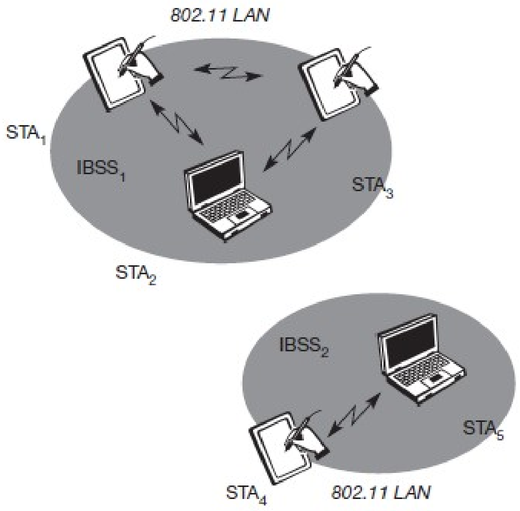


Figure 7.4 Architecture of IEEE 802.11 ad-hoc wireless LANs

IEEE 802.11- Adhoc based Architecture

- In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more **Independent BSSs (IBSS)** as shown in Figure 7.4.
- In this case, **an IBSS comprises a group of stations using the same radio frequency.**
- **Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2. This means for example that STA3 can communicate directly with STA2 but not with STA5.**
- **Several IBSSs can either be formed via the distance between the IBSSs (see Figure 7.4) or by using different carrier frequencies.**

IEEE 802.11- Protocol Architecture

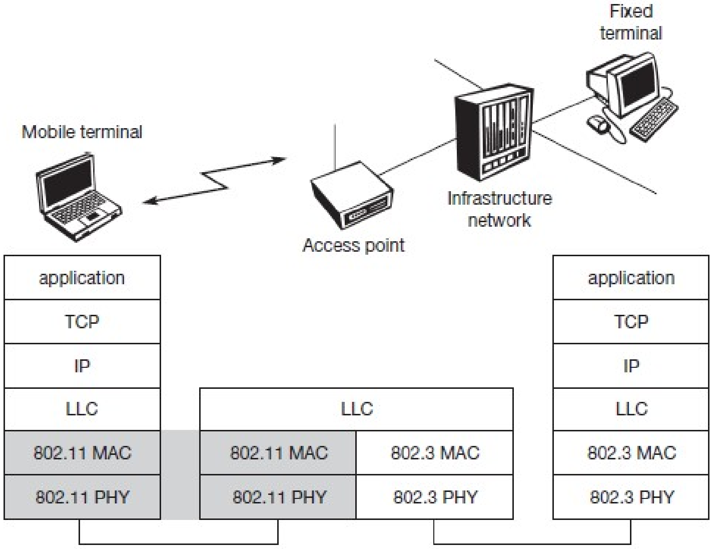


Figure 7.5 IEEE 802.11 protocol architecture and bridging

IEEE 802.11- Protocol Architecture

- IEEE 802.11 covers the physical layer **and** medium access layer.
- The physical layer **is subdivided** into **(PLCP) Physical Layer Convergence Protocol** and **Physical Medium Dependant (PMD)** sub layer.
- The **PLCP sub layer** provides a **carrier sense signal**, **called Clear Channel Assessment (CCA),** and **provides a common PHY Service Access Point (SAP)** independent of the transmission technology.
- Finally, the **PMD sublayer** **handles modulation and encoding/decoding of signals.**
- The basic **tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption.**

IEEE 802.11- Detailed Protocol Architecture

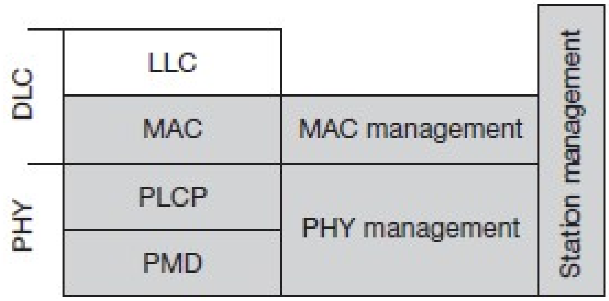


Figure 7.6 Detailed IEEE 802.11 protocol architecture and management

IEEE 802.11- Detailed Protocol Architecture

Functions of PMD:

- Handles modulation and encoding/decoding of signals.

Function MAC Management:

1. Supports association and re-association of station to access point.
2. Supports roaming.
3. Controls authentication, encryption, and synchronization of station with access point.
4. Power Management.
5. Maintain management information basic **MIB (Management Information Base).**

Function of PHY management:

1. Channel Tuning
2. Maintain PHY MIB

Functions of Station Management:

- Interacts with both management layers and is responsible for higher layer functions.

IEEE 802.11- Physical Layer

- IEEE 802.11 supports three different physical layers.

❖**One layer based on infrared.**

❖**Two layers based on radio transmission.**

- All the variants have the **CCA signal** clear channel assessment signal.
- CCA is needed for the MAC to check whether the medium is busy or idle.
- Indicates whether the medium is busy or idle.
- Offers a **SAP (Service access point) with 2 MBPS transfer rate.**

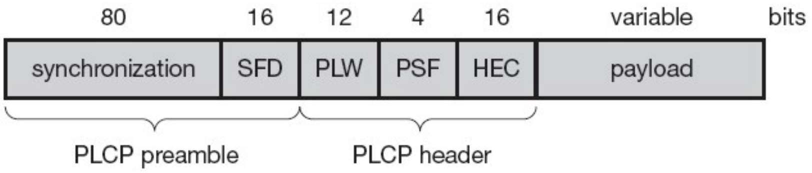
IEEE 802.11- Physical Layer

- **Three Version of PHY layer:**

1. Frequency hopping spread spectrum.
2. Direct sequence spread spectrum.
3. Infra-red.

IEEE 802.11- Physical Layer

Frequency Hopping Spread Spectrum

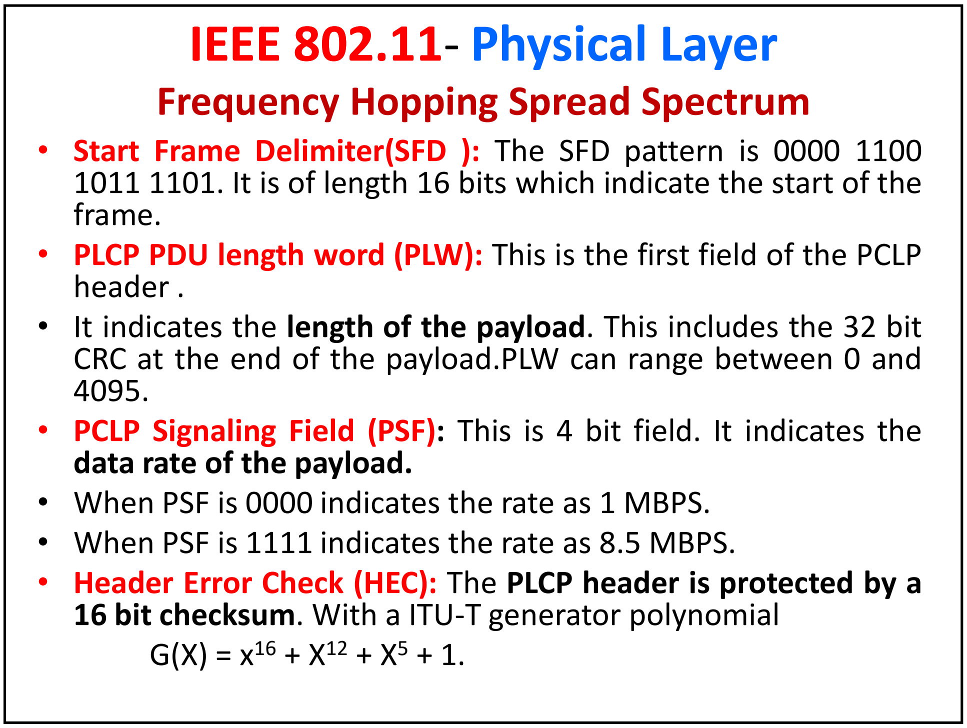


- Allows the co-existence of multiple networks in the same area by using different hopping sequence for different network.
- The Frame consists of 2 parts.

1. PLCP part (Physical Layer Convergence Protocol)
2. Payload part.

PLCP: Consists of Preamble and header.

- PLCP is transmitted @ MBPS.
- Data is **scrambled using the polynomial S(Z)=Z^7 +Z^4+1 for DC blocking and widening of spectrum.**
- **Synchronization:** 80 synchronization bits which is of the pattern 010101. This pattern is used for synchronization of receivers and signal detection.

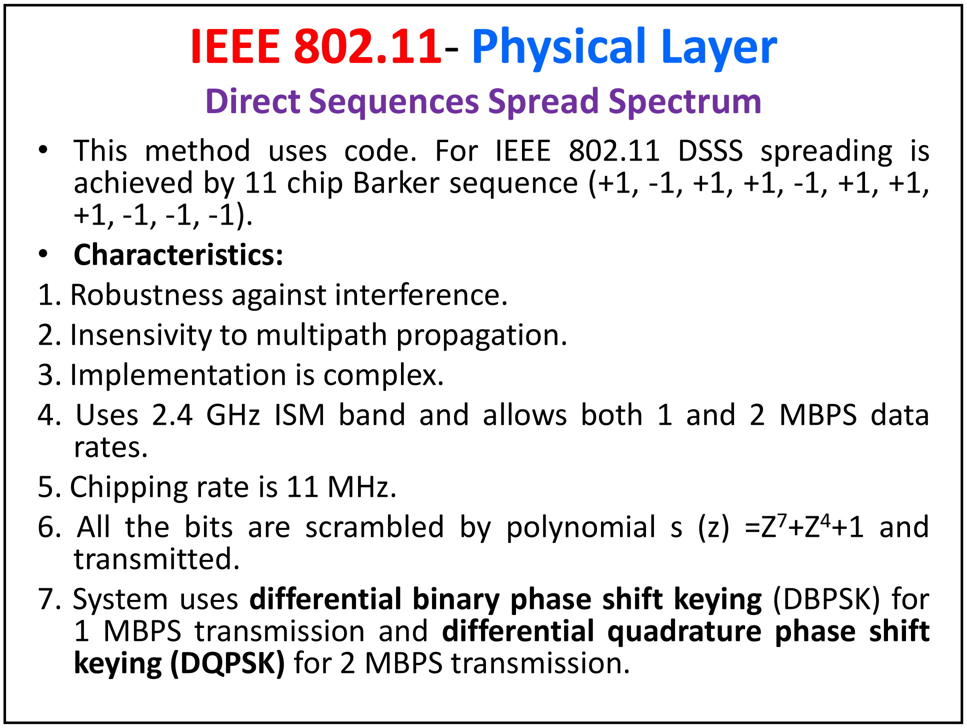


IEEE 802.11- Physical Layer

Frequency Hopping Spread Spectrum

- **Start Frame Delimiter(SFD):** The SFD pattern is 0000 1100 1011 1101. It is of length 16 bits which indicate the start of the frame.
- **PLCP PDU length word (PLW):** This is the first field of the PCLP header .
- It indicates the **length of the payload**. This includes the 32 bit CRC at the end of the payload.PLW can range between 0 and 4095.
- **PCLP Signaling Field (PSF):** This is 4 bit field. It indicates the **data rate of the payload.**
- When PSF is 0000 indicates the rate as 1 MBPS.
- When PSF is 1111 indicates the rate as 8.5 MBPS.
- **Header Error Check (HEC):** The **PLCP header is protected by a 16 bit checksum**. With a ITU-T generator polynomial

  $G(X) = x^{16} + X^{12} + X^5 + 1.$



IEEE 802.11- Physical Layer

Direct Sequences Spread Spectrum

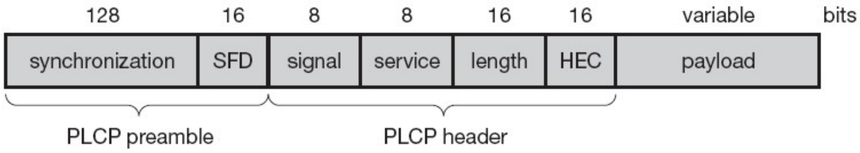
- This method uses code. For IEEE 802.11 DSSS spreading is achieved by 11 chip Barker sequence (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1).
- **Characteristics:**

1. Robustness against interference.
2. Insensivity to multipath propagation.
3. Implementation is complex.
4. Uses 2.4 GHz ISM band and allows both 1 and 2 MBPS data rates.
5. Chipping rate is 11 MHz.
6. All the bits are scrambled by polynomial s (z) $=Z^7+Z^4+1$ and transmitted.
7. System uses **differential binary phase shift keying** (DBPSK) for 1 MBPS transmission and **differential quadrature phase shift keying (DQPSK)** for 2 MBPS transmission.

IEEE 802.11- Physical Layer

Direct Sequences Spread Spectrum

Frame of Physical layer using DSSS



128	16	8	8	16	16	variable	bits
synchronization	SFD	signal	service	length	HEC	payload	

The frame has 2 parts

1. PLCP Part-transmitted at 1 MBPS
2. Payload part-Transmitted at 1 or 2 MBPS.

IEEE 802.11- Physical Layer

Direct Sequences Spread Spectrum

- **Synchronization (128 bits):** This field is used for Synchronization, Gain setting, Energy detection, Frequency offset compensation.
- **SFD (Start Frame Delimiter) 16 bits:** Used for synchronization at the beginning of the frame. The pattern used is 1111 0011 1010 0000 (8 bits).
- **Signal:** This field indicates the data rate of transmission of payload. Value of the field is OXOA- 1 MBPS (DBPSK) Value of the field is OX14-2 MBPS (DQPSK). Other Value reserved for future use.
- **Service (8 bits):** Reserved for future use. when the service field has 0x00 indicates a compliant frame.
- **Length (16 bits):** Length of the payload in microseconds.
- **Header Error Check(HEC) 16 bits:** This filed is used for protection of Signal, Service, Length.
- They are protected by checksum using ITU-T CRC 16 standard Polynomial $\lambda^{16}+ \lambda^{12} + \lambda^{5}+1$.

IEEE 802.11- Physical Layer

Infra-Red

- The physical layer is based on Infra red transmission.

Characteristics:

- **Doesn’t require line of sight** between sender and receiver.
- **Allows point to multipoint communication.**
- **Maximum range of transmission is 10m provided no interference with transmission.**
- **Best suited for network with in a building.**
- **Reuse of frequency is simple.**

IEEE 802.11- Medium Access Control Layer

MAC Layer Functions

- Control the medium access
- Support roaming
- Authentication
- Power conversation.

Traffic Service Provided by MAC

- Asynchronous Data Service-Mandatory
- Time bounded service(Optional).Used for transfer of data.

➢ **Asynchronous Data Service**

- Exchange of packets based on best efforts.
- It supports broadcast and multicast transmission.

➢ **Time Bounded Service:**

- This service is implemented using point co-ordination function (PCF).
- **802.11 offers asynchronous data service in ad hoc mode.**
- **802.11 offers asynchronous data and time bounded services in infrastructure mode.**

IEEE 802.11- Medium Access Control Layer

- To access the medium three methods are available.

➢ **DFWMAC-DCF CSMA/CA(mandatory)**

➢ **DFWMAC-DCF W/RTS/CTS (optional)**

➢ **DFW MAC-PCF (optional)**

DFW: Distributed Foundation Wireless
MAC: Medium Access Control
DCF: Distributed Co-ordination Function
PCF: Point Co-ordination Function

- The I method mandatory is **based on CSMA/CA**.
- The II method is **based on RTS/CTS** used to avoid hidden terminal problem.
- The III method is **based on polling** for time bounded service.
- DCF offers only asynchronous service.
- PCF offers both Asynchronous and time bounded service.

IEEE 802.11- Medium Access Control Layer

- The MAC mechanisms are called as **DFW MAC**. **When a node wants to transmit a packet it has to wait one DIFS amount of time before sensing the medium.**
- If the Medium is idle immediately the node transmits a packet. Else it has to wait.
- The waiting time depends upon **SIFS,PIFS,DIFS** based upon the data/control.
- The waiting time depends upon **PHY and slot time**.
- The slot time is dependent upon

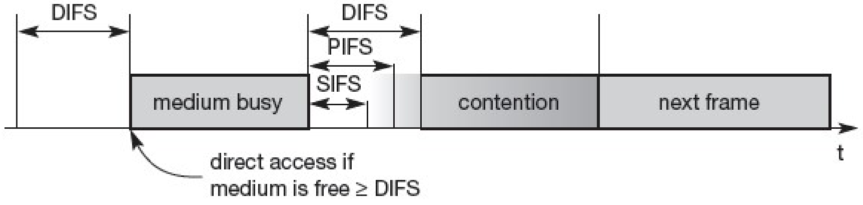
➢ Propagation Delay

➢ Transmitter Delay

➢ Other PHY dependent parameters

- **Slot time is 50 µs FHSS and 20 µs DSSS.**

IEEE 802.11- Medium Access Control Layer



- **SIFS: Short Inter Frame Spacing.** This waiting time has **highest priority**, shortest waiting time. **Its is used to transmit ACK,CTS and polling response.**
- **PIFS: PCF IFS- Point Co-ordination Function Inter Frame Space**. This waiting time has **medium priority**. PIFS waiting time is between SIFS and DIFS. **It is used for time bounded service.**
- **DIFS: DCF IFS- Distributed Co-ordination Function Inter Frame Space.**
- This has the **lowest priority** longest waiting time. **It is used for asynchronous data service.**

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF using CSMA/CA

- This method is used **to check whether the medium is idle or busy.** This is the **mandatory access method**. This method is **based on CSMA/CA.**

Concept:

- When the device is ready to send it starts sensing the medium. Carrier sense based on **Clear Channel Assessment(CCA).**
- **If the medium is free for the duration of Inter Frame space(IFS), the station can start sending. The IFS depends upon the service type.**
- **If the medium is busy the station has to wait for a free IFS. When more than one node compete after IFS they entering the contention phase.**
- During the contention phase, **each node chooses a random back off time within the contention window.**

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF using CSMA/CA

- The Nodes delays the medium sense for chosen random amount of time.
- After the **random amount of time the node senses** the medium, two scenario's exist.

(a) Medium is idle, the node can access the medium.

(b) The medium is busy, the cycle is lost and the node has to wait once again for on DIFS the idle medium.

- **The additional waiting time is measured in multiple of the slots.**
- The advantage of **randomness is that it avoids collision.**
- The disadvantage is that this method is not fair because **irrespective of the waiting time all the nodes have chance of transmitting data in the next cycle.**
- To have fairness **802.11 adds back off timer**.

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF using CSMA/CA

Concept of Back off timer:

- **All the nodes need to wait for IFS (Free).** Then each nodes selects a random waiting time within the contention window.
- **If the station does not get the access to the medium, it stops the back off timer.** Waits for the channel to be free for I DIFS and starts the counter again.
- **As soon as the counter expires the nodes access the medium.**
- The states that the deferred **station do not choose the back off timer again but counts down.**

Advantage:

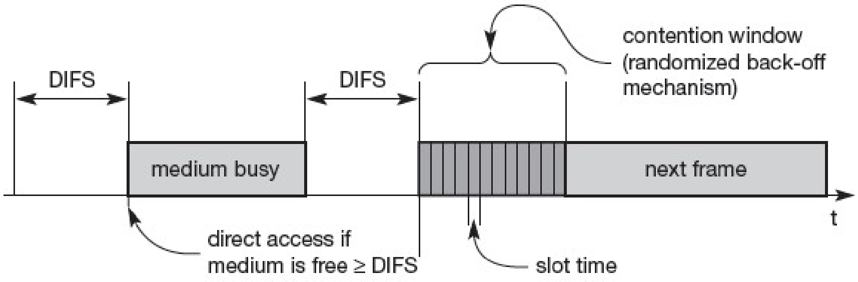
- Station waiting for a longer time has an edge over the nodes that have just entered, because
- it has to wait only for the **remainder of the back off timer from the previous cycles.**

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF using CSMA/CA

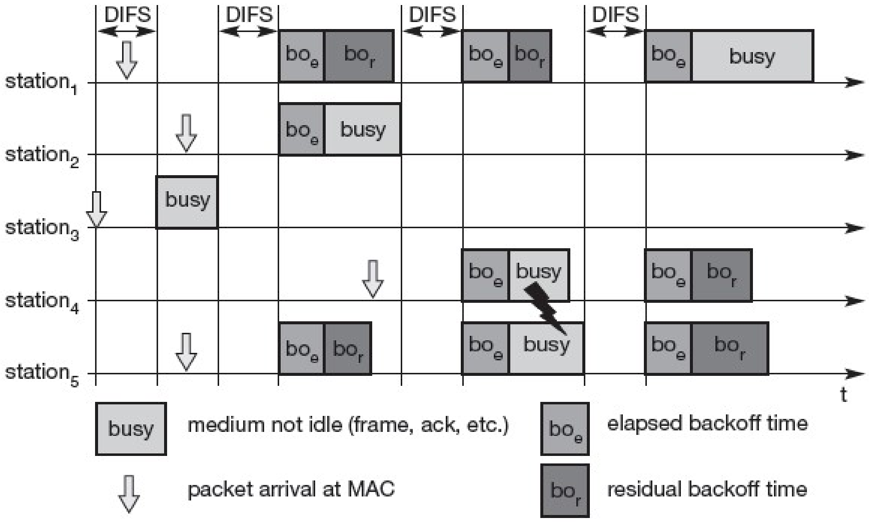
- **Broadcast Data Transmission**

To illustrate the concept consider 5 stations STA1 to STA5 are trying to send a packet at some point of timer.



IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF using CSMA/CA



IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF using CSMA/CA

- From the figure station 3 has the first request to send a packet. The station 3 senses the medium, finds the waits for medium is idle 1 DIFS and finds that the medium is idle throughout and sends the packet.
- Station1, Station2, Station5 need to wait for 1 DIFS after station 3 window and starts coming down their timer. The stations need to choose back off times because more stations compete.

  Back off time=BOe + BOr
- The back off timer for station 2 is very low. Hence it accesses the medium.
- The station 1 , and station 5 stops the clock and store **their residual back off timer.** Now station 4 wants to send a packet. It waits for 1 DIFS. Three stations try to get access the medium. Accidentally two stations can have the same back off time. Station 4 and Station 5-
- This results in collision and need to wait. Hence station 1 gets access to the medium. Due to the collision station 4 and 5 need to select a new back off timer.
- **The problem in this method is the selection of contention window size. If the window size is large causes unnecessary delay over the other hand when it is small results in unnecessary collisions.**
- The system tries to select the value based upon the number of stations trying to send. The size of the contention window follows exponential back off.

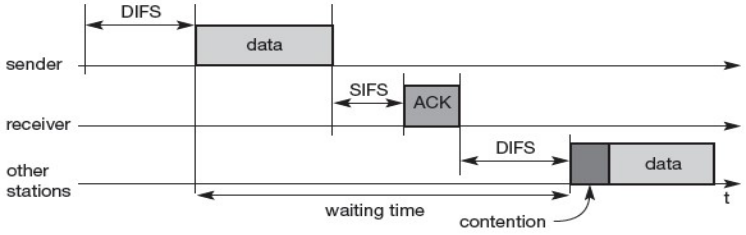
  (e.g.) Starts with CW=7.
- When collision occurs, CW size doubles CW=49 and goes on until maximum of CW, 255.
- The above scenario is for heavy load. Under light load, it starts decreasing until CW=7.

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF using CSMA/CA

For Unicast Data Transmission

- In the following unicast transmission the sender transmits data and receiver transmits acknowledgement.
- After receiving the data, the receiver waits for one **SIFS, only because** it is ACK.



•When the sender does not receive acknowledgement, it automatically retransmits the frame.
•No rules for Retransmissions.
•When more than one station complete for the medium, the system follows the regular 1 DIFS followed by contention window.

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF with RTS/CTS

- In order to **avoid the** hidden terminal problem **and for** contention free access RTS and CTS are used.
- When a sender wishes to send data to a receiver, waits for DIFS if the medium is free or DIFS + Back off when the medium is busy contended by many users.
- The sender sends **RTS** packet(**R**equest **T**o **S**end) a control packet.

Contents of RTS packet

1. Receiver address.
2. Duration (Data transmission plus acknowledgement).

- Every node in the range of sender receiving this RTS has its **Net Allocation Vector (NAV)** in accordance to duration field of RTS.
- NAV resolves the hidden terminal problem.
- If the receiver receives RTS, it sends CTS (Clear to send)control packet **after waiting for SIFS.**

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF with RTS/CTS

Contents of CTS Packet

- Sender and receiver address.
- Duration (Data and Acknowledge).
- **Every node in the range of the receiver receiving this CTS has to set the Node Allocation Vector (NAV) in accordance to the duration field of CTS.**

Note: **The receivers of RTS need not be the same set of CTS.**

Advantage: Medium is Exclusive to one sender.

- After receiving the CTS the sender sends the data packet after 1 SIFS.
- The receiver waits for SIFS after receives the data packet, then acknowledges to the sender.
- Thus the transmission is complete –NAV marks the medium as free.

Disadvantage:

- Collisions can occur at the beginning while the RTS is sent.
- Non negligible overhead in **wastage of bandwidth** for the transmissions of CTS and RTS.
- When the data size is high ,it needs to be fragmented.

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF with RTS/CTS

Fragmentations:

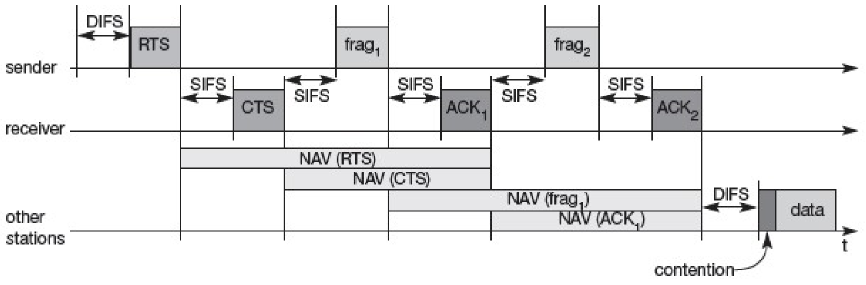
- Generally in wireless LAN, **bit error rate is higher .**
- **To decrease the bit error rate fragmentations needs to be done.**

Concept:

- A Sender can send RTS control packet to reserve the medium after waiting time of DIFS.
- The **RTS packet include the durations for the transmission of the first fragment and the corresponding acknowledgement.** The nodes that receives the **RTS set their NAV according the durations.**
- They receives answers with a CTS including the durations of data transfer and acknowledgement.
- The nodes that receive the CTS set their NAV according the durations.

IEEE 802.11- Medium Access Control Layer

DFWMAC-DCF with RTS/CTS



Content of Fragment:

- Data
- Duration of transmissions for the following fragment, its acknowledgement.
- The receiver of fragment responds in the acknowledgement after SIFS.
- **The fragment contains the duration for the next frame, until the last fragment.**
- **For the last fragments the sender does not reserve the medium any longer.**

IEEE 802.11- Medium Access Control Layer

DFWMAC-PCF with Polling

The disadvantage of the above 2methods:

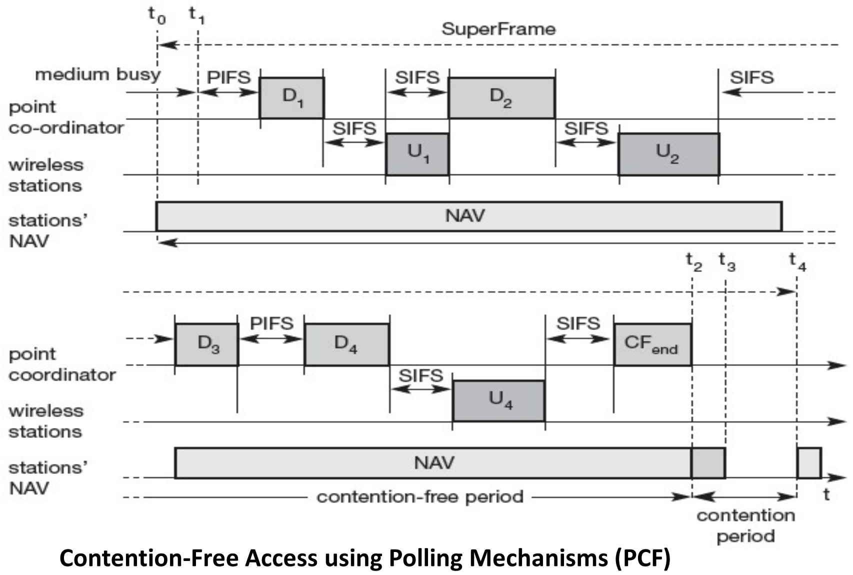
- Cannot guarantee a maximum delay.
- Minimum transmission bandwidth.

Advantages:

- **Provides at time bounded serviced** MAC follows PCF (Point Co-ordinate Function)
- **Requires an access point to control the medium access and polling.**
- The **access point splits the access time into super frame period.**
- The super frame period has
  1. Contentions free period,
  2. Contention period.
- **The Contention Period**: The nodes can use any one of the above methods to gain access to the medium.

IEEE 802.11- Medium Access Control Layer

DFWMAC-PCF with Polling



Contention-Free Access using Polling Mechanisms (PCF)

IEEE 802.11- Medium Access Control Layer

DFWMAC-PCF with Polling

- The super frame starts from t_0 to t_4.But the actual period is from t_1 to t_3 as it has no data from t_3 to t_4.
- **The medium needs to be free from t_0**.But the medium is busy till t_1.Hence the contention free periods starts from t_1 only.
- **After waiting for PIFS, the point co-coordinator can access the medium.**
- **As PIFS is smaller than DIFS no other stations can use the medium .The PCF can send data D_1 to the first wireless station as round robin. It has to transfer hence replies with U_1.**
- **The stations after receiving the data waits for SIFS. The point co-ordinates waits for SIFS and POLLS the second station by sending D_2.**
- **The station may answer to the coordinator with U_2 polling. When it has to transfer else remains unanswered. In the above figure D_3 has no data hence it remains unanswered.**

IEEE 802.11- Medium Access Control Layer

DFWMAC-PCF with Polling

Merits and Demerits:

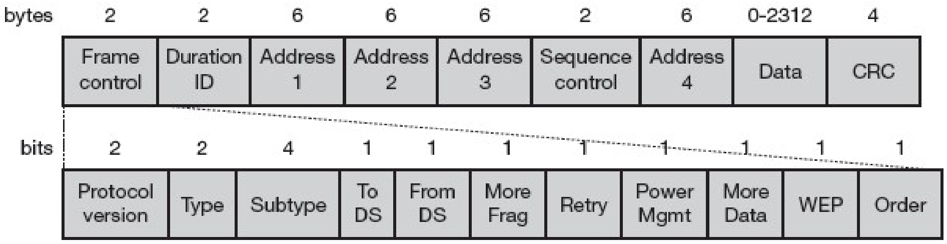
- As PCF needs access point the control and poll, **Ad hoc network cannot use this function**, so **no QOS but best effort services.**
- If only PCF is used and polling is distributed evenly, **bandwidth is also distributed** evenly resembles TDMA.
- This method has **overhead if nodes have nothing to send but access poll them.**

IEEE 802.11- Medium Access Control Layer

MAC Frames

The MAC frame structure of IEEE802.11 is: The frame control field contains:

- **Protocol Versions:** Indicate the current protocol version.
- **Type:** This field determines the **functions of the frame**. If the representation for the value is **00-Management , 01-Control, 10-Data, 11-Reserved**, Each type has several subtypes.
- **Subtype: Example:** 0000-Association Request,1000-Beacon,1011-RTS,1100-CTS
- **User Data:** Sub type=0000.



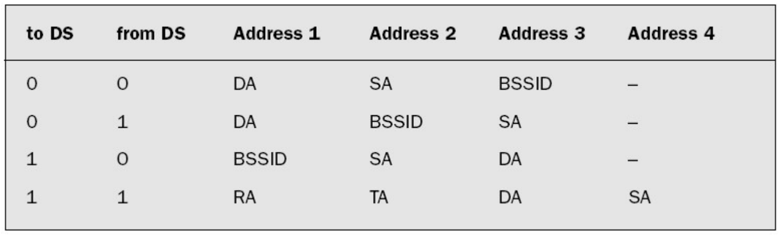
bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Duration ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Data	CRC

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order

IEEE 802.11- Medium Access Control Layer

MAC Frames

- **To DS/From DS(Distributed System):**



to DS	from DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	–
0	1	DA	BSSID	SA	–
1	0	BSSID	SA	DA	–
1	1	RA	TA	DA	SA

More Fragments: Set to **1 for data or management frame.**

Retry: This field is set to **1 when the current frame is a retransmissions of a frame.**

Power management: This field indicates the mode of a station after successful transmission of a frame.

When value = **1** implies the station goes to **power mode.**
= **0** the station is **active.**

IEEE 802.11- Medium Access Control Layer

MAC Frames

More Data: This field is indicates the receiver that the sender has more data to transmit.

- This field can be used by access point to inform that station that **when it is in the power save mode that the access points has buffered the data for the station.**
- This can be used by the station to indicate the access point that more polling is necessary as it has more data ready to transmit.

WEP: Wired Equivalent Privacy.

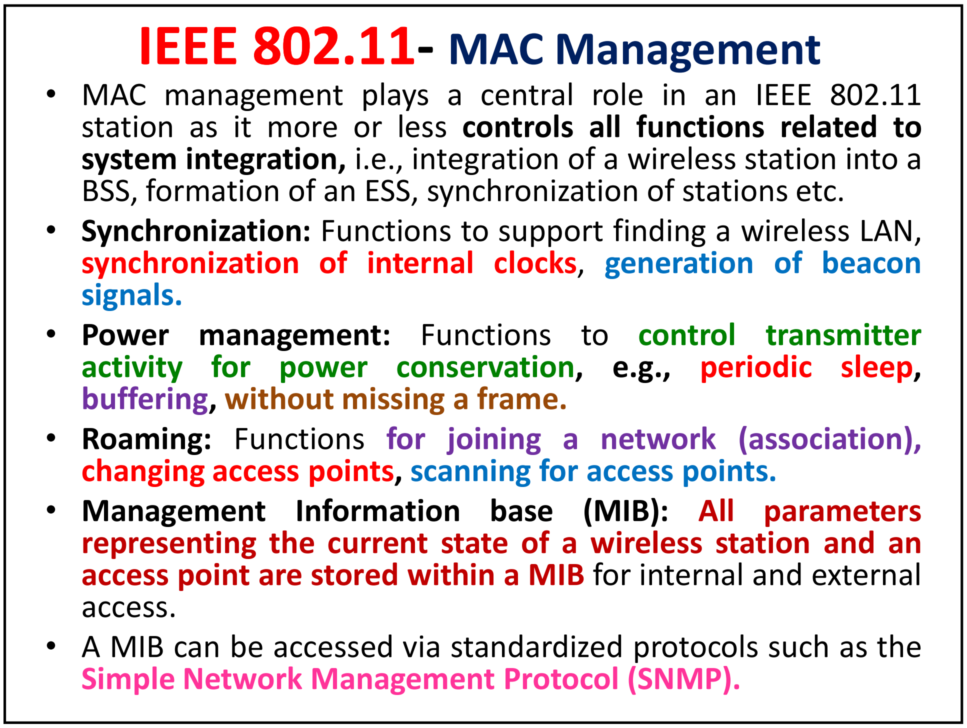
- **Indicates the security mechanism** of 802.11 is applied. But due to weakness of WEP algorithm, higher layer security is needed.

Order: When set, indicate that the received frame must be processed in strict order.

IEEE 802.11- Medium Access Control Layer

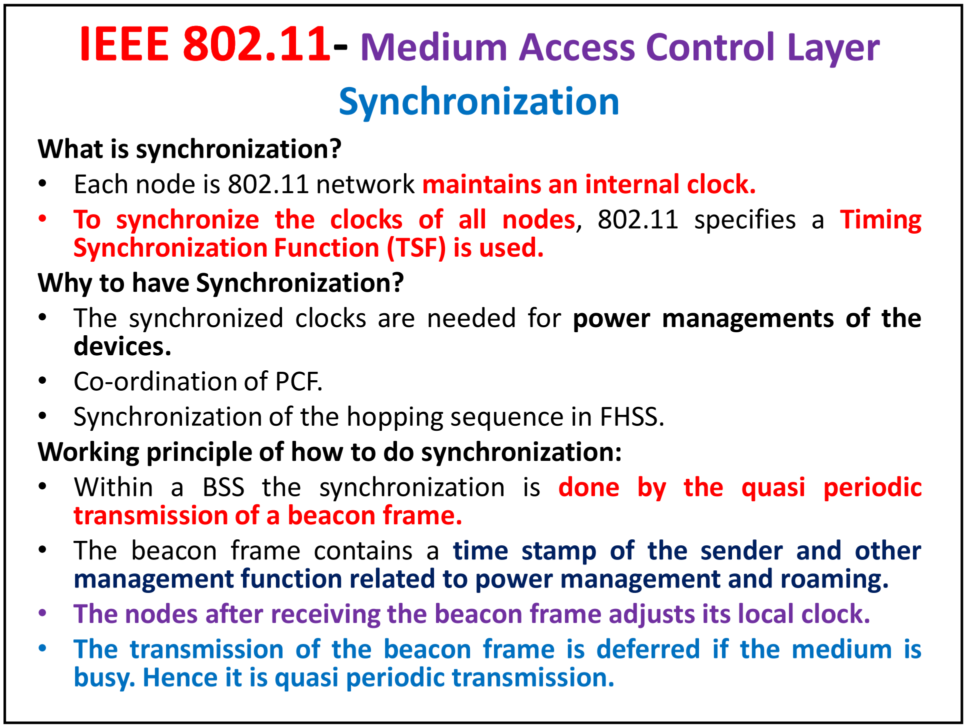
MAC Frames

- **Duration/ID:** when the field value is < 32,768 that the value indicates **the period of time in which the medium is occupied in µs**. when value is >32,768 they are **reserved for identifiers.**
- **Address 1 to Address 4:** the four address field contain MAC addresses. The meaning of the address depends on the DS bit in the frame control field.
- **Sequence Control:** the sequence number is used to filter duplicates.
- **Data:** the data transmitted is up to a maximum of 2312 byte. Which is transferred transparently from a sender to the receiver.
- **CRC:** finally a 32 bit checksum is used to protect the frame.



IEEE 802.11- MAC Management

- MAC management plays a central role in an IEEE 802.11 station as it more or less **controls all functions related to system integration,** i.e., integration of a wireless station into a BSS, formation of an ESS, synchronization of stations etc.
- **Synchronization:** Functions to support finding a wireless LAN, **synchronization of internal clocks**, **generation of beacon signals.**
- **Power management:** Functions to **control transmitter activity for power conservation**, **e.g.,** **periodic sleep**, **buffering**, **without missing a frame.**
- **Roaming:** Functions **for joining a network (association), changing access points**, **scanning for access points.**
- **Management Information base (MIB):** **All parameters representing the current state of a wireless station and an access point are stored within a MIB** for internal and external access.
- A MIB can be accessed via standardized protocols such as the **Simple Network Management Protocol (SNMP).**



IEEE 802.11- Medium Access Control Layer Synchronization

What is synchronization?

- Each node is 802.11 network **maintains an internal clock.**
- **To synchronize the clocks of all nodes**, 802.11 specifies a **Timing Synchronization Function (TSF) is used.**

Why to have Synchronization?

- The synchronized clocks are needed for **power managements of the devices.**
- Co-ordination of PCF.
- Synchronization of the hopping sequence in FHSS.

Working principle of how to do synchronization:

- Within a BSS the synchronization is **done by the quasi periodic transmission of a beacon frame.**
- The beacon frame contains a **time stamp of the sender and other management function related to power management and roaming.**
- **The nodes after receiving the beacon frame adjusts its local clock.**
- **The transmission of the beacon frame is deferred if the medium is busy. Hence it is quasi periodic transmission.**

IEEE 802.11- Medium Access Control Layer

Synchronization

Synchronization in Infrastructure based Network:

- In the infrastructure based network the access point performs Synchronization.
- It transmits the **quasi periodic beacon signal, all the other nodes adjust their local timer to the time stamp.**
- In the first interval. And 3rd interval the AP senses the medium to be idle, transmits the Beacon frame.
- In the second interval and fourth interval.
- The access point defers the beacon frame as the medium is busy.
- But the access point tries to schedule transmissions according to the expected beacon interval (Target Beacon Transmission Time).
- Beacon interval is not shifted if one beacon is delayed.
- The time stamp refers to the real transmit time.
- The Beacon frame has got the time stamp of the AP.

IEEE 802.11- Medium Access Control Layer

Synchronization

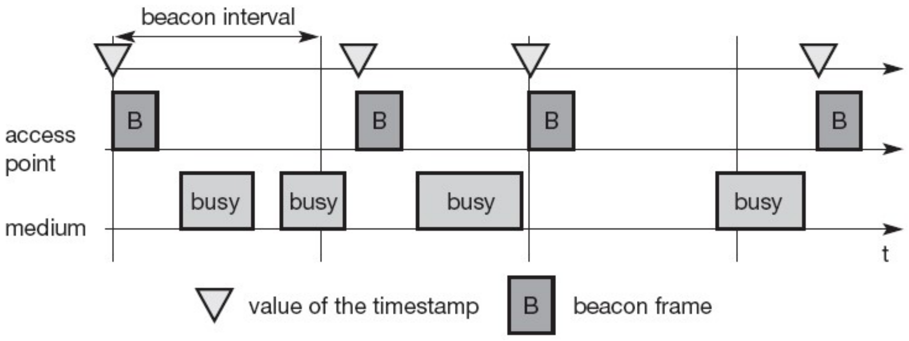


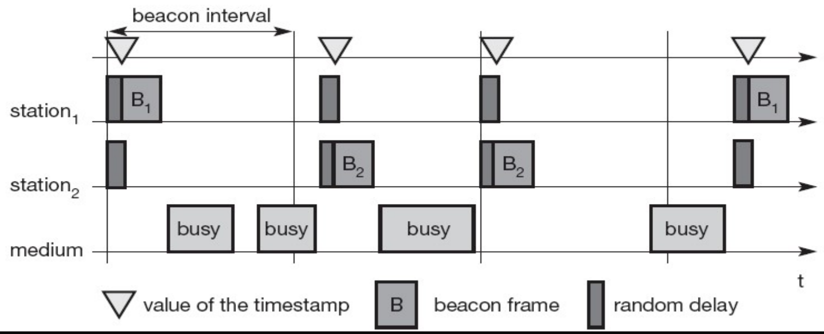
Fig 3.18: Beacon transmission in a busy 802.11 infrastructure network

IEEE 802.11- Medium Access Control Layer

Synchronization

Synchronization in Adhoc Network

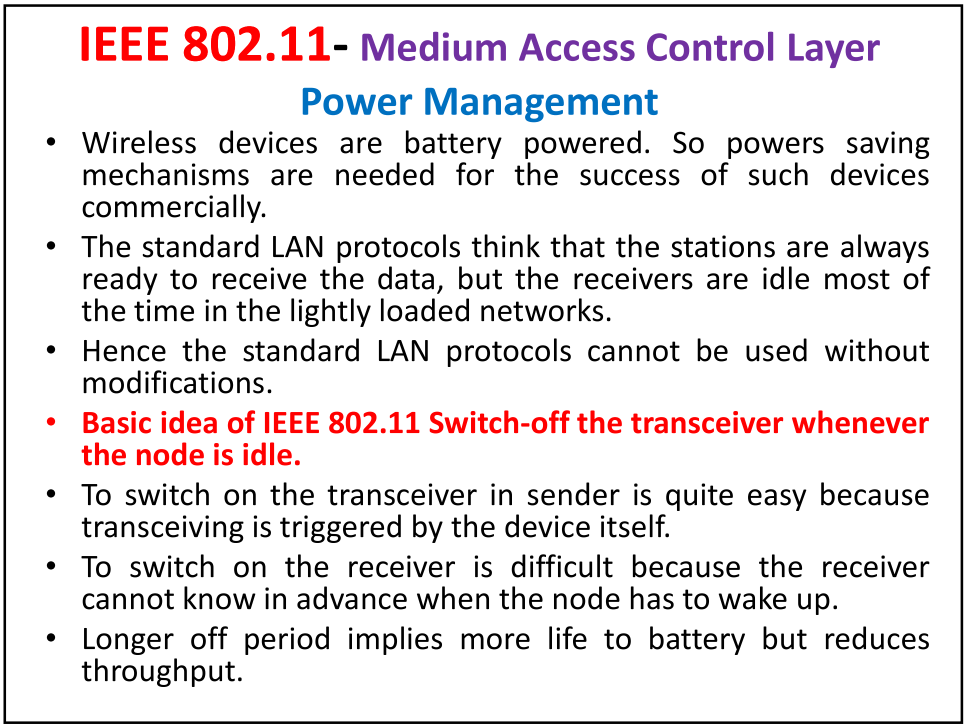
- The Synchronization is more complicated as there is no central arbitrar.
- They do not have the access point for transmission of beacon frame.
- Each node starts the transmission of a beacon frame after the beacon interval.



IEEE 802.11- Medium Access Control Layer

Synchronization

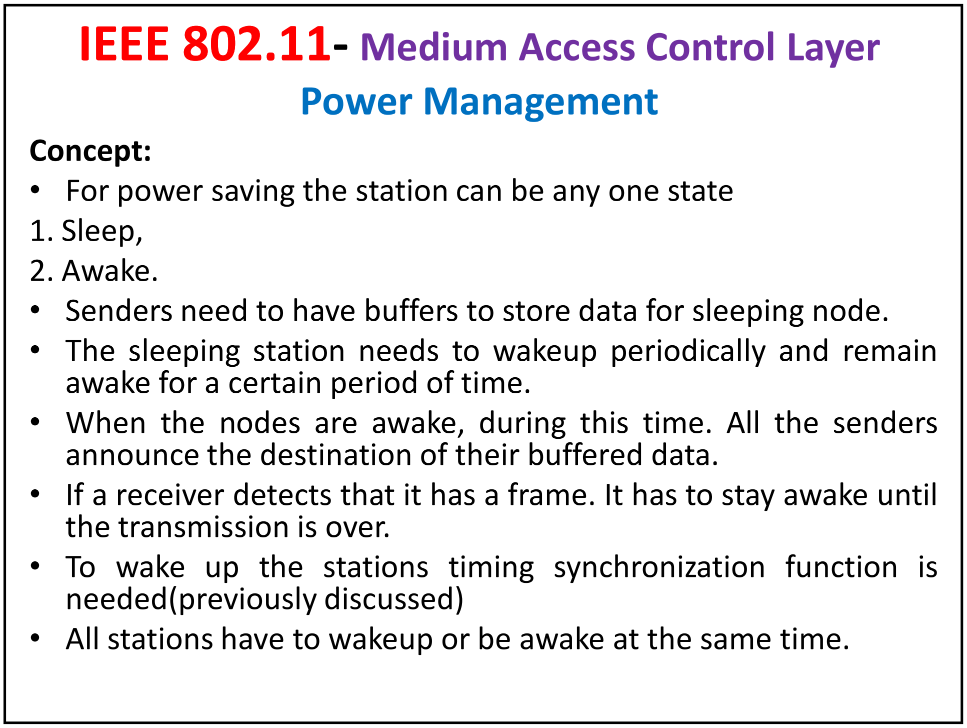
- **As more than one compete standard random back off algorithm is applied. Hence only one beacon wins.**
- All other stations adjust their internal dock in accordance with the received beacon.
- If collision occurs the beacon is lost. Hence the beacon interval is slightly shifted because all clocks may vary as the start of the beacon interval.
- In the above figure station 1 and 2 competes for the medium to transit beacon frame.
- Station 2 succeeds as it has smaller back off time and transmits its time as time stamp in Cycle1.
- In Cycle 2, Station 1 succeeds the medium and transmits its time as the timestamp.



IEEE 802.11- Medium Access Control Layer

Power Management

- Wireless devices are battery powered. So powers saving mechanisms are needed for the success of such devices commercially.
- The standard LAN protocols think that the stations are always ready to receive the data, but the receivers are idle most of the time in the lightly loaded networks.
- Hence the standard LAN protocols cannot be used without modifications.
- **Basic idea of IEEE 802.11 Switch-off the transceiver whenever the node is idle.**
- To switch on the transceiver in sender is quite easy because transceiving is triggered by the device itself.
- To switch on the receiver is difficult because the receiver cannot know in advance when the node has to wake up.
- Longer off period implies more life to battery but reduces throughput.



IEEE 802.11- Medium Access Control Layer

Power Management

Concept:

- For power saving the station can be any one state

1. Sleep,
2. Awake.

- Senders need to have buffers to store data for sleeping node.
- The sleeping station needs to wakeup periodically and remain awake for a certain period of time.
- When the nodes are awake, during this time. All the senders announce the destination of their buffered data.
- If a receiver detects that it has a frame. It has to stay awake until the transmission is over.
- To wake up the stations timing synchronization function is needed(previously discussed)
- All stations have to wakeup or be awake at the same time.

IEEE 802.11- Medium Access Control Layer

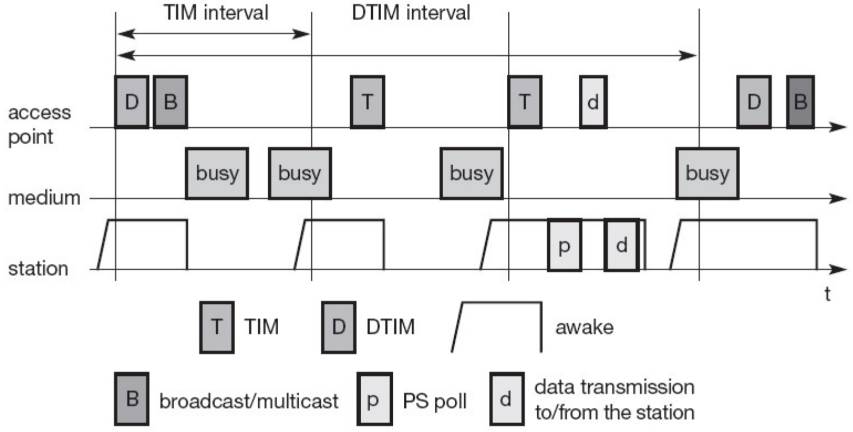
Power Management

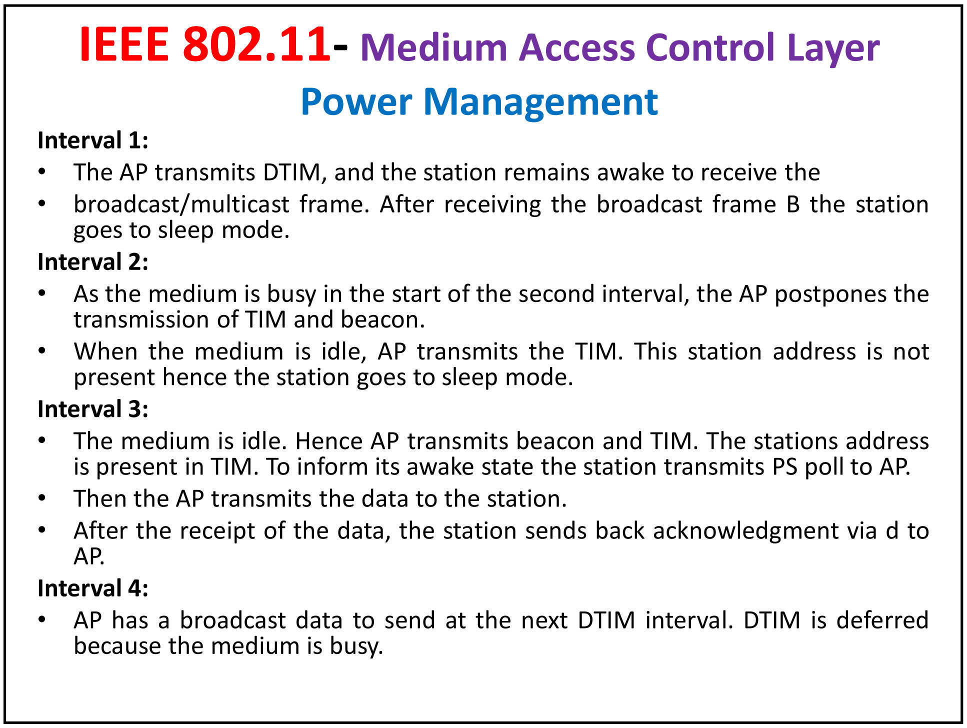
Power Management in infrastructure based network

- Power management is simple because of the presence of access points.
- **Access points buffers all the frames which are desired for stations in the sleeping mode.**
- Along with beacon AP transits TIM (traffic Indication Map) or DTIM (Delivery Traffic Indication Map) is transmitted.
- TIM contains to the list of stations for which unicast data is buffered in the access point.
- DTIM is used to contain the broadcast and multicast frame.
- All the stations wake up prior to TIM/DTIM.
- The Timing Synchronization Function (TSF) assures that the sleeping stations will wake up periodically and listen to the beacon and TIM or DTIM.
- If the station finds its address in the TIM/DTIM then it stays awake for the transmission referring to the above figure.

IEEE 802.11- Medium Access Control Layer

Power Management





IEEE 802.11- Medium Access Control Layer

Power Management

Interval 1:

- The AP transmits DTIM, and the station remains awake to receive the
- broadcast/multicast frame. After receiving the broadcast frame B the station goes to sleep mode.

Interval 2:

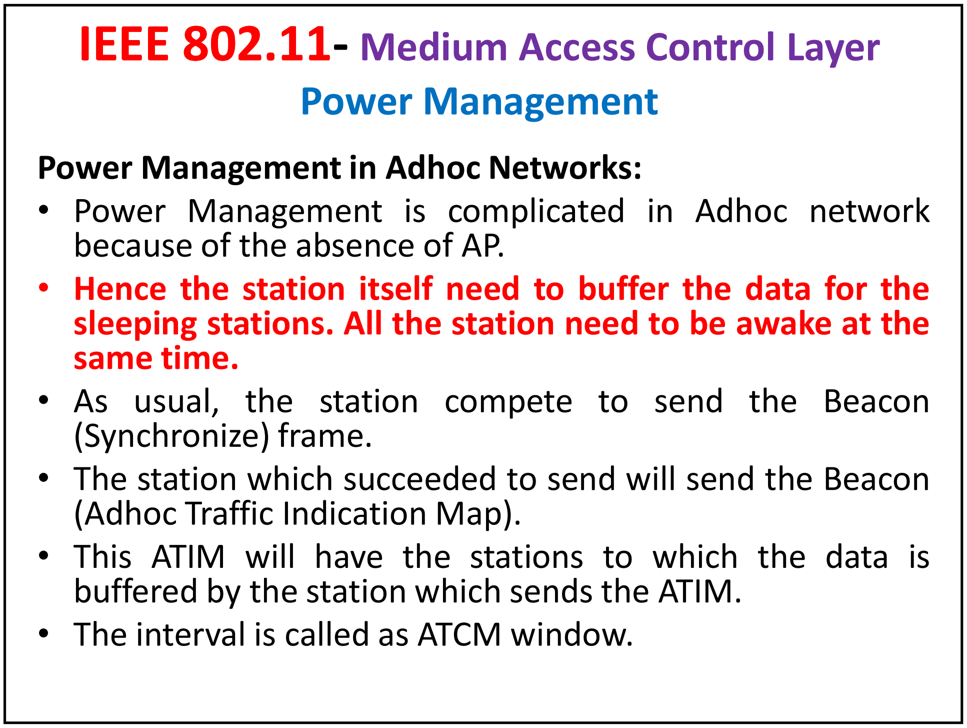
- As the medium is busy in the start of the second interval, the AP postpones the transmission of TIM and beacon.
- When the medium is idle, AP transmits the TIM. This station address is not present hence the station goes to sleep mode.

Interval 3:

- The medium is idle. Hence AP transmits beacon and TIM. The stations address is present in TIM. To inform its awake state the station transmits PS poll to AP.
- Then the AP transmits the data to the station.
- After the receipt of the data, the station sends back acknowledgment via d to AP.

Interval 4:

- AP has a broadcast data to send at the next DTIM interval. DTIM is deferred because the medium is busy.



IEEE 802.11- Medium Access Control Layer

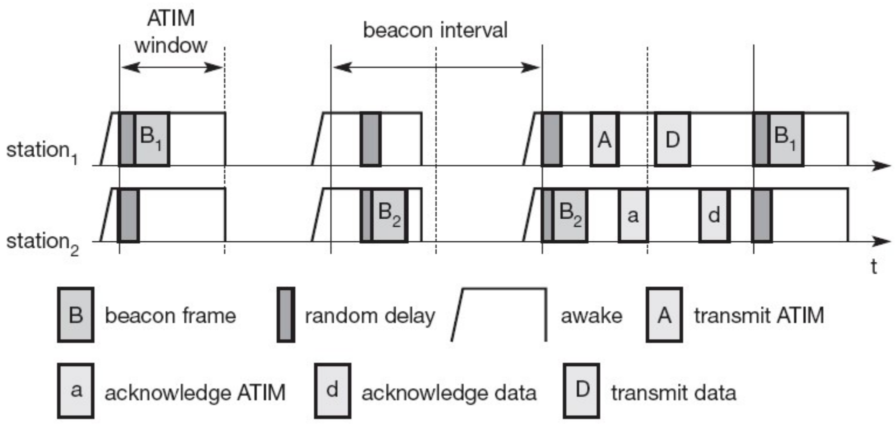
Power Management

Power Management in Adhoc Networks:

- Power Management is complicated in Adhoc network because of the absence of AP.
- **Hence the station itself need to buffer the data for the sleeping stations. All the station need to be awake at the same time.**
- As usual, the station compete to send the Beacon (Synchronize) frame.
- The station which succeeded to send will send the Beacon (Adhoc Traffic Indication Map).
- This ATIM will have the stations to which the data is buffered by the station which sends the ATIM.
- The interval is called as ATCM window.

IEEE 802.11- Medium Access Control Layer

Power Management



IEEE 802.11- Medium Access Control Layer

Power Management

Interval 1: Station 1 succeeds in sending the Beacon. It has not buffered any frame.

Interval 2: Station 2 succeeds in sending the Beacon which too has not buffered any frame.

Interval 3: Station 2 succeeds in sending the Beacon. Station 1 has buffered data to station 2. 1 replies with ATIM to station2. The station 2 acknowledges by sending acknowledgement ATIM (a).

- After receiving this acknowledgement Station 1 transmits data.
- The station 2 acknowledges the same by sending d.
- The stations remain awake in the full interval. Does not enter into sleep mode.

Problems:

1. Does not scale.
2. If many station operate in power save mode all the stations compete to transmit their ATIM within the ATIM within the ATIM window. Which results in collision hence more deferred.
3. Access delay cannot be predicted.
4. QOS cannot be guaranteed under heavy load.

IEEE 802.11- Medium Access Control Layer

Roaming

- If a user walks around with a wireless station, the station has to move from one access point to another to provide, uninterrupted service.
- **Moving between access point is called as Roaming** is another important function
- Steps needed for roaming between access points.

1. A station decides that the current link quality is too poor at present the station is connected to access point AP1. Hence the **station starts scanning for another access point.**
2. **Scanning means the active search for another BSS** that can be used for setting up a new BSS.

- Scanning can be done on single or multiple channels.

IEEE 802.11- Medium Access Control Layer

Roaming-Types of Scanning

Types of Scanning

1) **Passive Scanning**: Listening to the medium , to find other networks(i.e.) receiving the beacon of another network which was issued by the access point for synchronization.

2) **Active Scanning**: sending a probe on each channel and waiting for response. Beacon and probe contain the necessary information to join a new BSS.

3) The station selects the best access points based on scanning. The station sends the association request to the selected access points based on scanning. The station sends the association request to the selected access point AP2.

4) The new access point AP2 answers with an association response.

- If the response is successful the station has associated with a new access point. Else to has to continue scanning.

5) The access point indicates the new station in its BSS to the DS. The DS updates its data base which contains the current location of the wireless station.

- The data base is needed for forwarding frames between different CSS.
- DS informs the old access point AP1, that the station is no longer with in its BSS.

Mobile Network Layer

Mobile Network Layer

- Mobile IP,
- Dynamic Host Configuration Protocol(DHCP),
- Ad Hoc Networks.

Mobile Network Layer

- ➢ Mobile IP
- ➢ Dynamic Host Configuration Protocol(DHCP)

Mobile Network Layer

- Mobile network layer is to support mobility. The most prominent example is **Mobile IP**, which adds mobility support to the internet network layer protocol IP.
- To merge the world of mobile phones with the internet and to support mobility in the small more efficiently, so-called **micro mobility protocols** have been developed.
- Another kind of mobility, portability of equipment, is supported by the **Dynamic Host Configuration Protocol (DHCP).**
- In former times, computers did not often change their location. Today, due to laptops or notebooks, students show up at a university with their computers, and want to plug them in or use wireless access.
- A network administrator does not want to configure dozens of computers every day or hand out lists of valid IP addresses, DNS servers, subnet prefixes, default routers etc.
- DHCP sets in at this point to support automatic configuration of computers.

Mobile IP

Goals, assumptions and requirement of mobile IP

- The **main goal of mobile IP is** supporting end-system mobility **while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols.**
- A host needs a topologically correct address to deliver a packet (mail boat).
- **In a mobile state**, the system will receive many packets. (i.e.) when the system leaves one network and joins another network, in transit the system receives many packets. All these packets need to be delivered correctly.
- A host sends an IP packet with the header and the message. The header contains a destination address.
- The role of the header is to determine, **1) The receiver,2) Physical subnet of the receiver, 3) The packets come to the router, 4) The router routes the packet accordingly.**

Mobile IP

- **Domain Name System** is a table which has logical name and its equivalent IP address.
- The main advantage is its quick reach ability. It has its own disadvantages. Such as The DNS needs some time to update the table.
- If the nodes move often the table cannot be updated quickly and it uses caching to improve scalability (quality).
- **Routers** are built for extremely fast forwarding, but not for fast updates of routing tables.
- Routers are the **brains of the internet**, holding the whole net together.
- No service provider or system administrator would allow changes to the routing tables, probably sacrificing stability, just to provide mobility for individual users.

Mobile IP

- When the solutions did not work, a more general architecture had to be designed.
- Many field trials and proprietary systems finally led to mobile IP as a standard to enable mobility in the internet.
- Several requirements accompanied the development of the standard.

➢ **Compatibility (Capability of existing)**

➢ **Transparency(The quality of being clear and transparent)**

➢ **Scalability (quality) and Efficiency (ratio of the output)**

➢ **Security**

Mobile IP

Terminology used

- **Mobile Node(MN)*:*** Mobile node is an end system (or) router that can change its point of attachment to the internet using mobile IP. The mobile node keeps its IP address and can continuously communicate with any other system in the internet.
- **Correspondent Node(CN):** This is another end for communication. This node can be a fixed node or mobile node.
- **Home Network(HN):** Home network is the subnet the mobile node belongs to with respect to the IP address.
- **Foreign Network(FN):** Foreign Network is the current subnet the mobile node visits which is not the home network.
- **Foreign Agent(FA)*:*** The Foreign Agent provides services to the mobile node during its visit to the foreign network.
- The foreign agent can have a **COA (Care Of Address)** acting as a **tunnel end point forwarding packets to the mobile node.**

Mobile IP

Terminology used

- **The COA defines the current location of the mobile node from the IP point of view**. All the packets sent to the mobile network are delivered to the COA, not to the IP address of the mobile network. The COA is the tunnel end point.
- The COA can be present in either of one location.

➢ **1. Foreign Agent COA:** When the COA is present in FA, the COA is the IP address of FA**. FA is the tunnel end point** and forwards the packet to Mobile Network. Many mobile nodes using the FA can share this COA as common COA.

➢ **2. Co-located COA:** The COA is co-located if the COA is present in the mobile node itself. Here the Mobile Network **temporarily acquires an additional IP address which acts as COA. The tunnel end point is the Mobile Network itself**. This method does not work well in IPV4 due to the scarcity of addresses.

Mobile IP

Terminology used

- **Home Agent(HA)** : Home Agent is present in the home network itself. The Home Agent provides services to the Mobile Network. Home Agent is the tunnel entry point.
- Home Agent has a location registry. **This registry informs the current location of the Mobile Network with the help of current COA.**
- The Home Agent can be present in

➢ **1. Router of the home network:** This is the best position because all the packets for the MN have to go through the router.

➢ **2. Arbitrary node in the subnet:** The disadvantage is the double crossing of the router by the packet, if the Mobile Network is in foreign networks. The packet comes via the router, the HA sends the packet through the tunnel which crosses the router.

➢ **3. Router:** Acts as a manager for Mobile Network belonging to the virtual home network. Disadvantage is that all Mobile Network‟s are always in a foreign network.

Mobile IP

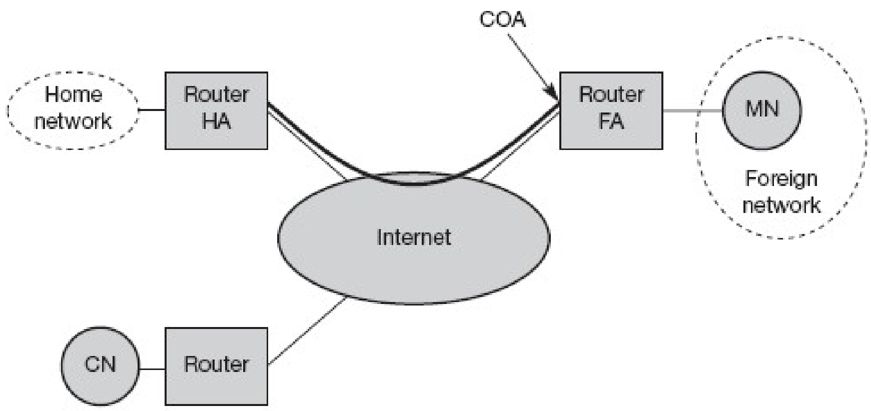


Fig 4.1: Mobile IP example network

Mobile IP

- **IP Packet delivery**

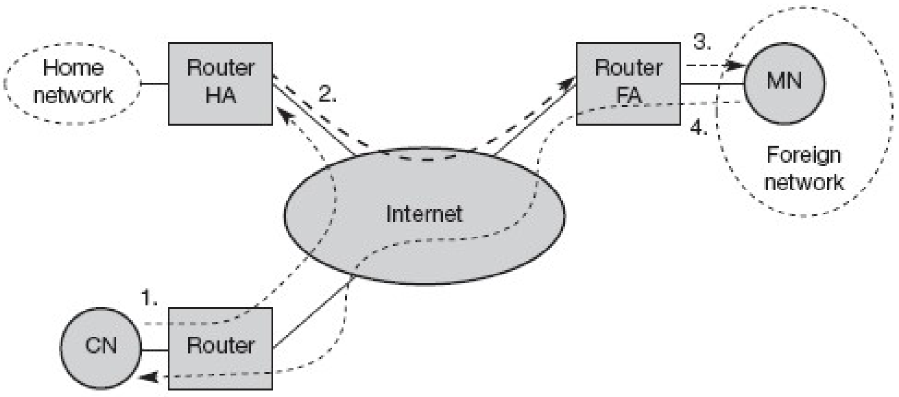


Fig 4.2: Packet delivery to and from the mobile node

Mobile IP

- **IP Packet delivery**

- When the correspondent node wants to send an IP packet to the MN. It transfers the packet to its Router (device) and it does not need to know about the current location of the Mobile Node.
- **Step 1:** Correspondent Node sends the packet to the IP address of the Mobile Network, (i.e.,) Correspond Node sends a packet with MN as destination address, to the router(the HA). The Mobile IP is to support transparency to the packet in transferred to the home network of the Mobile Node.
- **Step2:** Home Agent receives and intercepts the packet .It knows that the MN is not in the Home Network currently with the help of the registry . Hence the packet is not forwarded as usual. **But the packet is encapsulated (reduce in volume) and travelled to the COA**.A new header is attached which contains the Home Agent as the resource add and COA as the destination address.
- **Step 3:** The FA receives the packets, de-capsulate the packet and forwards the original packet to the destination Mobile Node.
- **Step 4:** The Mobile Node sends the packet as usual with its own fixed IP address as source and Correspondent Node's address as destination.

Mobile IP

- **Agent discovery**

  - When the MN moves to a Foreign Network it needs the support of Foreign Agent. To identify the FA, mobile IP suggests two methods.

1. Agent Advertisement.

2. Agent Solicitation.

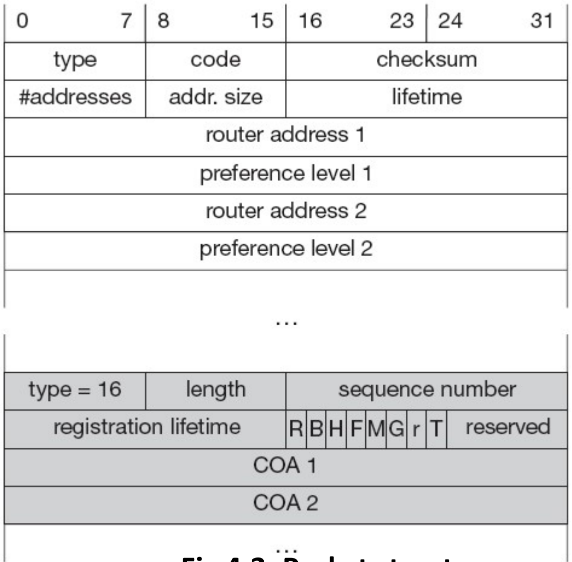
Mobile IP

Agent discovery- 1. Agent Advertisement.

- In this method the **HA and Foreign Agent advertise periodically** the "Agent advertisement messages". These messages are sent as **beacon broadcast to the subnet.**
- **To advertise ICMP (Internet Control Message Protocol) are used.**
- The agent advertisement packet follows RFC 1256 standard plus mobility extension.
- The packets have the following structure in Figure 4.3.
- The **upper part represents the ICMP packet**, the **lower part is the extension needed for mobility.**
- The TTL field of IP packet is =1 for all advertisements to avoid forwarding.
- IP destination address for advertisement is **224.0.0.1** the multicast address (or**) 255.255.255.255** the broadcast address

Mobile IP

Agent Discovery- 1. Agent Advertisement.



0 7	8 15	16 23	24 31
type	code	checksum	
#addresses	addr. size	lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			
...			
type = 16	length	sequence number	
registration lifetime		R B H F M G r T	reserved
COA 1			
COA 2			
...			

Fig 4.3: Packet structure

Mobile IP

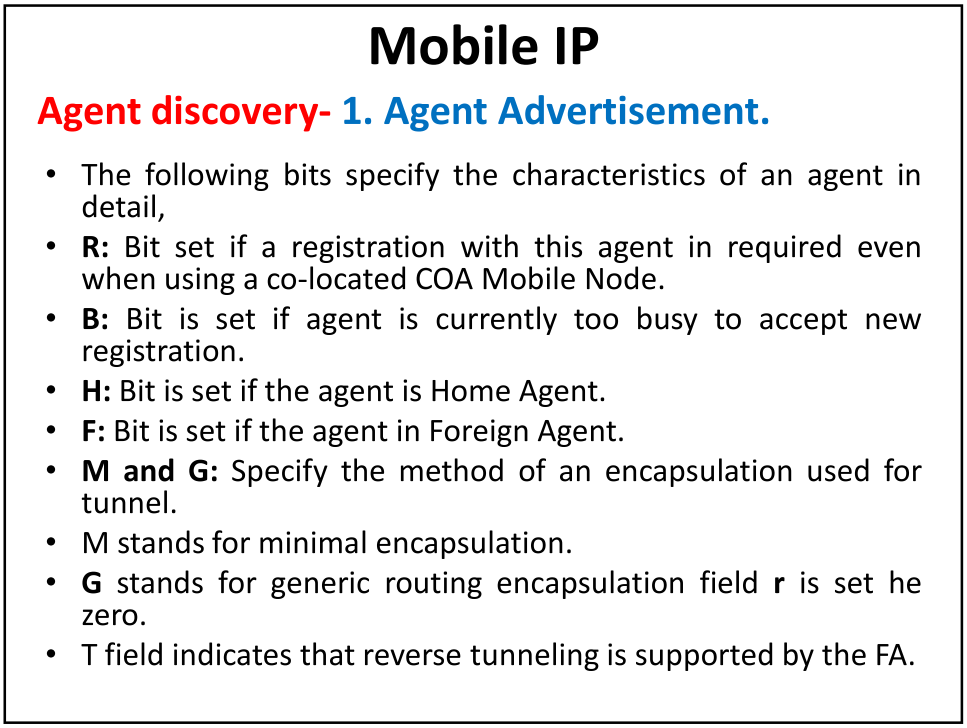
Agent discovery- 1. Agent Advertisement.

- The description for the fields is as follows,
- **Type** is set to 9 (Agent Advertisements) Code =0 if the agent also routes traffic from non-mobile mode.
- Else **Code=16** if the agent routes traffic only from mobile node.
- **Addresses:** The number of router's addresses advertised with this packet, while the addresses themselves follow as shown.
- **Lifetime:** Denotes the length of time this advertisement is valid.
- **Preference Levels** for each address help a node to choose the router that is most eager to get a new node.

Mobile IP

Agent discovery- 1. Agent Advertisement.

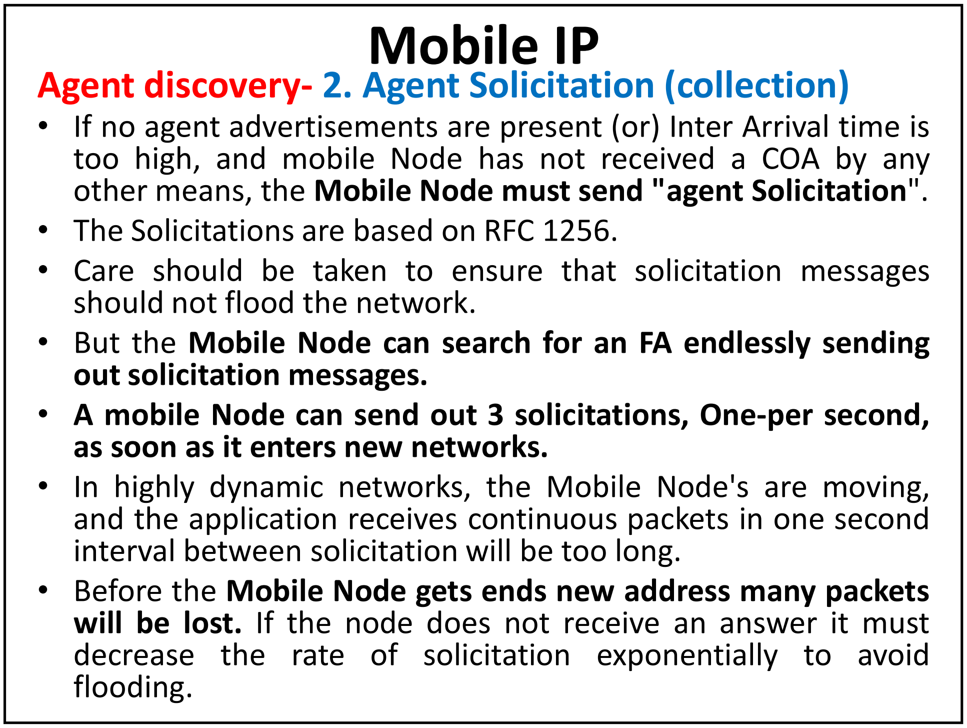
- The extension for the mobility has the following.
- **Type:** Type is set to 16.
- **Length:** Depends upon the number of COA provided with the message and =6 +4*(Number of addresses).
- **Sequence Number:** The total number of advertisements sent since initialization.
- **Registration Life Time:** The agent can specify the maximum life time in seconds a node can request during registration. The Bits specify the character of an agent.



Mobile IP

Agent discovery- 1. Agent Advertisement.

- The following bits specify the characteristics of an agent in detail,
- **R:** Bit set if a registration with this agent in required even when using a co-located COA Mobile Node.
- **B:** Bit is set if agent is currently too busy to accept new registration.
- **H:** Bit is set if the agent is Home Agent.
- **F:** Bit is set if the agent in Foreign Agent.
- **M and G:** Specify the method of an encapsulation used for tunnel.
- M stands for minimal encapsulation.
- **G** stands for generic routing encapsulation field **r** is set he zero.
- T field indicates that reverse tunneling is supported by the FA.



Mobile IP

Agent discovery- 2. Agent Solicitation (collection)

- If no agent advertisements are present (or) Inter Arrival time is too high, and mobile Node has not received a COA by any other means, the **Mobile Node must send "agent Solicitation"**.
- The Solicitations are based on RFC 1256.
- Care should be taken to ensure that solicitation messages should not flood the network.
- But the **Mobile Node can search for an FA endlessly sending out solicitation messages.**
- **A mobile Node can send out 3 solicitations, One-per second, as soon as it enters new networks.**
- In highly dynamic networks, the Mobile Node's are moving, and the application receives continuous packets in one second interval between solicitation will be too long.
- Before the **Mobile Node gets ends new address many packets will be lost.** If the node does not receive an answer it must decrease the rate of solicitation exponentially to avoid flooding.

Mobile IP

- Mobile Node can discover a new agent.

➢ **1. When it is connected to a new network.**

➢ **2. When the Mobile Node is looking for better connection.**

- After either advertisements (or) Solicitation the **Mobile Node receives a COA.**
- **The next step is the registration with HA if Mobile Node is in foreign networks.**

Mobile IP

Registration

- After receiving a COA, the mobile node has to register with HA.
- The function of registration is **to inform the HA the current location for forward of packets.**
- Two ways of registration depending upon the location of the COA.

➢ **COA at FA**

➢ **Co-located COA**

Mobile IP

Registration

- ➢ **COA at FA**

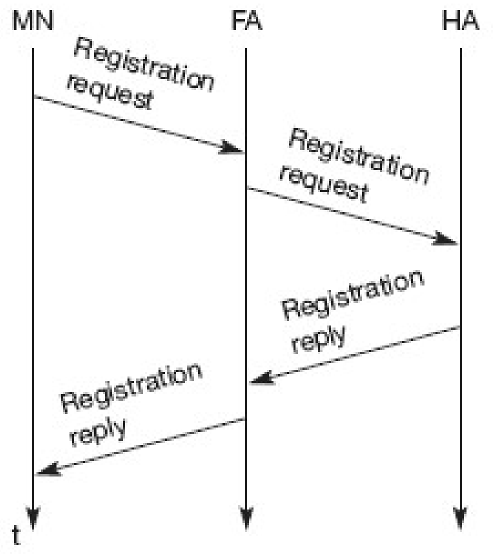


Fig 4.4: COA at FA

Mobile IP

Registration

- ➢ **COA at FA**
- The mobile node sends the registration request to the Foreign Agent.
- The registration request message contains the CAO. The Foreign Agent will forward the request to the HA.
- The Home Agent sets up **mobility binding**. **This contains the mobile node‟s home IP** address and **the current COA.**
- The **mobility binding also contains the life time of the registration.**
- Registration expires after the life time and deleted.
- Registration should be renewed before expiration.
- **After mobility binding, the Home Agent acknowledges by the Sending Registration**
- Reply Message, to FA which in turn is forwarded to Mobile Node.

Mobile IP

Registration

- ➢ Co-located COA

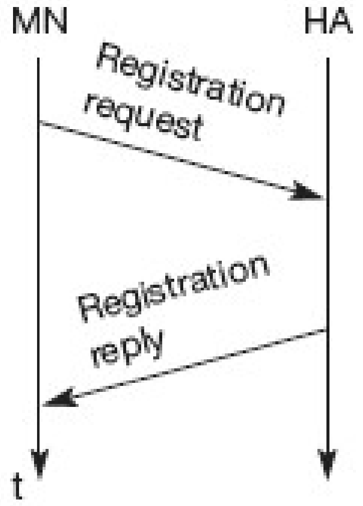


Fig 4.5: Co-Located at COA

Mobile IP

Registration- Format of Registration Request

0 7	8 15	16 23	24 31
type 1	S B D M G r T x	lifetime	
home address			
home agent			
COA			
identification			
extensions . . .			

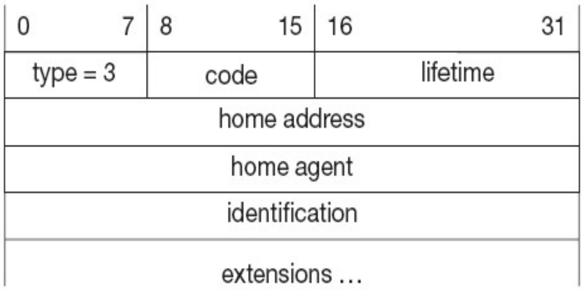
Mobile IP

Registration- Format of Registration Request

- **IP Source address:** It is the Interface address of MN.
- **IP destination address:** It is the FA or HA depending upon the location of COA.
- **Type:** This field is set to "1" for registration request.
- **S Bit:** Set when the MN wants the HA to retain prior mobility bindings.
- **B:** Set when the MN wants to receive the broadcast packets which have been received by the HA.
- **D Bit:** If the MN uses co-located COA it also takes care of decapsulation at the tunnel end point, and then the D-bit is set.
- **M :** Minimal encapsulation.
- **G :** Generic routing encapsulations.
- **T :** Reverse Tunneling: r, x are set to zero**.**
- **Life Time**: It denotes the validity of the registration in seconds. When Life time = 0, It is called as deregistration. All bits set indicate Infinity.
- **Home Address**: Fixed IP address of the MN.
- **Home Agent:** IP address of the HA.
- **COA:** Tunnel end point.
- **Identification:** 64 Bits generated by the MN to identify a request and match in with registration replies.
- **Extension:** Contains the parameter to authentication.

Mobile IP

Registration- Registration Reply



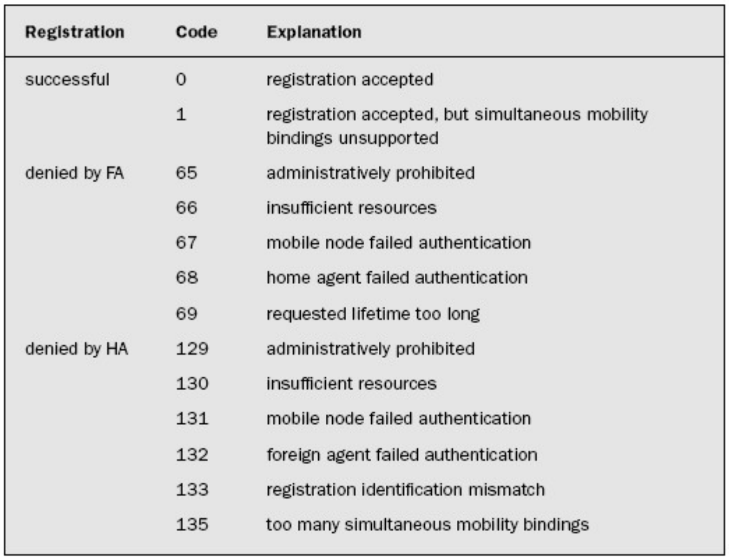
0 7	8 15	16 31
type = 3	code	lifetime
home address		
home agent		
identification		
extensions …		

The fields indicates,

- **Code:** Indicates the result of registration request.
- **Life Time:** Validity of registration in seconds
- **Home Address:** Home address of MN
- **Home Agent:** Address of HA
- **Identification:** 64 Bit, Match the Registration Request and Reply
- **Extension:** Contains the parameter for authentication

Mobile IP

Registration- Registration Reply



Registration	Code	Explanation
successful	0	registration accepted
	1	registration accepted, but simultaneous mobility bindings unsupported
denied by FA	65	administratively prohibited
	66	insufficient resources
	67	mobile node failed authentication
	68	home agent failed authentication
	69	requested lifetime too long
denied by HA	129	administratively prohibited
	130	insufficient resources
	131	mobile node failed authentication
	132	foreign agent failed authentication
	133	registration identification mismatch
	135	too many simultaneous mobility bindings

Fig 4.8: Example Registration Reply codes

Mobile IP

Encapsulation

➢ **Tunneling and Encapsulation**

- **Tunneling** describes the mechanism used to forward the packets between HA and COA.
- **Tunnel** is a **virtual pipe to transfer data packets between the tunnel entry and end point.** Packets entering the tunnel are forwarded and leave the tunnel unchanged.
- To send a packet through a tunnel it is encapsulated.
- **Encapsulation:** Encapsulation is the mechanism of attaching a new header to the existing packet.
- **Decapsulation:** The reverse operation where by the attached header is removed and the original packet are taken out.

Mobile IP

Encapsulation

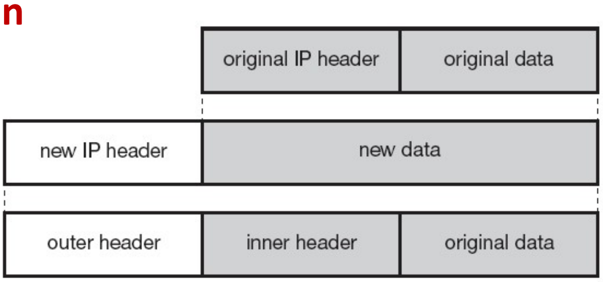


Fig 4.9: IP Encapsulation

- The above fig represents what happens at tunnel entry point.
- The Home agent takes the original packet, and attaches a new IP header which contains the destination address as the COA.
- The new header is called as outer header.
- The already existing header is called as inner header.

Mobile IP

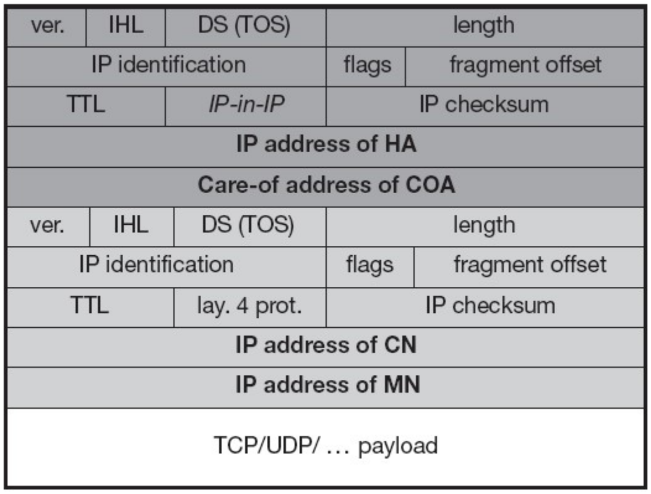
Encapsulation- Types

Three methods of encapsulation are:

1. IP-in-IP Encapsulation
2. Minimal Encapsulation
3. Generic Routing Encapsulation.

Mobile IP

- **IP-in-IP Encapsulation:** This encapsulation is mandatory for mobile IP. The fig 4.9 shows the packet inside a tunnel.



ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		*IP-in-IP*	IP checksum	
IP address of HA				
Care-of address of COA				
ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		lay. 4 prot.	IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ … payload				

Fig 4.9: IP-IP Encapsulation

Mobile IP

Ver: version 4 when it is IPV4

IHL: Internet header length denotes the length of the outer header in 32 bit words.

DS: (TOS) is copied from inner header.

Length: Length of the encapsulated packet.

TTL: TTL must be set high so that the packet can reach the tunnel end point.

IP-in-IP: Protocol type used in IP pay load. set to 4 if protocol type ,the protocol type for IPV4.

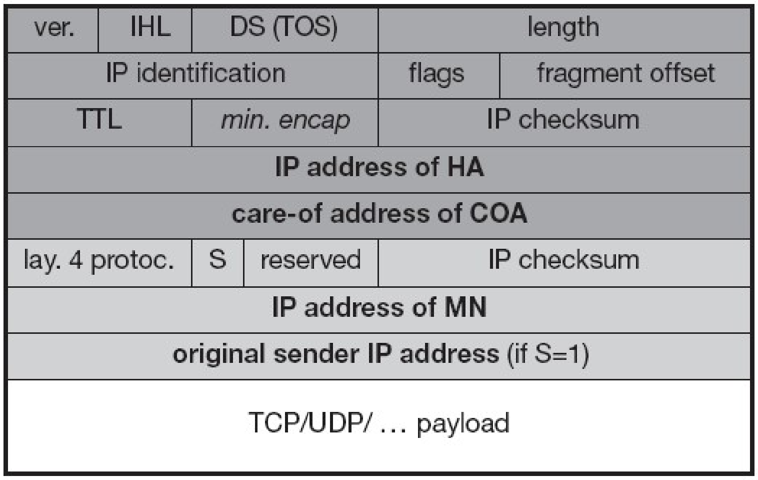
IP Checksum: IP checksum is calculated.

IP address of HA: Tunnel entry point address, which is the address of HA.

COA: Tunnel exit point address, which is the address of COA.

Mobile IP

- **Minimal Encapsulation**: This encapsulation is an optional encapsulation method for mobile IP. The tunnel entry point and end point are specified.



<table>
<tr><td>ver.</td><td>IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="4">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2"><i>min. encap</i></td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6"><b>IP address of HA</b></td></tr>
<tr><td colspan="6"><b>care-of address of COA</b></td></tr>
<tr><td colspan="2">lay. 4 protoc.</td><td>S</td><td>reserved</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6"><b>IP address of MN</b></td></tr>
<tr><td colspan="6"><b>original sender IP address</b> (if S=1)</td></tr>
<tr><td colspan="6">TCP/UDP/ … payload</td></tr>
</table>

Fig 4.10: Minimal Encapsulation

Mobile IP

- **Generic Routing Encapsulation**: This encapsulation supports other network layer protocols. The GRE header is pretended to the packet which contains the original header and data. (The packet is different protocol suite).To the above the new header is pretended. This header is the second protocol suite.

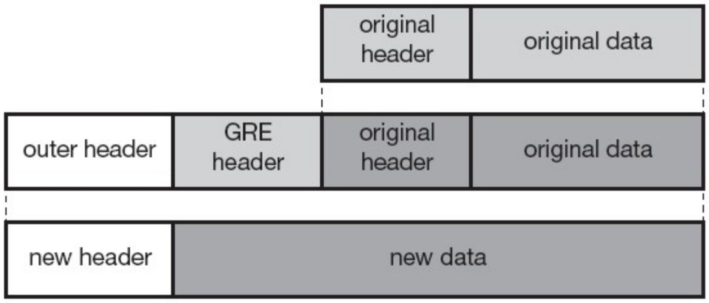
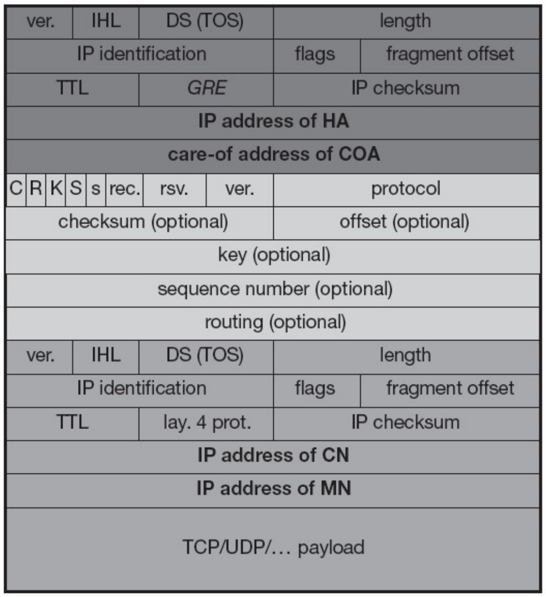


Fig 4.11: Generic Routing Encapsulation(GRE)

Mobile IP

Generic Routing Encapsulation



<table>
<tr><td colspan="4">ver.</td><td colspan="2">IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="8">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="2"><em>GRE</em></td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="10"><strong>IP address of HA</strong></td></tr>
<tr><td colspan="10"><strong>care-of address of COA</strong></td></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>s</td><td>rec.</td><td>rsv.</td><td>ver.</td><td colspan="2">protocol</td></tr>
<tr><td colspan="8">checksum (optional)</td><td colspan="2">offset (optional)</td></tr>
<tr><td colspan="10">key (optional)</td></tr>
<tr><td colspan="10">sequence number (optional)</td></tr>
<tr><td colspan="10">routing (optional)</td></tr>
<tr><td colspan="4">ver.</td><td colspan="2">IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="8">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="2">lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="10"><strong>IP address of CN</strong></td></tr>
<tr><td colspan="10"><strong>IP address of MN</strong></td></tr>
<tr><td colspan="10">TCP/UDP/… payload</td></tr>
</table>

Fig 4.12: Protocol fields for GRE according to RFC1701

Mobile IP

GRE Header:

- Minimal GRE header user 4 bytes.
- **Bits C** when set indicates check sum is present and the field contains a valid Checksum.
- **R Bit** when indicates the offset and routing fields are present and contain valid information.
- **Offset:** Represent offset in Bytes for the first source routing entry.
- **C Bit:** If the C Bit is set offset is also present.
- **R Bit Set:** Check sum must be present.
- **K Bit:** Key field used for authentication.
- **S Bit:** Sequence number field in set when sequence number is present .S in important for in order transmission of packets.
- **Rec:** Recursion control field. This field represents a counter that shows the number of allowed recursive encapsulation.
- When the packet arrives at an encapsulation it checks whether the field=0.
- If not Zero, additional encapsulation is allowed packet is encapsulated, field in by 1, decremented else packet is discarded.
- Default value is 0; allows only one level of encapsulation.

Reserved Fields:

- Field=0 and are ignored at reception.
- **Version: =0 For GRE version.**

Mobile IP

Optimization

- Consider the example. Japanese and a German meet at a conference on Hawaii. Both use their laptops for exchanging data both run mobile IP for mobility support.
- If the Japanese sends a packet to the German, his computer sends the data the Home Agent of the German. (i.e.) from Hawaii to German. The Home Agent in Germany encapsulates the packets and tunnels them to the COA of the German laptop on Hawaii.

➢ The packets have to travel around the world.

➢ This inefficient behavior is called Triangular Routing.

- To optimize needs four additional messages.: **1. Binding Request, 2. Binding Update, 3.Binding Acknowledgement, 4.Binding Warning**

Mobile IP

Optimization

1. Binding Request:

- Any Correspondent Node that wants to know the current location of a mobile Node can send a binding request to the Home Agent.
- The Home Agent can check if the Mobile Node has allowed dissemination of the current location.
- If the Home Agent is allowed to reveal the location it sends back a binding update.

2. Binding Update:

- This message sent by Home Agent to Correspondent Node.
- This message tells the current location of network.
- This message can request an acknowledgement.

Mobile IP

Optimization

3. Binding Acknowledgement:

- If requested Correspondent Node return this acknowledgement after receiving a binding update message.

4. Binding Warning:

- A node decapsulates a packet for a Mobile Node, but the MN has moved to a new FA, the old FA sends binding warning.
- The warning contains Mobile Node‟s HA and the target node address. Target node address in the address of the node that has tried sending packet to Mobile Node.
- The Home Agent receives this message, and the Home Agent sends a binding update to the node that has a wrong COA.

Mobile IP

Optimization

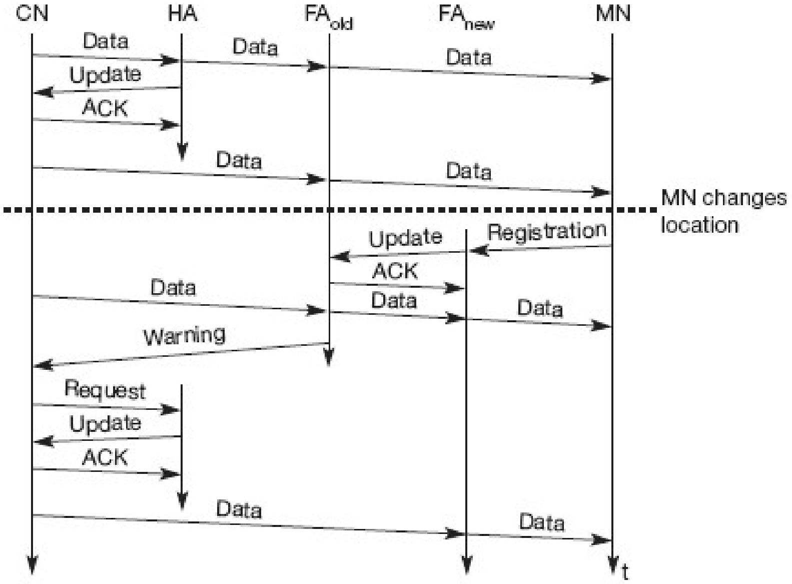


Fig 4.13: Change of the foreign agent with an optimized mobile IP

Mobile IP

Optimization

Explanation: (When the MN has moved)

- The Mobile Node changes its location and register with FA.
- The registration is forwarded to Home Agent.
- The Home Agent updates the registry.
- FA informs FA about the change in location of Mobile Node.
- The new FA passes this old information via update message.
- This message is acknowledged by FA old.
- In case when the Correspondent does not know about the new changes of location, the Correspondent Node transmits packet to FA old.
- The FA old will notice that the Mobile Node is not attached to it. Hence it will forward the packets to FA new.
- This forwarding of packets is called smooth handover.
- In the absence of smooth handover the packets will be lost in the transit.
- To tell the CN that has a sate binding FA old sends warning message to CA.
- CN requests for binding update.
- The Home Agent sends an update to inform them to inform the CN about the new location.
- This message is acknowledged. Hence after CN directly sends the packet to
- Foreign Agent new and avoids triangular routing.

Mobile IP

Reverse Tunneling: The return path from the Mobile Node to CN is not simple. The MN can directly send packets to CN but the problems faced are:

- **Fire Walls:** When the Mobile Node sends a packet with its fixed IP address fire walls will filter these packets because Mobile Node cannot send packets .To overcome this **Network Address Translation** is used by many companies. Reverse tunnel is used to resolve.
- **Multi Cast:** For a Mobile Node in a foreign network to **transmit multicast packets** they need a reverse tunnel.
- **TTL**: When the Mobile Node has removed to a foreign network this **TTL is very low** .Hence the packet will not reach the destination. This scenario reverse tunnel is needed whereby it considers the distance as 1 hop so that the packet reaches the destination within the specified TTL.

Mobile IP- IPV6

Several features that had to be separately specified for V4 come free in IPV6.

1) **Security for authentication** is a feature for IPV6.No special mechanisms needed for security.

2) **Every node masters auto configuration** (i.e.) the mechanisms to acquire COA is built in.

3) **Neighbor discovery** is mandatory for every node .For this no FA is needed to advertise.

4) Every IPV6 nodes can send **binding update** to another node. So the mobile node can send its current COA directly to COA and Home Agent.

Mobile IP- IPV6

5)**A soft handover is possible** .For this the Mobile Node sends in new COA to the old router and the old router encapsulates all incoming packets for the MN and forwards them to the new COA.

6) **FA is not needed any more**. The CN only has to be able to process binding updates .As no FA, the **Mobile Node should be able to decapsulate packets** to detect when needs a new COA and to determine when to send binding update to HA and CN.

7) **IPV6 does not solve any firewall** (or) privacy problem.

Mobile IP- Micro Mobility

- **The Mobile IP faces many problems in the duration of the handover and scalability of registration**. Consider a **larger number of nodes change the network frequently**, a heavy load is present on the home agents and network for registration and binding update messages exists. To have fast seamless handover the “IP micro mobility protocols” comes as handy.
- **Concept:** To understand the concept of Micro mobility protocol considers the following **example**. **A client arrives to the customer‟s place with a laptop.** The Home Agent needs to know only an entry point to the customer network .The entry point acts as the current location. When the client the location within the customer‟s network it should be handle locally to avoid the traffic and to speed up the local handover.

Mobile IP- Micro Mobility

- **Principle:** The Home Agent needs to be informed only when the node changes a region. Three IP micro mobility approaches are

(1)Cellular IP

(2)Hawaii

(3)Hierarchical mobile IPV6

Mobile IP- Micro Mobility

1.Cellular IP

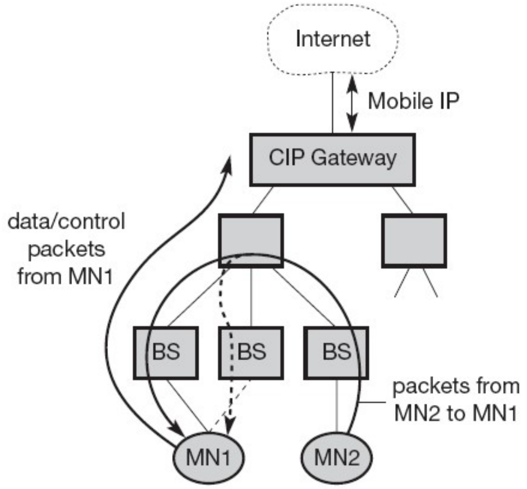


Fig 4.14: Basic Architecture of cellular IP

Mobile IP- Micro Mobility

1.Cellular IP

- Cellular IP provides local handovers by installing a single cellular IP gateway for each Domain.
- This domain acts as a foreign agent to the outside world.
- Inside the domain, all nodes collect the routing information for accessing Mobile Node based on the origin of the packets.
- Soft handover is achieved by simultaneous forwarding of packets destined for a node along multiple paths.

Mobile IP- Micro Mobility

2.Hawaii (Hand-off Aware Wireless Access Internet Infrastructure)

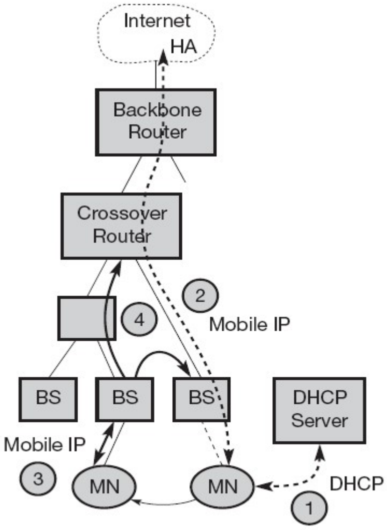


Fig 4.15: Basic architecture of Hawaii

Mobile IP- Micro Mobility

2.HAWAII (Hand-off Aware Wireless Access Internet Infrastructure)

- Tries to keep micro mobility support transparent to Home Agent and Mobile Node.
- Increase Performance and Reliability.
- Support QOS.

Concept:

- **Step1:** When a mobile node enters a HAWAII domain, the mobile Node obtains a co-located COA.
- **Step 2:** Registers with Home Agent.
- **Step 3:** When moving to another cell inside the foreign domain, the MN sends a registration requests to the new base station as to foreign agent.
- **Step 4:** The base station intercepts the registration request and sends out a handoff update message, which reconfigures all routers on paths from the old and new base station to the cross over routes. Routing changes are a initiated by the foreign domain‟s infrastructure and the message as are authenticated.

Mobile IP- Micro Mobility

3. Hierarchical Mobile IPV8

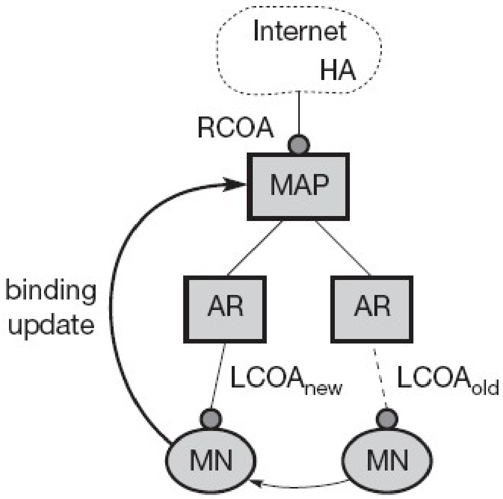


Fig 4.16: Basic architecture of hierarchical mobile IP

Mobile IP- Micro Mobility

3. Hierarchical Mobile IPV8

- Micro mobility is supported by installing a **Mobility Anchor Pointer (MAP).** This MAP is responsible for certain domains and **act as a local HA** with in this domain for visiting Mobile Node.
- MAP receives all packets on behalf of Mobile Node encapsulates and forwards to the Mobile Node‟s current address.
- As long as Mobile Node stays within the domain of MAP, the global COA does not change. This Global COA is called as Regional COA (RCOA).
- The MAP‟s boundaries are defined by Access Routers (AR). The MAP helps in local hand from RCOA to LCOA.
- The Mobile Node registers with the RCOA.
- When the Mobile Node moves locally, it should register with the new LCOA (Local COA) with its MAP.
- RCOA is unchanged.

Dynamic Host Configuration Protocol (DHCP)

1) The aim of DHCP is to simplify the installation and maintenance of network computer.
2) When a new computer is added to the network, DHCP can provide with all necessary information for integration.
3) DHCP provides IP address.

Dynamic Host Configuration Protocol (DHCP)

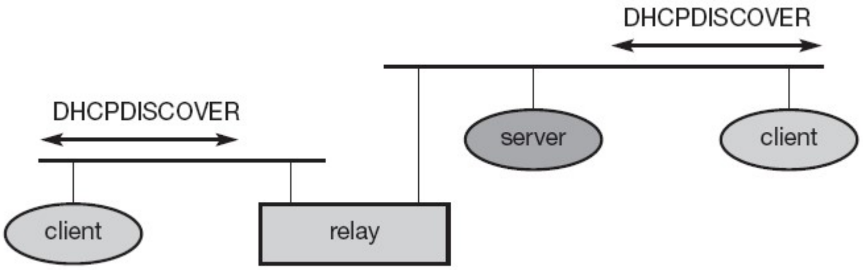


Fig 4.17: Basic DHCP configuration

- DHCP is based on client server model.
- DHCP client sends a request to the server using DHCP Discover, which is broadcasted.
- The server responds.
- The relay is needed to forward across the interworking units to a server.

DHCP- Client Initialization via DHCP

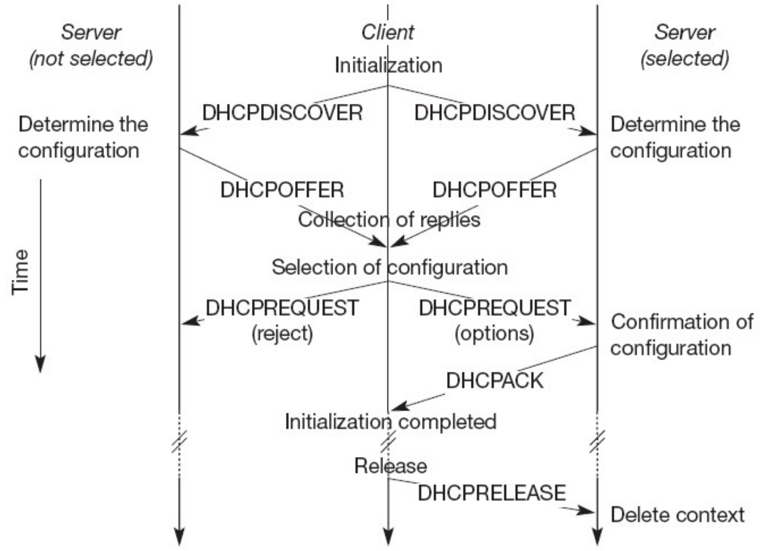


Fig 4.18: Client initialization via DHCP

DHCP- Client Initialization via DHCP

Initialization phase:

- The client broadcasts a DHCPDISCOVER to the subnet. There may be a relay to forward this broadcast.
- In the above figure two servers receive this broadcast and determine the configuration they can offer to the client.
- Server‟s reply to the client‟s request with DHCPOFFER and offers a list of configuration parameters.
- The client can choose one of the configurations offered.
- The client replies to the servers either accepting or rejecting using DHCPREQUEST for rejection the client sends DHCP REQUEST with a reject.
- The rejected server releases the reserved configuration.
- The accepted server sends back DHCPACK acknowledgement.
- This completes the initialization phase.

DHCP- Release

Release:

- When the client leaves the subnet it should release the configuration received from the server.
- It does using the DHCPRELEASE.
- The period of service is fixed.
- If the client dose not reconfirm within that duration the server will free the configuration.
- Thus the DHCP supports the acquisition of COA for the mobile modes.

Dynamic Host Configuration Protocol (DHCP)

- DHCP is a good candidate for supporting the acquisition of care-of addresses for mobile nodes.
- The same holds for all other parameters needed, such as addresses of the default router, DNS servers, the timeserver etc.
- A DHCP server should be located in the subnet of the access point of the mobile node, or at least a DHCP relay should provide forwarding of the messages.
- RFC 3118 specifies authentication for DHCP messages which is needed to protect mobile nodes from malicious DHCP servers.
- Without authentication, the mobile node cannot trust a DHCP server, and the DHCP server cannot trust the mobile node.

Ad Hoc Networks

- Routing

➢ Destination Sequence Distance Vector

➢ Dynamic Source Routing

- Alternative metrics
- Overview of ad-hoc routing protocols

UNIT 3

END