Manet

List the characteristics of Manet

- **Dynamic Topologies:**
  Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network
- **Autonomous Behavior:**
  Each node can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:**
  As nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.
- **Limited Security:**
  Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.
- **Less Human Intervention:**
  They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

Define the term dynamic topology

Network topology which is typically multi hop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.

Explain the meaning of "every node is autonomous"

Each node can act as a host and router, which shows its autonomous behavior.

What do you understand by self-configuring n self-healing nodes

They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature. Separation from central network administration. Each node can play both the roles ie. of router and host showing autonomous nature. Self-configuring and self-healing nodes do not require human intervention.

A self-configurable system must be able to extract the necessary information supporting its software intelligence from the data it collects. They periodically discard the network topology information and rebuild the network from scratch. Basically, if there is change in network topology in the network, there is no certain action that is taken separately to rectify this, so the nodes are capable of rectifying the topology on their own.

Self-healing is the property of a system to detect that it is not operating correctly and, with or without user intervention, makes the necessary adjustments to restore itself to normal. If any errors are found in the network, the nodes can rectify it themselves.

List pros n cons of Manets

Pros	Cons
• Separation from central network administration. • Each node can play both the roles ie. of router and host showing autonomous nature. • Self-configuring and self-healing nodes do not require human intervention. • Highly scalable and suits the expansion of more network hub.	• Resources are limited due to various constraints like noise, interference conditions, etc. • Lack of authorization facilities. • More prone to attacks due to limited physical security. • High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes.

What is manet and list the types of Manets

- **Vehicular Ad hoc Network (VANETs) –**
  Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks(InVANETs) deals with another vehicle or with roadside equipments.

- **Smart Phone Ad hoc Network (SPANC) –**
  To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it.

- **Internet based Mobile Ad hoc Network (iMANETs) –**
  It supports internet protocols such as TCP/UDP and IP. To link mobile nodes and establish routes distributed and automatically.

- **Hub-Spoke MANET:**
  Multiple sub MANET's may be connected in hub-spoke VPN to create a geographically distributed MANET. Normal Ad-hoc routing algorithm does not apply directly.

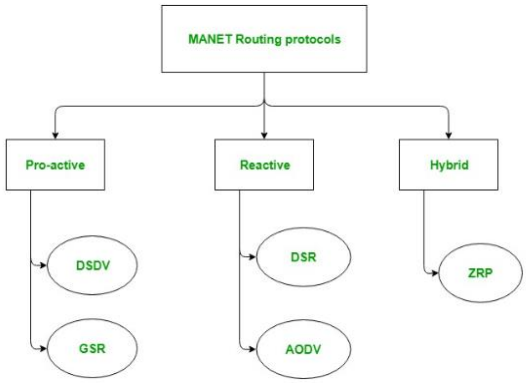
- **Military or Tactical MANETs –**
  This is used by the military units. Emphasis on data rate, real-time demand, fast re-routing during mobility, security, radio range, etc.

- **Flying Ad hoc Network (FANETs) –**
  This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility.

What is the concept of routing in Manet

Nodes do not know the topology of their network, instead they must discover it by their own as the topology in the ad-hoc network is dynamic topology.

The basic rules are that a new node whenever enters an ad-hoc network, must announce its arrival and presence, and should also listen to similar announcement broadcasts made by other mobile nodes.



Differentiate between proactive n reactive routing protocols in Manet

ProActive	ReActive
• These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes. • Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes. • It has a limitation that it doesn't work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.	• These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. • The process of route discovery occurs by flooding the route request packets throughout the mobile network. • It consists of two major phases namely, route discovery and route maintenance.

Explain DSDV Protocol with example

DSDV protocol uses and maintains a single table only, for every node individually. The table contains the following attributes.

Routing Table : It contains the distance of a node from all the neighboring nodes along with the sequence number(SEQ No means the time at which table is updated).

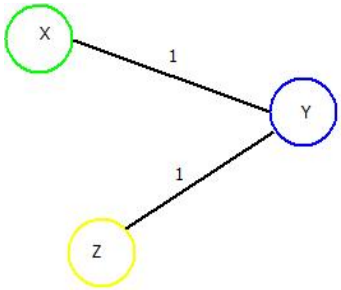
Destination Sequenced Distance Vector Routing : Format

This table is updated on every step and ensures that each node broadcast as well as receives correct information about all the nodes including their distance and sequence number.

In DSDV, nodes broadcasts their routing tables to immediate neighbors with the sequence number.

Every time any broadcasting occurs, the sequence number is also updated along with distances of nodes.

- Consider a network of 3 nodes having distances of “1” on each of the edges respectively. Below mentioned steps will let you know how DSDV works and routing tables are updated.



For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	200-Y
X	Z	Y	2	300-Z

For Y:

Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	200-Y
Y	Z	Y	1	300-Z

For Z:

Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	200-Y
Z	Z	Z	0	300-Z

If “Y” wants to broadcast the routing table. Then updated routing tables of all the nodes in the network will look like as depicted in the below tables where red marked cell denotes the change in sequence number.

For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	210-Y
X	Z	Y	2	300-Z

For Y:

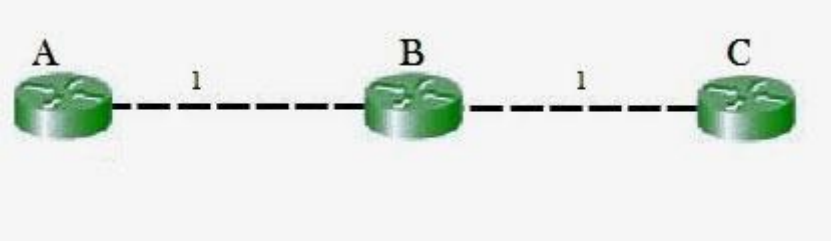
Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	210-Y
Y	Z	Z	1	300-Z

For Z:

Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	210-Y
Z	Z	Z	0	300-Z

Highlight how count to infinity problem be solved using DSDV

- B will know that it can get to C at a cost of 1, and A will know that it can get to C via B at a cost of 2.
- if the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table.
- Before it can send any updates it's possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2.
- B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3. A will then receive updates from B later and update its cost to 4.
- They will then go on feeding each other bad information toward infinity which is called as **Count to Infinity problem**.



Explain the working of GSR protocol along with example and format of all tables

- GSR protocol uses and maintains three tables for every node individually. These tables are:

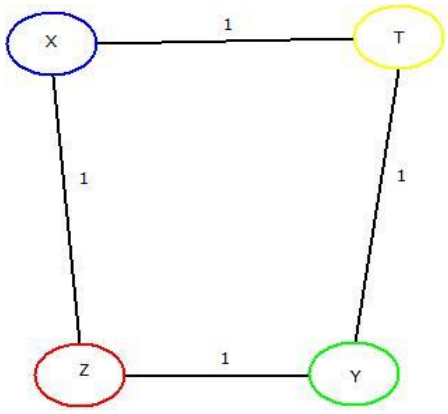
1. Distance Table: This table contains the distance of a node from all the nodes in network.

2. Topology Table: This table contains the information of Link state data along with the sequence number which can be used to determine when the information is updated last.

3. Next Hop Table: Next hop table will contain the information about the immediate neighbor of a particular node.

These tables are updated on every step and ensures that each node receives correct information about all the nodes including their distances.

- Consider a network of 4 nodes having a distance of "1" on each of its edge. Below mentioned steps will let you know how GSR works and how its routing tables are updated.



- For Node "X" : Firstly three tables as mentioned above will be maintained which includes distance table, Topology table and Next hop tables. This same process will be done for rest of the nodes too.

Topology Table

Node	Link State	Sequence
X	{}	----
Y	{}	----
Z	{}	----
T	{}	----

Next Hop Table

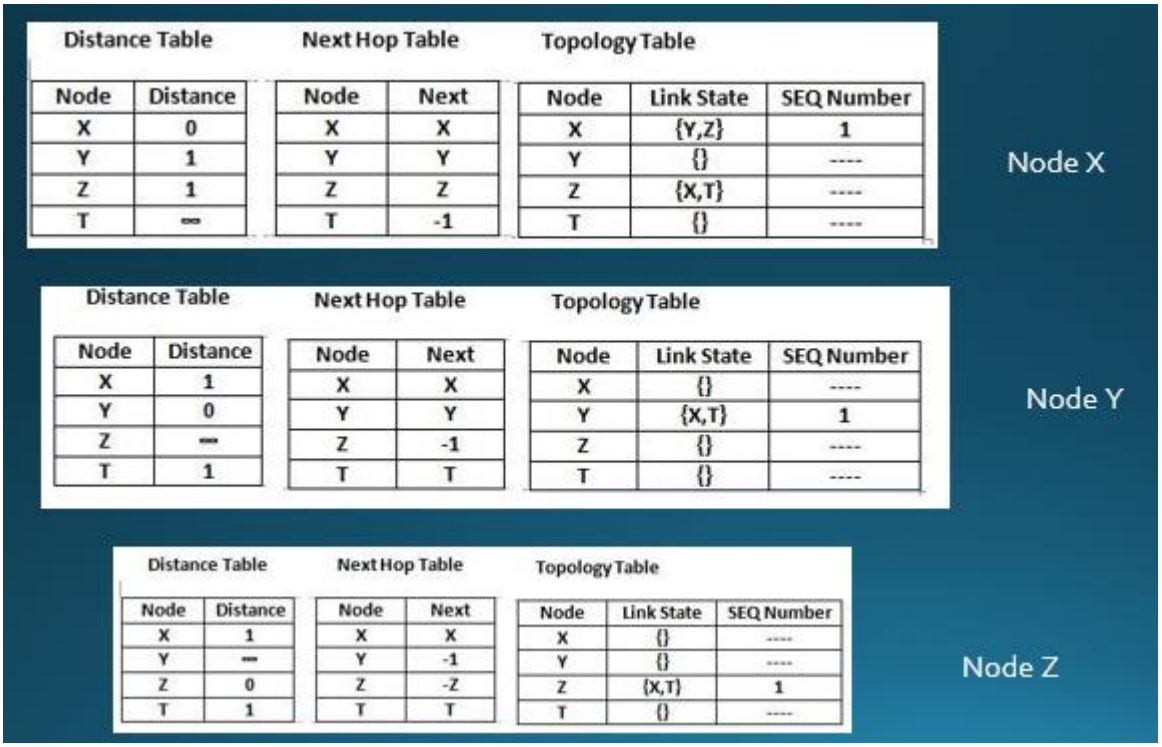
Node	Link State
X	X
Y	-1
Z	-1
T	-1

Distance Table

Node	Distance
X	0
Y	Infinite
Z	Infinite
T	Infinite

- Secondly, broadcasting of all the tables will be done to all the immediate neighbors of "X" i.e. "Y" and "Z".
- These tables are updated at "X", "Y" & "T" nodes respectively.
- Same will be done for node "Y". After first updation from "X", node "Y" will broadcast the tables to its immediate neighbors i.e. "X" & "T" and those tables will be updated accordingly. This will be done for "T" & "Z" also.

- Once done, all the nodes “X”, “Y”, “Z” & “T” will be having the updated routing tables containing distances from each, with the help of which an optimal path can be chosen if data needs to be transferred from one node to other.



Node X

Distance Table

Node	Distance
X	0
Y	1
Z	1
T	∞

Next Hop Table

Node	Next
X	X
Y	Y
Z	Z
T	-1

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{}	----
Z	{X,T}	----
T	{}	----

Node Y

Distance Table

Node	Distance
X	1
Y	0
Z	∞
T	1

Next Hop Table

Node	Next
X	X
Y	Y
Z	-1
T	T

Topology Table

Node	Link State	SEQ Number
X	{}	----
Y	{X,T}	1
Z	{}	----
T	{}	----

Node Z

Distance Table

Node	Distance
X	1
Y	∞
Z	0
T	1

Next Hop Table

Node	Next
X	X
Y	-1
Z	-Z
T	T

Topology Table

Node	Link State	SEQ Number
X	{}	----
Y	{}	----
Z	{X,T}	1
T	{}	----

- **Now, broadcasting of topology tables of “X” will take place to its neighbour i.e. “Y” & “Z” and updated tables will be like as mentioned below.**

For Y:

Distance Table

Node	Distance
X	1
Y	0
Z	2
T	1

Next Hop Table

Node	Next
X	X
Y	Y
Z	X
T	T

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{X,T}	1
Z	{}	----
T	{}	----

For Z:

Distance Table

Node	Distance
X	1
Y	2
Z	0
T	1

Next Hop Table

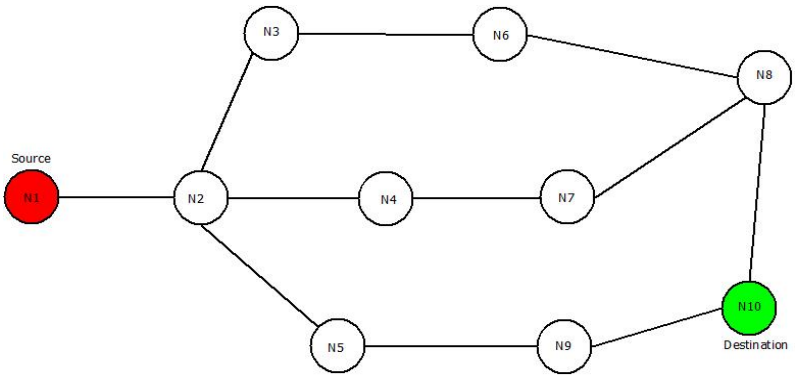
Node	Next
X	X
Y	X
Z	Z
T	T

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{}	----
Z	{X,T}	1
T	{}	----

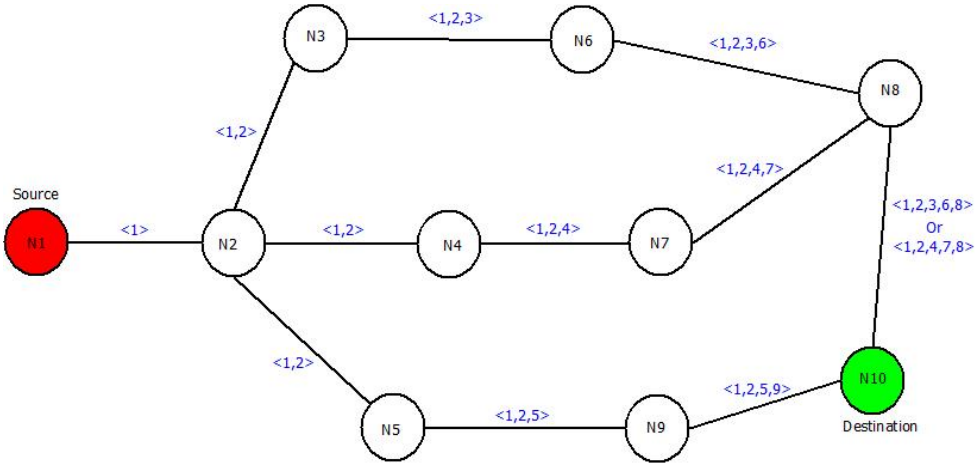
Similarly, these tables are further updated with topology tables of “Y”, “Z” & “T” as done in case of “X.

Explain the process of identifying an optimal path in dynamic source routing with an example



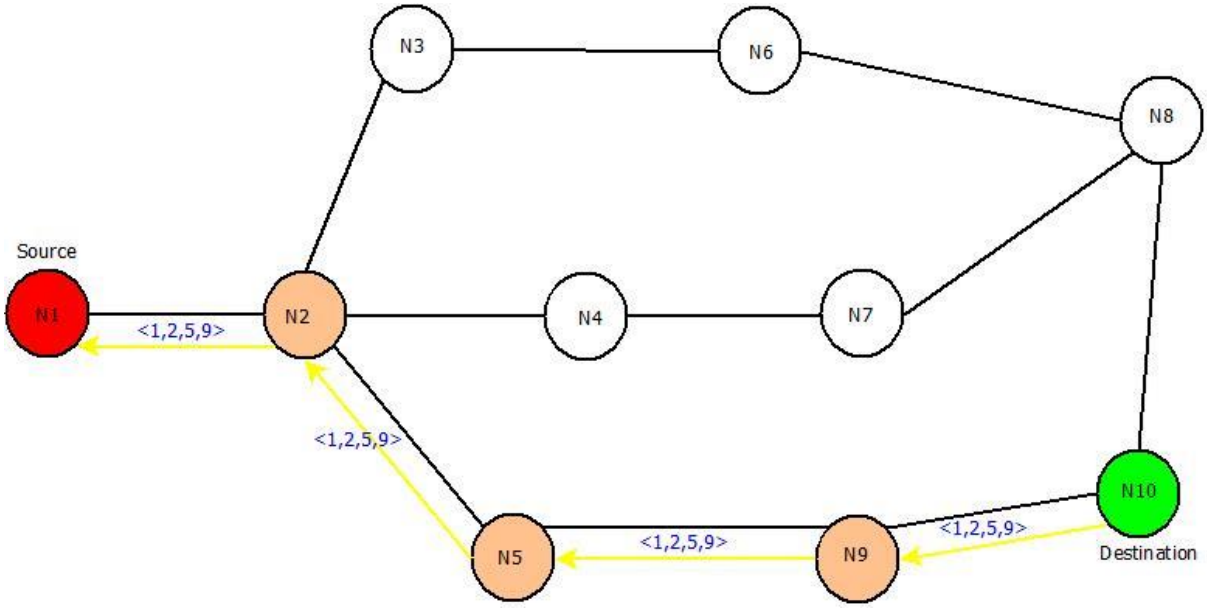
- Step 1: Start from source node N1 and broadcast the information about it to its neighbors i.e. in this case the route information is “<1>”, because of its one-to-one link between node N1 and N2.
- Step 2: Broadcast previous route information to neighbors of node N2 i.e. to node N3, N4, N5. The new route will remain same “<1,2>” in all the cases.
- Step 3: Take node N3 and broadcast previous route(<1,2>) to next neighboring nodes i.e. node N6. New route till node N6 will be “<1,2,3>” and same process can be done for other nodes i.e. Node N4 and N5.
- Step 4 : Further, broadcast the new routes i.e. <1,2,3,6> , <1,2,4> , <1,2,5> to nodes N8, N7 & N9 respectively.
- Step 5: Repeat the above steps until destination node is reached via all the routes.

The updated routes will be as:



- After this, “Re-Request” packet will be sent in backward direction i.e. from destination node “N10” to source node “N1”. It will trace the shortest route by counting the number of nodes from route discovered in previous steps.
- The three possible routes are :
- Route 1: <1,2,3,6,8>

- Route 2: <1,2,4,7,8>
- Route 3: <1,2,5,9>
- Route 3 i.e. "<1,2,5,9>" will be chosen as it contains the least number of nodes and hence it will definitely be the shortest path and then data can be transferred accordingly.
- The Re-Request Packet route can be located as:

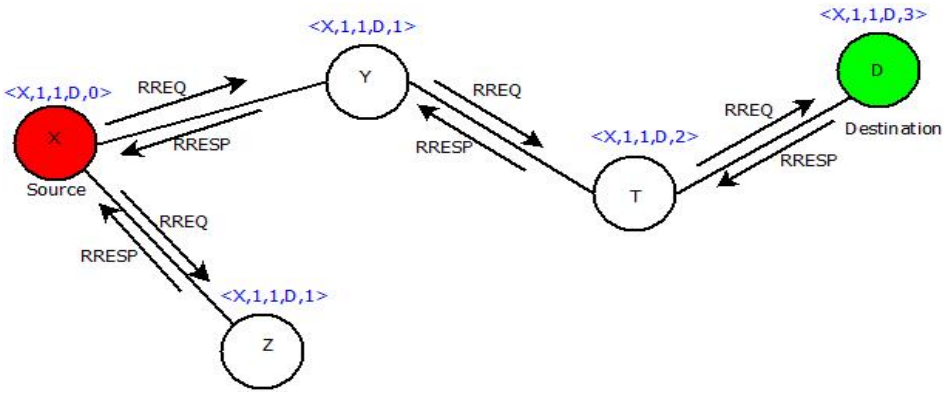


Explain the working of AODV protocol

- In Ad-Hoc On Demand Distance Vector Routing, the source node and destination nodes IP addresses are already known.
- The goal is to identify, discover and maintain the optimal route between source and destination node to send/receive data packets and informative.
- Each node comprises of a routing table along with below mentioned format of Route Request (RREQ) packet.
- RREQ {Destination IP, Destination Sequence Number, Source IP, Source Sequence Number, Hop Count}
- Consider a network containing 5 nodes that are “X”, “Y”, “Z”,” T”,”D” present at unit distance from each other, where “X” being the source node and “D” being the destination node.
- **The IP addresses of source node “X” and destination node “D” is already known. Below mentioned steps will let you know how AODV works, and concept of Route Request (REREQ) and Route Response (RRESP) is used.**
- **Step 1: Source node “X” will send Route Request i.e., RREQ packet to its neighbor’s “Y” and “Z”.**
- **Step 2: Node “Y” & “Z” will check for route and will respond using RRESP packet back to source “X”. Here in this case “Z” is the last node but the destination. It will send the**

RREQ packet to “X” stating “Route Not Found”. But node “Y” will send RRESP packet stating “Route Found” and it will further broadcast the RRESP to node “T”.

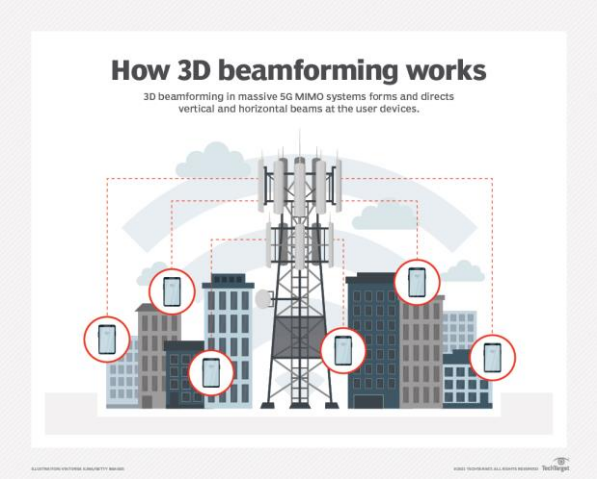
- **Step 3: Now the field of net hop in the RREQ format will be updated, Node “T” will send back the “Route Found” message to Node “Y” and will update the next hop field further.**
- **Step 4: Then Node “T” will broadcast and RREQ packet to Node “D”, which is the destination and the next hop field is further updated. Then it will send RRES packet to “T” which will further be sent back to the source node “X” via node “Y” and Node “T” resulting in generation of an optimal path. The updated network would be:**



MIMO

Explain the concept of beam forming in MIMO

Beamforming is an RF management technique that maximizes the signal power at the receiver by focusing broadcast data to specific users instead of a large area. With 5G, three-dimensional (3D) beamforming forms and directs vertical and horizontal beams at the user. These can reach devices even if they're at the top of a high-rise, for example. The beams prevent interference with other wireless signals and stay with users as they move throughout a given area.



What is the advantage of MIMO technology

- MIMO enables stronger signals. It bounces and reflects signals, so a user device doesn't need to be in a clear line of sight.
- Video and other large-scale content can travel over a network in large quantities.
- This content travels more quickly because MIMO supports greater throughput.
- Many data streams improve visual and auditory quality. They also decrease the chance of lost data packets.

Differentiate between OFDM and FDM

- OFDM builds on simpler frequency-division multiplexing (FDM).
- In FDM, the total data stream is divided into several subchannels, but the frequencies of the subchannels are spaced farther apart so they do not overlap or interfere.
- With OFDM, the subchannel frequencies are close together and overlapping but are still orthogonal, or separate, in that they are carefully chosen and modulated so that the interference between the subchannels is canceled out.

Application of OFDM systems

- Digital radio, Digital Radio Mondiale, and digital audio broadcasting and satellite radio.
- Digital television standards, Digital Video Broadcasting-Terrestrial/Handheld (DVB-T/H), DVB-Cable 2 (DVB-C2). OFDM is not used in the current U.S. digital television Advanced

Television Systems Committee standard, but it is used in the future 4K/8K-capable ATSC 3.0 standard.

- Wired data transmission, Asymmetric Digital Subscriber Line (ADSL), Institute of Electrical and Electronics Engineers (IEEE) 1901 powerline networking, cable internet providers. Fiber optic transmission may use either OFDM signals or several distinct frequencies as FDM.
- Wireless LAN (WLAN) data transmission. All Wi-Fi systems use OFDM, including IEEE 802.11a/b/g/n/ac/ax. The addition of OFDMA to the Wi-Fi 6/802.11ax standard enables more devices to use the same base station simultaneously. OFDM is also used in metropolitan area network (MAN) IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX>) installations.
- Cellular data. Long-Term Evolution (LTE) and 4G cellphone networks use OFDM. It is also an integral part of 5G NR cellular deployments.

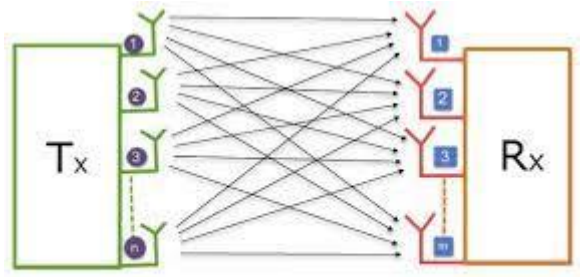
Define the term MIMO and Diversity gain in MIMO

MIMO

Multiple-Input Multiple-Output (MIMO) is **a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time**.

All wireless products with 802.11n support MIMO. The technology helps allow 802.11n to reach higher speeds than products without 802.11n.

an antenna technology for wireless communications in which multiple antennas are used at both the source (transmitter) and the destination (receiver).



Basic Structure of a MIMO System

Diversity Gain

Diversity gain is **the decreased required receive SNR for a given bit error rate (BER) averaged over the fading**.

This is the reduction in fading margin that's obtained by reducing the fading with the smart antenna.

WLAN

What are the advantages of wireless LAN

- very flexible within the reception area
- Ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

Compare infrared and radio transmission technology wrt wireless LAN

Infrared	Radio
• uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.) Advantages • simple, cheap, available in many mobile devices • no licenses needed • simple shielding possible Disadvantages • interference by sunlight, heat sources etc. • many things shield or absorb IR light • low bandwidth • Example • IrDA (Infrared Data Association) interface available everywhere	• typically using the license free ISM band at 2.4 GHz Advantages • experience from wireless WAN and mobile phones can be used • coverage of larger areas possible (radio can penetrate walls, furniture etc.) Disadvantages • very limited license free frequency bands • shielding more difficult, interference with other electrical devices • Example • WaveLAN, HIPERLAN, Bluetooth

Explain basics of zigbee technology.

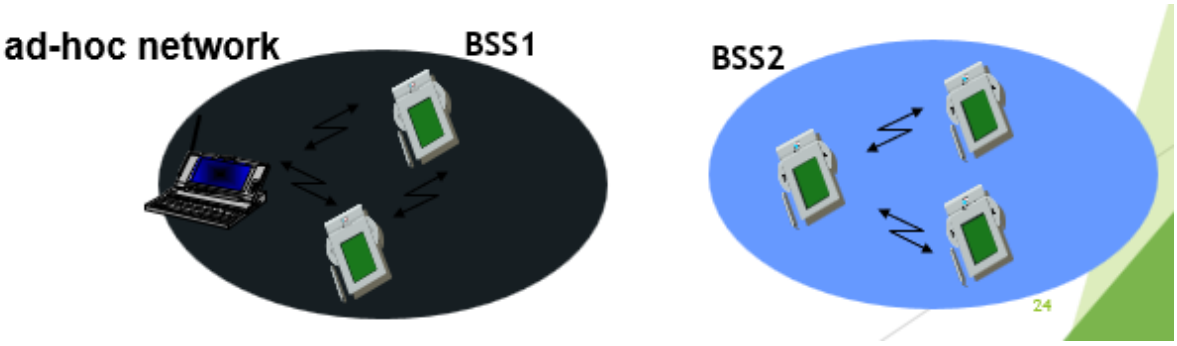
- Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.
- Zigbee is for low-data rate, low-power applications and is an open standard.
- Zigbee products have been extended and customized by vendors and, thus, plagued by interoperability issues.
- In contrast to Wi-Fi networks used to connect endpoints to high-speed networks, Zigbee supports much lower data rates and uses a mesh networking protocol to avoid hub devices and create a self-healing architecture.
- IEEE 802.15.4 wireless standard for wireless personal area networks (WPANs). The Zigbee WPANs operate on 2.4 Ghz, 900 MHz and 868 MHz frequencies.

Differentiate between single hop and multi-hop wireless transmission.

Single-Hop	Multi-Hop
• The network in which the devices (i.e. citation and location) are the only stations on the system. • If a packet moves from origin to target using a single node unit, it is known as a single hop method. • Single hop network is a growing network within a 192.168.0.1 to 255 IP router.	• A network that, apart from the two nodes, there is at least 1 other platform in the route between source and the target. • Multi-hop routing is a form of communication in radio networks where the area of the system is greater than the radar range of individual points. • In the multi-hop routing system, nodes positioned farther away from the node use other intermediary points forwarding data to the node.

Explain the architecture of IEEE 802.11.

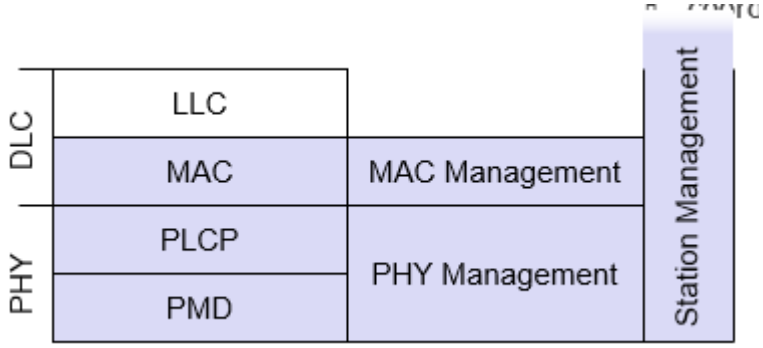
- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN
- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations



Describe the 802.11layers and their respective functions.

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
  - PMD

- Physical Medium Dependent modulation, coding
- PHY Management
    - channel selection, MIB
    - Station Management
    - coordination of all management functions



Describe the variants of physical layer used in 802.11.

IEEE 802.11 supports three different physical layers: one layer based on infra-red and two layers based on radio transmission

All PHY variants include the provision of the clear channel assessment signal (CCA). This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle. The transmission technology (which will be discussed later) determines exactly how this signal is obtained

3 versions of spread spectrum:

2 radio (typ. 2.4 GHz),

1 IR data rates 1 or 2 Mbps

1. FHSS (Frequency Hopping Spread Spectrum)

spreading, despreading, signal strength, typically 1 Mbps min. 2.5 frequency hops/s (USA), two-level GFSK modulation

a. Synchronization

synch with 010101... pattern

b. SFD (Start Frame Delimiter)

0000110010111101 start pattern

c. PLW (PLCP_PDU Length Word)

length of payload incl. 32 bit CRC of payload, PLW < 4096

d. PSF (PLCP Signaling Field)

data of payload (1 or 2 Mbit/s)

e. HEC (Header Error Check)

CRC with x16+x12+x5+1

2. DSSS (Direct Sequence Spread Spectrum)

DBPSK modulation for 1 Mbps (Differential Binary Phase Shift Keying), DQPSK for 2 Mbps (Differential Quadrature PSK)

preamble and header of a frame is always transmitted with 1 Mbps, rest of transmission 1 or 2 Mbps

chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)

max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

3. Infrared

850-950 nm, diffuse light, typ. 10 m range carrier detection, energy detection, synchronization

How is mobility restricted using WLANs? What additional elements are needed for roaming between networks, how and where can WLANs support roaming? In your answer, think of the capabilities of layer 2 where WLANs reside.

Without further mechanisms mobility in WLANs is restricted to the coverage of a single access point. To support roaming additional, inter access point protocols are needed. The access points must inform each other about the current active stations within their coverage. This approach is only feasible for local areas, otherwise location registers etc. like GSM are required. The access points simply operate as transparent, self-learning bridges that need additional information to —forget stations faster compared to the aging mechanisms in fixed network bridges. Station identification is based on MAC addresses. Roaming typically requires a switched layer-2-network.

If Bluetooth is a commercial success, what are the remaining reasons for the use of infrared transmission for WLANs?

One reason for infrared is still cost – IR devices are very cheap and very simple to integrate. Another advantage is the simple protection from eavesdropping. Attackers can much more easily tap Bluetooth communication, incautious users even let their Bluetooth devices open for public access (simply scan for Bluetooth devices at public devices - many are detectable). IR communication is much more secure as the devices must face each other (directed IR).

How do 802.11 and Bluetooth solve the hidden terminal problem.

802.11 uses the MACA mechanism sending RTS/CTS to solve the hidden terminal problem. In Bluetooth, too, are no hidden terminals as the master controls all visible slaves. If a terminal does not see the master, it cannot participate in communication. If this terminal sends anyway, it will not interfere as this terminal, then acts as master with a different hopping sequence.

How are fairness problems regarding channel access solved in IEEE 802.11 and Bluetooth respectively?

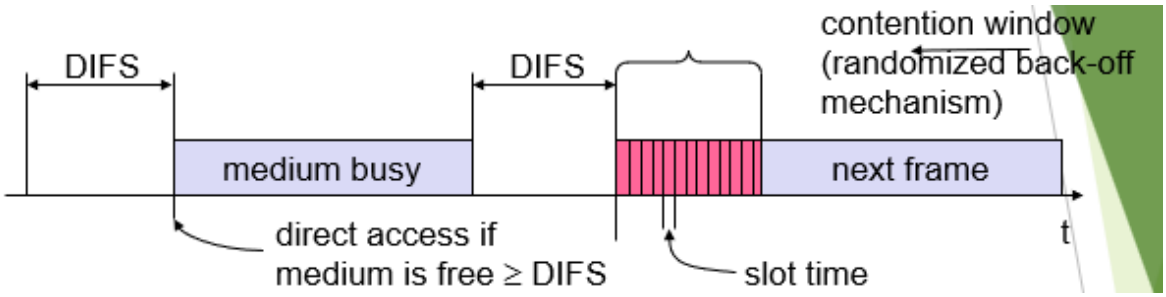
802.11 implements a back-off mechanism that tries to offer fair access to the medium in the standard case (no polling from the access point). If all systems behave well this mechanism gives a

fair share of the overall bandwidth to all stations. In HiperLAN2 and Bluetooth medium access is controlled by an access point or master, respectively. Fairness then depends on these special nodes, which also decide upon the waiting time of a packet when it will be transmitted. In 802.11 the waiting time directly influences the chances for transmission in the next contention cycle.

Explain the access methods used in 802.11.

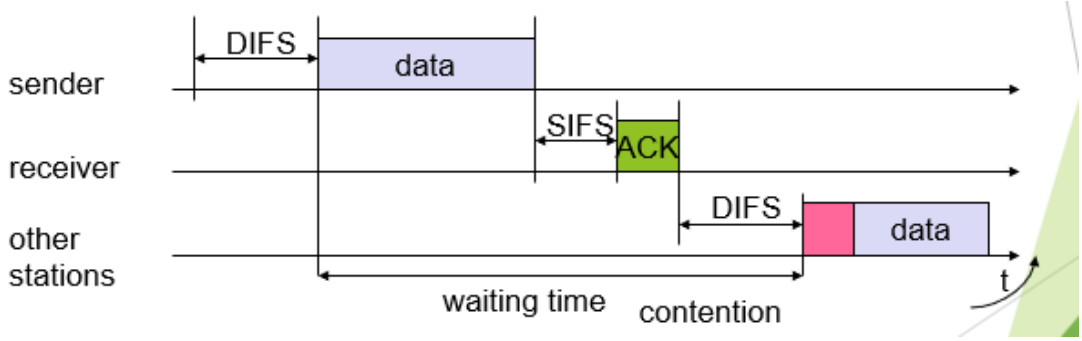
Method 1

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)



Method 2

- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors



Explain carrier sensing and different ways of carrier sensing in 802.11.

- **In IEEE 802.11, carrier sensing is performed**
  - at the air interface (*physical carrier sensing*), and

- at the MAC layer (*virtual carrier sensing*)

- **Physical carrier sensing**
  - detects presence of other users by analyzing all detected packets
  - Detects activity in the channel via relative signal strength from other sources
- **Virtual carrier sensing** is done by sending MPDU duration information in the header of RTS/CTS and data frames
  - Channel is busy if **either** mechanisms indicate it to be
  - Duration field indicates the amount of time (in microseconds) required to complete frame transmission
  - Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV)

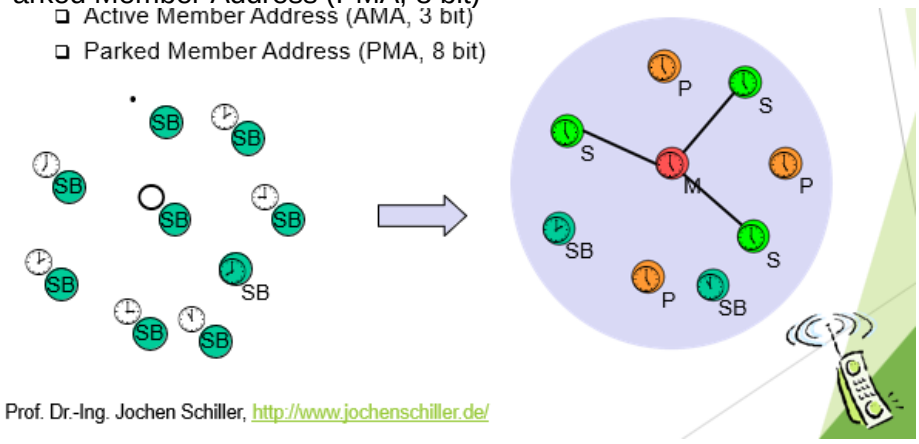
Explain the process of piconet formation.

All devices in a piconet hop together

- Master gives slaves its clock and device ID
  - Hopping pattern: determined by device ID (48 bit, unique worldwide)
  - Phase in hopping pattern determined by clock

Addressing

- Active Member Address (AMA, 3 bit)
- Parked Member Address (PMA, 8 bit)



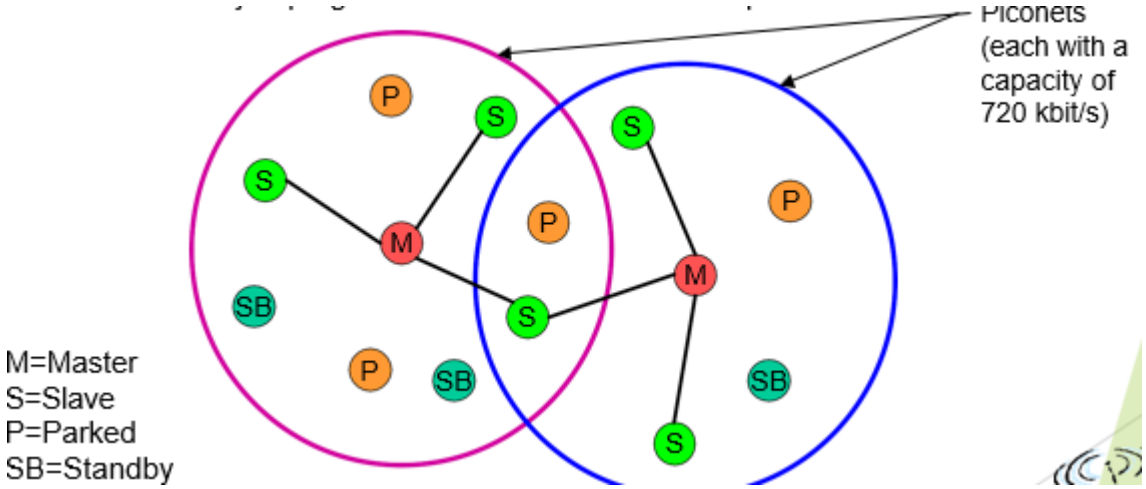
What is a scatternet?

Linking of multiple co-located piconets through the sharing of common master or slave devices

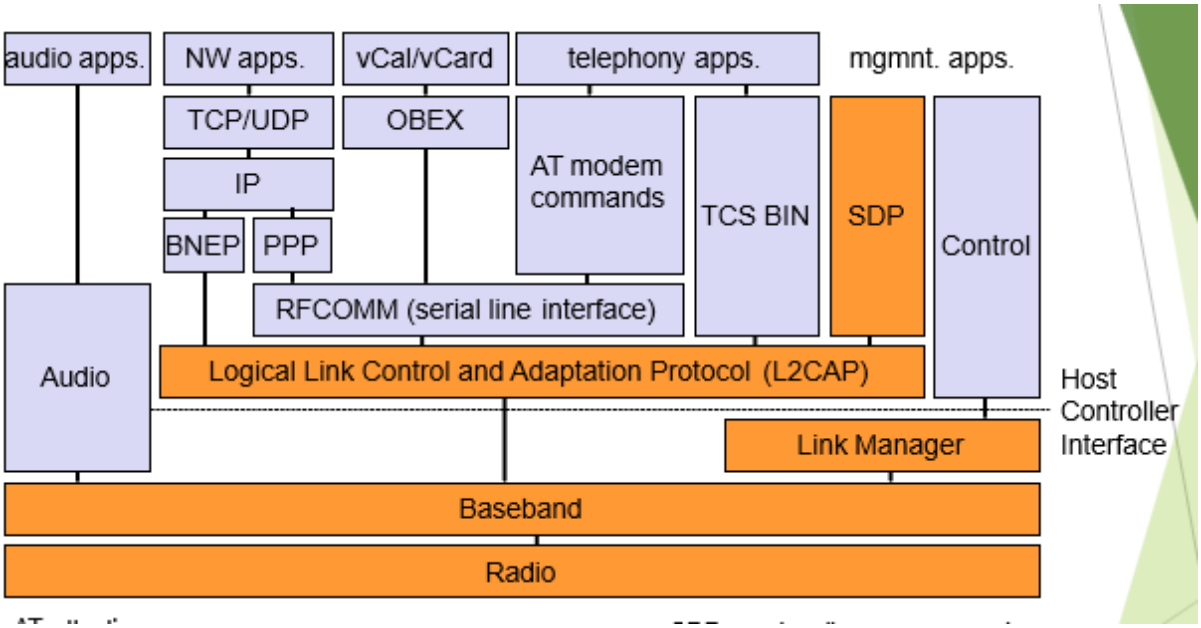
- Devices can be slave in one piconet and master of another

Communication between piconets

- Devices jumping back and forth between the piconets



Explain Bluetooth protocol stack.



- Radio: Specification of the air interface, i.e., frequencies, modulation, and transmit power
- Baseband: Description of basic connection establishment, packet formats, timing, and basic QoS parameters
- Link manager protocol: Link set-up and management between devices including security functions and parameter negotiation
- Logical link control and adaptation protocol (L2CAP): Adaptation of higher layers to the baseband (connectionless and connection-oriented services,
- Service discovery protocol: Device discovery in close proximity plus querying of service characteristics
- Cable replacement protocol RFCOMM that emulates a serial line interface following the EIA-232 (formerly RS-232) standards. RFCOMM supports multiple serial ports over a single physical channel.
- The telephony control protocol specification – binary (TCS BIN) describes a bit-oriented protocol that defines call control signaling for the establishment of voice and data calls

between Bluetooth devices. It also describes mobility and group management functions. The host controller interface (HCI) between the baseband and L2CAP provides a command interface to the baseband controller and link manager, and access to the hardware status and control registers. The HCI can be seen as the hardware/software boundary.

What are low power states of Bluetooth?

- Sniff state: The sniff state has the highest power consumption of the low power states. Here, the device listens to the piconet at a reduced rate (not on every other slot as is the case in the active state).
- Hold state: The device does not release its AMA . If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet.

Compare Bluetooth and ZigBee

Bluetooth	Zigbee
▶ **Bluetooth** was developed under IEEE 802.15.1, which is used for providing wireless communication through radio signals. The frequency range supported in Bluetooth varies from 2.4 GHz to 2.483 GHz. It covers less distance than Zigbee. In Bluetooth, GFSK modulation technique is used. ▶ Bluetooth networks can be built using the point-to-point master-slave approach in which there is one master and up to seven slaves form a piconet, which leads to forming a scatter net which is a linking of two or more piconets.	▶ **Zigbee**, BPSK and QPSK modulation techniques are used like UWB (Ultra-Wide Band). the frequency range supported in Zigbee is mostly 2.4 GHz worldwide, which means 2.4 GHz is not supported at all times. It covers more distance as compared with Bluetooth. ▶ Zigbee devices can be networked in a variety of generic topologies, including a star, mesh, and others. A cluster can be created by connecting different Zigbee-based network topologies. Zigbee Coordinator, Zigbee Router, and Zigbee Endpoint nodes make up any Zigbee network.

What is ZigBee?

- Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.
- Zigbee is for low-data rate, low-power applications and is an open standard.
- Zigbee products have been extended and customized by vendors and, thus, plagued by interoperability issues.