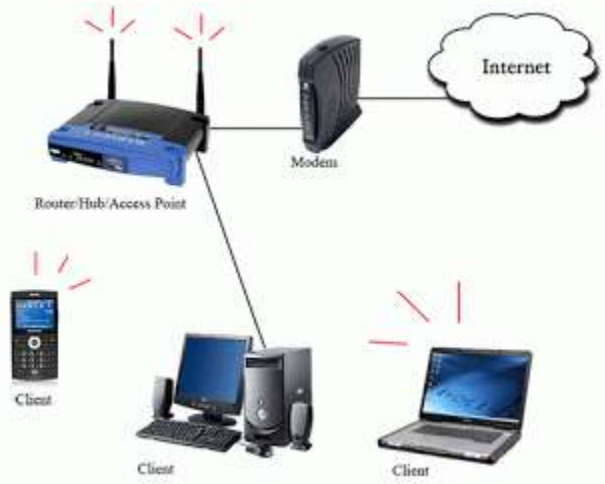
Wireless notes

We know about wired (LAN) and wireless (WLANs) networks.Whats the main difference between them ? Wired networks are connected to each other using wires and here in wireless networks we don‟t use cables but we are using radio waves to transmit out data



Unlike a wired network which operates at full-duplex (send and receive at the same time), **a wireless network operates at half-duplex**(send or receive at a time)We can get collisions if we use wireless networks but it's rather hard to detect whether there have been 2 wireless signals that bumped into each other somewhere in the air.We know LAN use CSMA/CD (Carrier Sense Mutli Access/Collision Detection).But here in wireless network its impossible to detect collision if it happen.So wireless LAN use **CSMA/CA (Carrier Sense Multi Access / Collision Avoidance).**CSMA/CA Algorithmassign specific time slots for each clients attached to the network.Wlans use RF (Radio Frequency) waves to communicate.A WAP (wireless access point) broadcast RF signals to air and clients use same frequency to communicate.

So what are the main issues we come across in wireless networks ?

1. **Coverage:** We need to place access point at a place where all your clients get proper signals Different materials will affect on your signal.
2. **Interference:** There are many devices working on 2.4 and 5Ghz frequencies that you will get interference which will weaken your signal quality.
3. **Privacy:** Our data "flies around in the air" which means we have no way of securing our physical layer, we need to make sure we have strong authentication and encryption.
4. **Regulations:** There are restrictions in using wireless spectrum in all countries.. You are not allowed to transmit on any given frequency you like. The **International Telecommunication Union-Radio communication Sector (ITU-R)** has determined a couple of frequencies we can use for our wireless networks.

These frequency bands are called the **ISM band which stands for Industrial, Scientific and**

Medical. Everyone can use these frequencies without the requirement of getting a license.That‟s also the downside since everyone is using them you are likely to get interference.

The ISM band has the following frequencies

1. **902-928MHz:** We don‟t use this low frequency for our Wi-Fi equipment.
2. **2.4-2.4835 GHz:** This is a frequency we use for 802.11b, 802.11g and 802.11n
3. **5 GHz:** There are a couple of frequencies on the 5 GHz band we can use, 802.11a and 802.11n operate here.

Below are the main three factors effecting our wireless networks

Reflection is when your wireless signal bounces off the material. Metal is a very good
example of this. It‟s very hard to get your wireless signal through a metal ceiling or elevator since the signal just bounces off. So now you know why you cant get wi-fi in your elivator.right ?

Scattering means your wireless signal hits a surface and “breaks” apart in multiple pieces leaving the original signal far weaker.

Absorption happens when material absorbs our wireless signal. Examples of absorption are water and the human body…absorption is terrible for your wireless signal since there‟s not much left after passing through this material!

What standards do we have? There‟s 802.11a, 802.11b, 802.11g and 802.11n. What are
the differences? First let me show you this table:

Security in WireLess Networks

Security of our data have to take care of well while using wireless network.Its hard to protect data in in WLANs than Lan network.Basic three security measures we use in WLANs are

- **Filtering MAC addresses.**
- **Hiding your SSID (name of the network).**

- **Enabling WEP encryption.**

All of above methods are not much secure.A hacker or intruder can easly break into your WLAN network in a very short period of time.
First of all filtering MAC addresses doesn‟t add anything to security since MAC addresses are always sent in **clear text**.
Hiding the SSID (name of your network) is also nonsense since there are 3 frame types
where you will find the SSID:

- Beacon: Your wireless access point will send beacons, broadcasting it‟s SSID and other information like data rates.
- Probe request and probe response: These are used when a client wants to connect to your wireless access point.

If you hide your SSID its only disabled in the beacon. It‟s still in the probe request andprobe response in clear-text ready to be sniffed by a wireless hacker. WEP encryption is unsafe. **WEP networks can be hacked in 5-10 minutes no matter if you use a 64,128 or 256-bit key.** The next protocol in line is WPA (version 1). WPA uses the same encryption (RC4) as WEP but a lot has changed to increase security. WEP uses static keys where WPA uses TKIP (Temporal Key Integrity Protocol) as the input for RC4.Since WEP and WPA both use RC4 encryption all old hardware that only supported WEP can be upgraded to use WPA but not WPA 2. **WPA 2** is completely redesigned. Instead of using the RC4 encryption algorithm it works by using AES. **AES is the most secure encryption algorithm up-to-date.**

There are 2 methods of using a key for WPA and WPA 2.

- **Preshared key:** This is what you probably use at home. You made up a key that‟s being used for your wireless encryption.
- **802.1x and EAP**: This is what you use for serious wifi setups since you can authenticate users.

Using a Preshared key is easy but you don‟t have any control. You don‟t know who has your key and it‟s easy to share it. It‟s also being saved in clear-text in your Windows registry. If you have a strong Preshared key it‟s impossible to break it

The most secure method is by using 802.1X also known as port-based control. This is something you can do for wireless but also for wired networks. The idea behind it is that users need to authenticate themselves before they get any access to the network. You don‟t even receive an IP address from the DHCP server…the only thing you are allowed to do is send authentication information.

Basic Terminologies

- **WiMAX** : Worldwide Interoperability for Microwave Access (WiMax) is defined by the WiMax forum and standardized by the IEEE 802.16 suite. The most current standard is 802.16e.
- **Basic Service Set (BSS) :** A group of stations that share an access point are said to be part of one BSS.
- **Extended Service Set (ESS) :** Some WLANs are large enough to require multiple access points. A group of access points connected to the same WLAN are known as an ESS. Within an ESS, a client can associate with any one of many access points that use the same Extended service set identifier (ESSID). That allows users to roam about an office without losing wireless connection.
- **Temporary Key Integrity Protocol (TKIP)** is a short-term solution that fixes all WEP weaknesses.
- **Counter Mode with CBC-MAC Protocol (CCMP)** is a new protocol . It uses AES as its cryptographic algorithm, and, since this is more CPU intensive than**RC4 (used in WEP and TKIP)**
- **802.1X :** Port-Based Network Access Control
- **WAP** : Wireless Access Points
- **AES :** AES stands for Advanced Encryption Standard and is a totally separate cipher system. It is a 128-bit, 192-bit, or 256-bit block cipher and is considered the gold standard of encryption systems today. Used in WPA2

- **EAP** : Extensible Authentication Protocol (EAP) [RFC 3748] is just the transport protocol optimized for authentication, not the authentication method

Make sure that you have prepared the answers for the below questions before your interview

- What is Wi-Fi?
- What is a Wi Fi Hotspot?
- What is IBSS,BSS and ESS ?
- Why WPA encryption is preferred over WEP?
- What is 802.1x and EAP ?
- Name two devices can interfere with the operation of a wireless network because they operate on similar frequencies?
- What are three basic parameters to configure on a wireless access point?
- What is the maximum data rate specified for IEEE 802.11b WLANs?
- Which encryption type does WPA2 uses ?
- When two laptops directly directed wirelessly,what type of topology has been created ?
- Which Spread spectrum technology does the 802.11b standard define for operation ?
- which two wireless encryption method are based on RC4 encryption algorithm ?
- which is the minimum parameter need on the access point inorder to allow a wireless client to operate on it ?
- What is the frequency range of the IEEE 802.11g standard?
- What is the maximum data rate for the 802.11a standard?
- What is the maximum data rate for the 802.11g standard?