Unit V: Wireless LAN: Wireless LAN Advantages – Wireless LAN Architecture –Mobility in Wireless LAN – Deploying Wireless LAN- Mobile Adhoc Networks and Sensor Networks – Wireless LAN security – Wireless Access in Vehicular Environment. Intelligent Networks and Interworking : Fundamentals of Call Processing – Intelligence in the Networks – SS#7 signaling - IN conceptual Model (INCM) – Softswitch – Programmable networks - Virtual Private Network (VPN).

CHAPTER 10

Wireless LAN

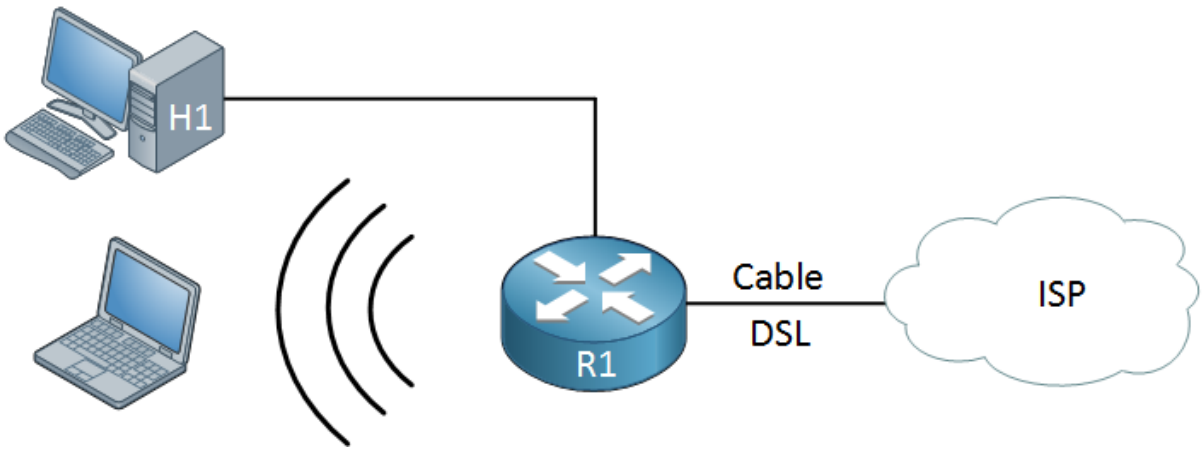
10.1 Introduction to Wireless LAN

About 10 years ago, most offices only had desktops and some other network devices like printers. All of these were connected with wires. Today, a lot of users have a laptop, smartphone, and tablet. That's three wireless devices for each user. Wireless speeds have increased significantly, getting close to wireless Gigabit.

IEEE uses 802.11 for all protocols that are related to wireless. Most of us have seen or heard about 802.11a, 802.11b, 802.11g, 802.11n and/or 802.11ac before. We also have the Wi-Fi Alliance that helps with the promotion of wireless networking. For example, IEEE has described authentication and encryption in their 802.11i standard. The Wi-Fi alliance has based WEP, WPA, and WPA2 on this standard. These names are easier to work with than referring to 802.11i.

SOHO Wireless LAN

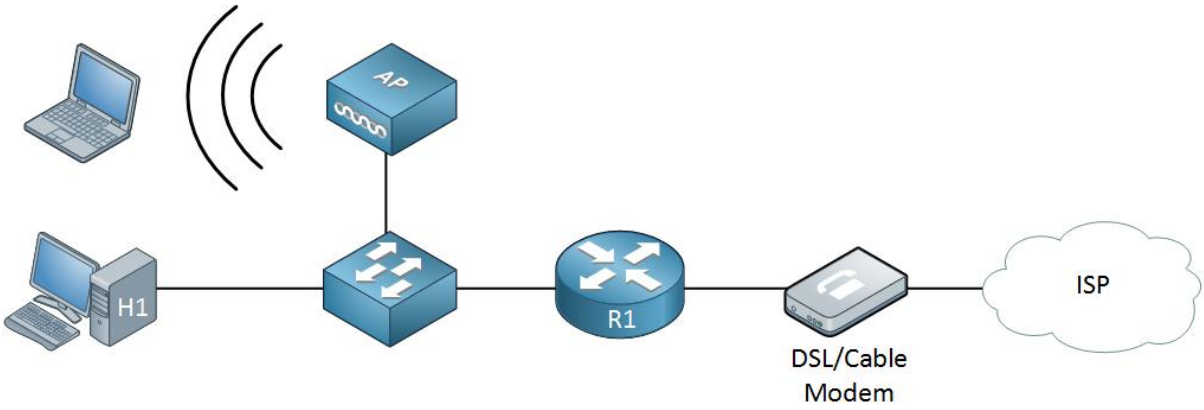
Your router at home probably has the same capabilities as the one below:



It is connected to your ISP through cable or DSL, or perhaps fiber. It has some Ethernet ports to connect your computers and it has antennas for wireless users. In reality, these components are all built into one device:

- Ethernet Switch
- Wireless Access Point
- (Cable or DSL Modem)
- Router

If you take everything apart, it looks like this:



In small networks like this, the AP does everything by itself. We call this an autonomous access point. It uses 802.11 protocols to talk with the wireless clients and uses Ethernet on the LAN side.

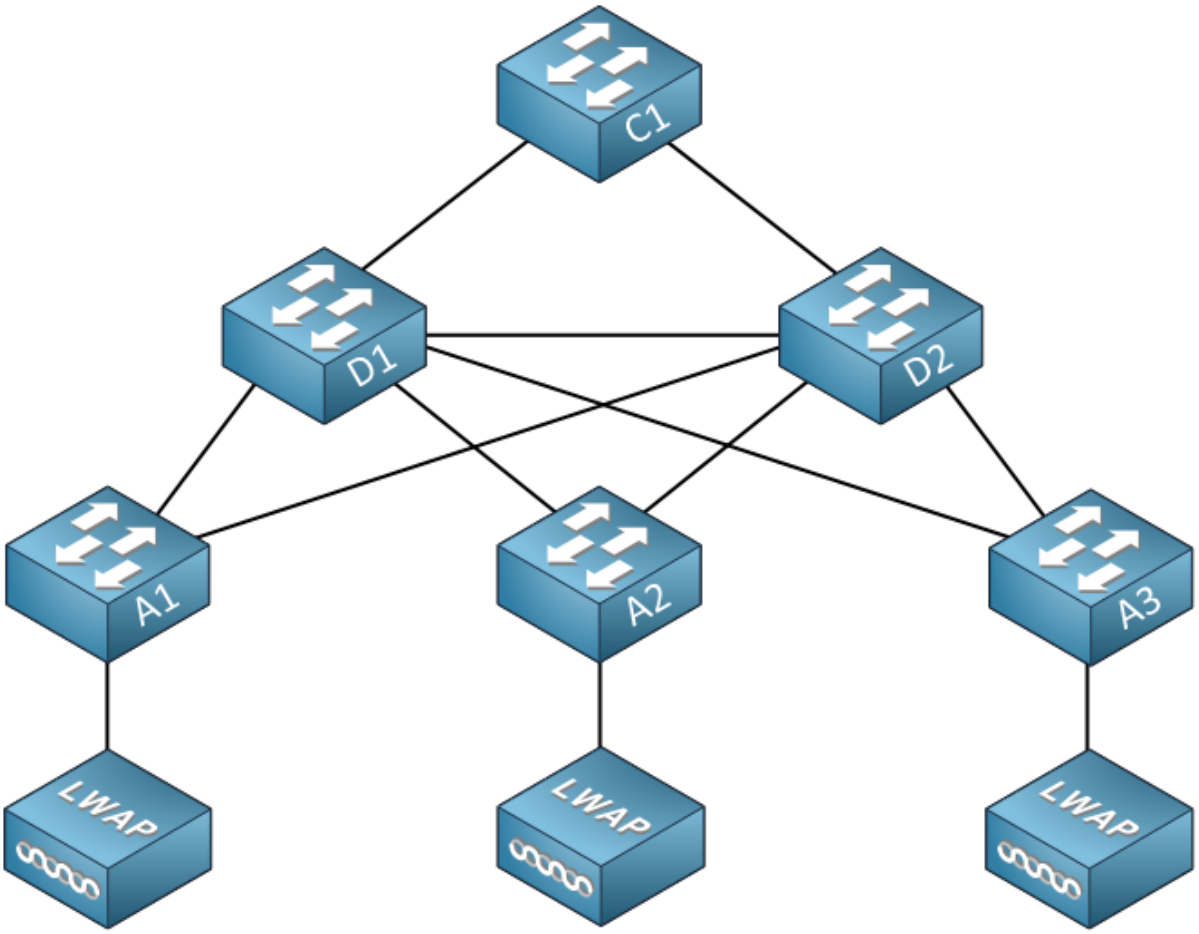
Enterprise Wireless LAN

When we look at large Enterprise networks, a single access point is not enough. Imagine a network with hundreds or thousands of users. When you walk around the office, you don't want to get disconnected every time when your phone switches from one access point to another. You want to have a stable wireless connection, wherever you go. Switching seamlessly from one access point to another is called roaming.

A single access point also has limited bandwidth. If you have a meeting room with 100 users then a single access point might be unable to provide enough bandwidth for everyone.

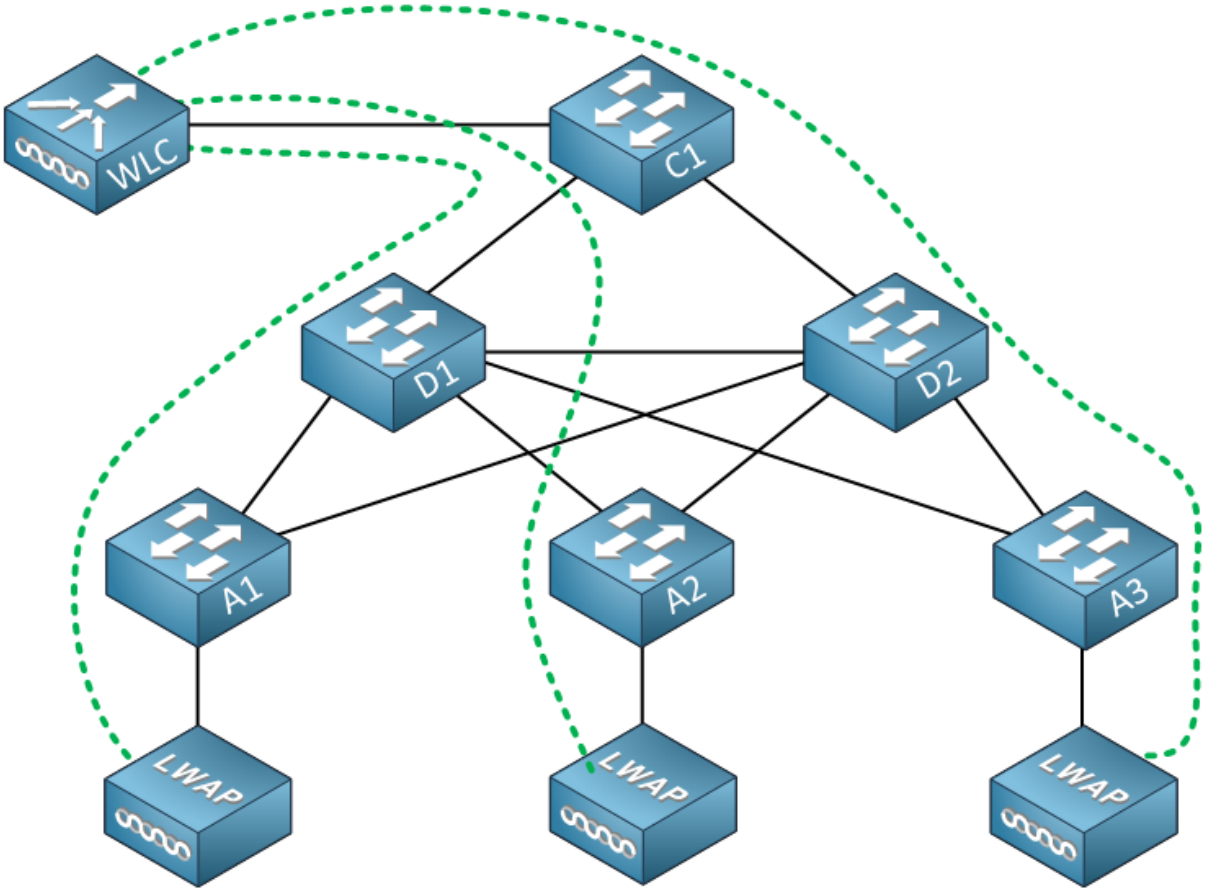
Since we use wireless networking for our users, it has to be close to our users. That's why you will find access points on the access layer of your network, just like your computers and

printers:



There's still one issue. Let's say you are connected to an access point and you start walking around the office, your phone will switch to another access point. How does this second access point know that you are already authenticated to the network? You could re-authenticate but that will break your connection…not a good idea. With autonomous access points, roaming could be difficult. To guarantee seamless roaming, the access points need to exchange authentication information of a client that roams from one access point to another.

Nowadays, most wireless networks use a wireless LAN controller:



All management tasks are moved from the access points to the wireless LAN controller. It takes care of authentication, roaming, creating new wireless networks, etc. The access points are only responsible for forwarding traffic, we call these LWAPs (Light Weight Access Point).

To achieve this, all traffic has to be sent from the access points to the wireless LAN controller. This is done by tunnels called CAPWAP (Control And Provisioning of Wireless Access Points). The green dotted lines are the CAPWAP tunnels between the APs and WLC.

We now have one big wireless network. If you create a new wireless network (SSID) then it will be pushed to all access points. Roaming is also no problem since all traffic is forwarded to the WLC.

10.2 WirelessLAN Architecture :

Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

1) Stations (STA) − Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

- Wireless Access Pointz (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- Client. − Clients are workstations, computers, laptops, printers, smartphones, etc.

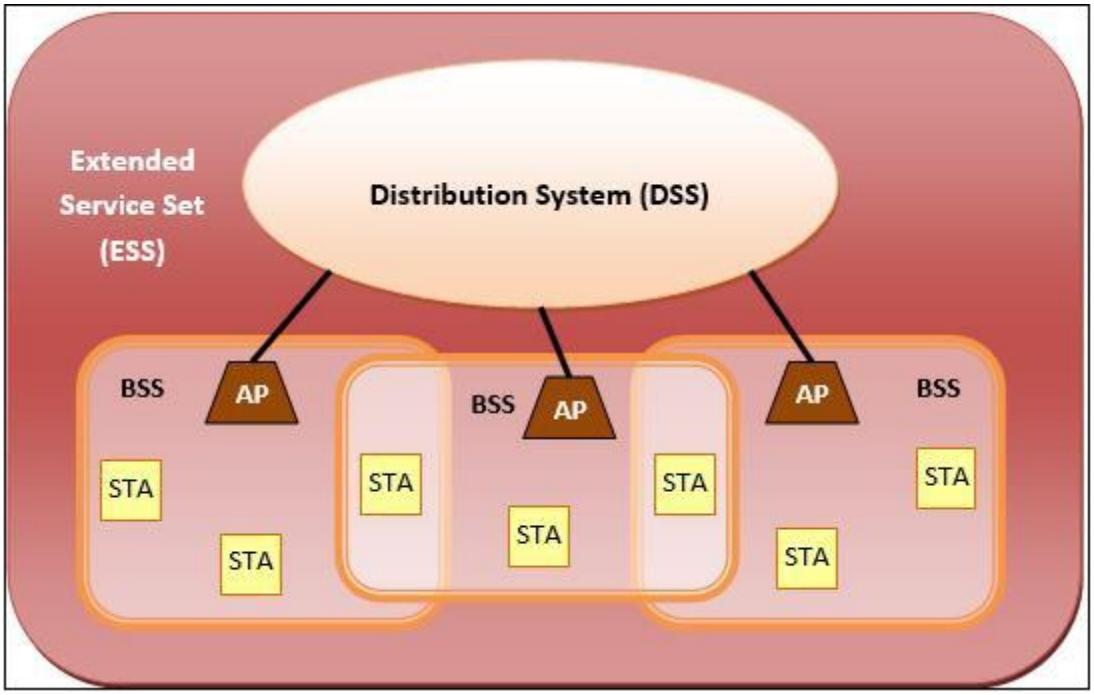
Each station has a wireless network interface controller.

2) Basic Service Set (BSS) −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

- Infrastructure BSS − Here, the devices communicate with other devices through access points.
- Independent BSS − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS) − It is a set of all connected BSS.

4) Distribution System (DS) − It connects access points in ESS.



WIRELESS LAN- Architecture elements

An 802.11 LAN is based on a cellular architecture where the system is divided

- into cells called basic Service set (BSS) and each cell is Controlled by a base
- station called Access point (AP).
- The WLAN can be formed by a single cell or several cells, where the access points
- are connected through some kind of backbone called distribution system (DS)
- typically Ethernet.
- The whole interconnected WLAN including different cells, their access points and
- the distribution system is seen to upper layers of OSI model as a single 802
- network and it is called in the standard as Extended service set (ESS).
- ESS is a set of BSSs interconnected by a distribution system (DS)
- The standard defines the concept of portal, a portal is a device that interconnects
- between 802.11 and another 802 LAN

Advantages and Disadvantages of WLAN

Advantages of wireless local area network (WLAN) :

- It's a reliable sort of communication.
- As WLAN reduces physical wires so it's a versatile way of communication.
- WLAN also reduces the value of ownership.
- It's easier to feature or remove workstation.
- It provides high rate thanks to small area coverage.

- You'll also move workstation while maintaining the connectivity.
- For propagation, the sunshine of sight isn't required.

- The direction of connectivity are often anywhere i.e. you'll connect devices in any direction unless it's within the range of access point.
- Easy installation and you would like don't need extra cables for installation.
- WLAN are often useful in disasters situation e.g. earthquake and fire. A wireless network can connect people in any disaster
- It's economical due to the tiny area access.
- The amount of power it requires is more as it uses transmitter; therefore, the battery life of laptops can be affected

Disadvantages :

- WLAN requires license.
- It's a limited area to hide.
- Mobility in Wireless LAN

The Government agencies can control the flow of signals of WLAN and can also limit it if required. this will affect data transfer from connected devices to the web.

10.3 Mobility Management

With the convergence of the Internet and wireless mobile communications and with the rapid growth in the number of mobile subscribers, mobility management emerges as one of the most important and challenging problems for wireless mobile communication over the Internet. Mobility management enables the serving networks to locate a mobile subscriber's point of attachment for delivering data packets (i.e. location management), and maintain a mobile subscriber's connection as it continues to change its point of attachment (i.e. handoff management). The issues and functionalities of these activities are discussed in this section.

Location management

Location management enables the networks to track the locations of mobile nodes. Location management has two major sub-tasks: (i) location registration, and (ii) call delivery or paging. In location registration procedure, the mobile node periodically sends

specific signals to inform the network of its current location so that the location database is kept updated. The call delivery procedure is invoked after the completion of the location registration.

Based on the information that has been registered in the network during the location registration, the call delivery procedure queries the network about the exact location of the mobile device so that a call may be delivered successfully.

The design of a location management scheme must address the following issues: (i) minimization of signaling overhead and latency in the service delivery, (ii) meeting the guaranteed quality of service (QoS) of applications, and (iii) in a fully overlapping area where several wireless networks co-exist, an efficient and robust algorithm must be designed so as to select the network through which a mobile device should perform registration, deciding on where and how frequently the location information should be stored, and how to determine the exact location of a mobile device within a specific time frame.

Handoff management

Handoff management is the process by which a mobile node keeps its connection active when it moves from one access point to another. There are three stages in a handoff process. First, the initiation of handoff is triggered by either the mobile device, or a network agent, or the changing network conditions. The second stage is for a new connection generation, where the network must find new resources for the handoff connection and perform any additional routing operations. Finally, data-flow control needs to maintain the delivery of the data from the old connection path to the new connection path according to the agreed-upon QoS guarantees.

Depending on the movement of the mobile device, it may undergo various types of handoff. In a broad sense, handoffs may be of two types: (i) intra-system handoff (horizontal handoff) and (ii) inter-system handoff (vertical handoff). Handoffs in homogeneous networks are referred to as intra-system handoffs. This type of handoff occurs when the signal strength of the serving BS goes below a certain threshold value.

An inter-system handoff between heterogeneous networks may arise in the following scenarios (Mohanty, 2006) - (i) when a user moves out of the serving network and enters an overlying network, (ii) when a user connected to a network chooses to handoff to an underlying or overlaid network for his/her service requirements, (iii) when the overall load on the network is required to be distributed among different systems.

The design of handoff management techniques in all-IP based next-generation wireless networks must address the following issues: (i) signaling overhead and power requirement for processing handoff messages should be minimized, (ii) QoS guarantees must be made, (iii) network resources should be efficiently used, and (iv) the handoff mechanism should be scalable, reliable and robust.

Mobility management at different layers

A number of mobility management mechanisms in homogeneous networks have been presented and discussed in (Akyildiz et al., 1999). Mobility management in

heterogeneous networks is a much more complex issue and usually involves different layers of the TCP/IP protocol stack. Several mobility management protocols have been proposed in the literature for next-generation all-IP wireless networks. Depending on the layers of communication protocol they primarily use, these mechanisms can be classified into three categories – protocols at the networks layer, protocols at the link layer and the cross-layer protocols.

Network layer mobility protocols use messages at the IP layer, and are agnostic of the underlying wireless access technologies (Misra et al., 2002). Link layer mobility mechanisms provide mobility-related features in the underlying radio systems. Additional gateways are usually required to be deployed to handle the inter-operating issues when roaming across heterogeneous access networks. In link layer protocols, handoff signals are transmitted through wireless links, and therefore, these protocols are tightly-coupled with specific wireless technologies. Mobility supported at the link layer is also called access mobility or link layer mobility (Chiussi et al., 2002).

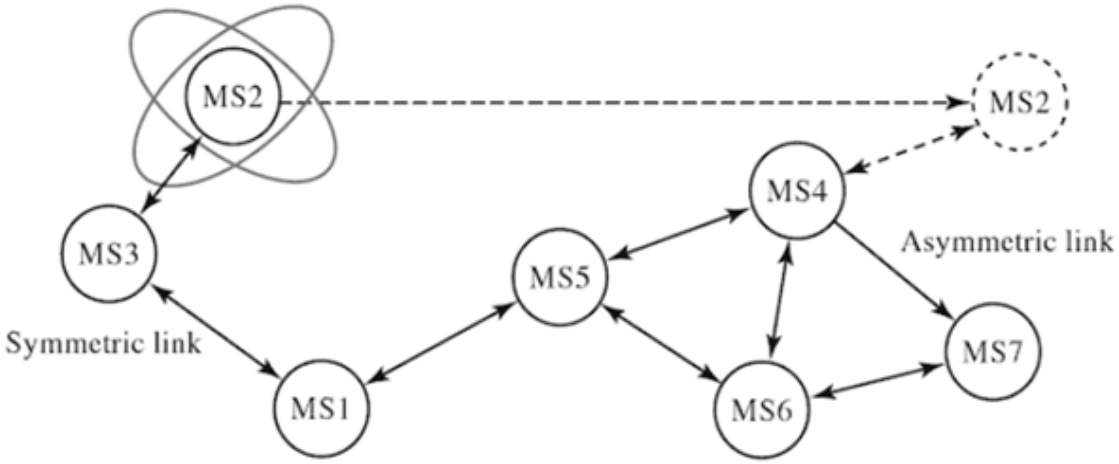
The cross-layer protocols are more common for handoff management. These protocols aim to achieve network layer handoff with the help of communication and signaling from the link layer. By receiving and analyzing, in advance, the signal strength reports and the information regarding the direction of movement of the mobile node from the link layer, the system gets ready for a network layer handoff so that packet loss is minimized and latency is reduced.

- If the amount of connected devices increases then data transfer rate decreases.
- WLAN uses frequency which may interfere with other devices which use frequency.
- If there's rain or thunder then communication may interfere.
- Due to Low security as attackers can get access to the transmitted data.
- Signals could also be suffering from the environment as compared to using fiber optics.
- The radiation of WLAN are often harmful to the environment.
- WLAN is more expensive than wires and hubs as it access points.
- Signals can get from nearest signals by access points.
- It's required to vary the network card and access point when standard changes.
- LAN cable remains required which acts because the backbone of the WLAN.
- Low data transfer rate than wired connection because WLAN uses frequency.
- Chances of errors are high.
- Communication isn't secure and may be accessed by unauthorized users.

10.4 Mobile Adhoc Network (MANET) :

- A MANET consists of a number of mobile devices that come together to form a network as needed, without any support from any existing internet infrastructure or any other kind of fixed stations.

- A MANET can be defined as an autonomous system of nodes or MSs(also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph.
- This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication between two mobile nodes relies on the wired backbone and fixed base stations.
- In a MANET, no such infrastructure exists and network topology may be changed dynamically in an unpredictable manner since nodes are free to move and each node has limiting transmitting power, restricting access to the node only in the neighboring range.
- MANETs are basically peer-to-peer, multi-hop wireless networks in which information packets are transmitted in a store and forward manner from a source to an arbitrary destination, via intermediate nodes as given in the figure:



- As nodes move, the connectivity may change based on relative locations of other nodes. The resulting change in the network topology known at the local level must be passed on to other nodes so that old topology information can be updated.

- For example, as MS2 in the figure changes its point of attachment from MS3 to MS4, other nodes that are part of the network should use this new route to forward packets to MS2. In the figure, we assume that it is not possible to have all nodes within each other's radio range. In case all nodes are closed by within each other's radio range, there are no routing issues to be addressed.

- In figures raise another issue, that of symmetric and asymmetric (bidirectional) and asymmetric (unidirectional) links. Consider symmetric links with associative radio range; for example, if MS1 is within radio range of MS3, then MS3 is also within radio range of MS1. The communication links are symmetric. This assumption is not

always valid because of differences in transmitting power levels and the terrain. Routing in asymmetric networks is relatively hard task. In certain cases, it is possible to find routes that exclude asymmetric links, since it is cumbersome to find the return path. The issue of efficient is one of the several challenges encountered in a MANET.

- The other issue is varying the mobility patterns of different nodes. Some other nodes are highly mobile, while others are primarily stationary. It is difficult to predict a node's movement and direction of movement and numerous studies have been performed to evaluate their performance using different simulators.

Characteristics of MANET

Some characteristics of adhoc network are as follows:

- Dynamic topologies: nodes are free to move arbitrarily; thus the network topology may be changed randomly and unpredictably and primarily consists of bidirectional links. In some cases where the transmission power of two nodes is different, a unidirectional link may exist.
- Bandwidth-constrained and variable capacity links: wireless links continue to have significantly lower capacity than infrastructure networks.
- Energy-constrained operation: some or all of the MSs in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes or devices, the most important system design optimization criteria may be energy conservation.
- Limited physical security: MANETs are generally more prone to physical security threats than wire line networks. The increased possibility of eavesdropping, spoofing, and denial of services (DoS) attacks should be considered carefully. To reduce security threats, many existing link security techniques are often applied within wireless networks.

Applications of MANET

Some specific applications of ad hoc networks include industrial and commercial applications involving cooperative mobile data exchange. There are many existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks, with many of these networks consist of highly dynamic autonomous topology segments. Advanced features of Mobile ad hoc networks, including data rates compatible with multimedia applications global roaming capability, and coordination with other network structures are enabling new applications.

- Defense applications: Many defense applications require on the fly communications set-up, and ad hoc/sensor networks are excellent candidates for use in battlefield management.

- Crisis management applications: These arise, for example, as a result of natural disasters in which the entire communication infrastructure is in disarray. Restoring communications quickly is essential.
- Telemedicine: The paramedic assisting the victim of a traffic accident in a remote location must access medical records (e.g. X-rays) and may need video conference assistance from a surgeon for an emergency intervention. In fact, the paramedic may need to instantaneously relay back to the hospital the victim's X-rays and other diagnostic tests from the site of the accident.
- Tele-geoprocessing application: The combination of GPS, GIS (Geographical Information Systems), and high-capacity wireless mobile systems enables a new type of application referred to as tele- geo processing.
- Virtual Navigation: A remote database contains the graphical representation of building, streets, and physical characteristics of a large metropolis. They may also "virtually" see the internal layout of buildings, including an emergency rescue plan, or find possible points of interest.
- Education via the internet: Educational opportunities available on the internet or remote areas because of the economic infeasibility of providing expensive last-mile wire line internet access in these areas to all subscribers.
- Vehicular area network: This a growing and very useful application of adhoc network in providing emergency services and other information. This is equally effective in both urban and rural setup. The basic and exchange necessary data that is beneficial in a given situation.

Wireless Sensor Networks :

Introduction :

Mobile wireless sensor networks (MWSNs) play a vital role in today's real world applications in which the sensor nodes are mobile. MWSNs are much more versatile than static WSNs as the sensor nodes can be deployed in any scenario and cope with rapid topology changes. Mobile sensor nodes consist of a microcontroller, various sensors (i.e., light, temperature, humidity, pressure, mobility, etc.), a radio transceiver, and that is powered by a battery .

The major applications of MWSNs are economics, environmental monitoring, mining, meteorology, seismic monitoring, acoustic detection, health care applications, process monitoring, infrastructure protection, context aware computing, undersea navigation, smart spaces, inventory tracking and tactical military surveillance . There are two sets of challenges to MWSNs; hardware and environment.

The main hardware constraints are limited battery power and low-cost requirements. i.e., the mobile sensor nodes should be energy efficient, low complexity algorithms required for microcontrollers and use of only a simplex radio . The mobility models to define the movements towards/away the sensor nodes, and how the mobile sensor nodes location, velocity and acceleration change over time, also predicts the future node positions.

Types of WSNs

Usually, the sensor nodes are deployed on land, underground and under water environments and that forms a WSN. Based on the sensor nodes deployment, a sensor network faces different challenges and constraints. Types of the WSNs are terrestrial, multimedia, underground, multi-media and mobile WSNs. In this chapter, we are discussing the overview of the mobile WSNs.

According to the resources of the sensor nodes on an MWSN, it can be classified into homogeneous and heterogeneous MWSNs [3]. Homogeneous MWSN consists of identical mobile sensor nodes and they may have unique properties. But, heterogeneous MWSN consists of a number of mobile sensor nodes with different abilities in node property such as battery power, memory size, computing power, sensing range, transmission range, and mobility, etc. Also, the nodes deployment of heterogeneous MWSN is more complex than homogeneous MWSN

Why are mobile nodes considered in WSNs?

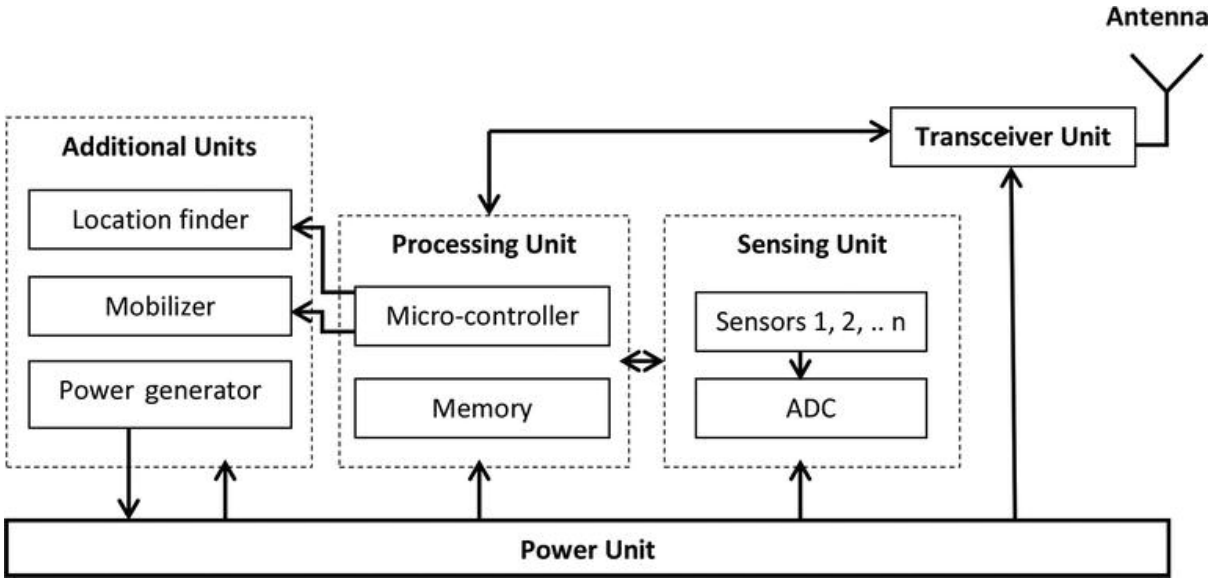
Kay Romer and FriedemannMattern investigated the design space of the wireless sensor networks and suggested many applications such as bird observation on great duck island, zebranet, cattle herding, bathymetry, glacier monitoring, cold chain management, ocean water monitoring, grape monitoring, power monitoring, rescue of avalanche victims, vital sign monitoring, tracking military vehicles, parts assembly, self-healing mine field, and sniper localization. Among 15 different applications, 10 applications are purely mobile and one of them is partially mobile. Therefore, mobile sensor nodes play an important role in humans real world applications

Mobile sensor node architecture

Usually, the sensor nodes are designed with one or more sensors (i.e., temperature, light, humidity, moisture, pressure, luminosity, proximity, etc.), microcontroller, external memory, radio transceiver, analog to digital converter (ADC), antenna and battery.

Again, the nodes are limited on-board storage, battery power, processing and radio capacity due to their small size . However, the mobile sensor node architecture is almost similar to the normal sensor node. But, some additional units are considered on mobile sensor nodes such as localization/position finders, mobilizer, and power generator..

The location or position finder unit is used to identify the position of the sensor node and the mobilizer provides mobility for a sensor node. The power generator unit is responsible to generate a power for fulfilling further energy requirements of the sensor node by applying any specific techniques such as the solar cell.



10.5 Wireless LAN security

- Wireless Network provides various comfort to end users but actually they are very complex in their working. There are many protocols and technologies working behind to provide a stable connection to users. Data packets traveling through wire provide a sense of security to users as data traveling through wire probably not heard by eavesdroppers.

- To secure the wireless connection, we should focus on the following areas –

- Identify endpoint of wireless network and end-users i.e., Authentication.
- Protecting wireless data packets from middleman i.e., Privacy.
- Keeping the wireless data packets intact i.e., Integrity.

We know that wireless clients form an association with Access Points (AP) and transmit data back and forth over the air. As long as all wireless devices follow 802.11 standards, they all coexist. But all wireless devices are not friendly and trustworthy, some rogue devices may

be a threat to wireless security. Rogue devices can steal our important data or can cause the unavailability of the network.

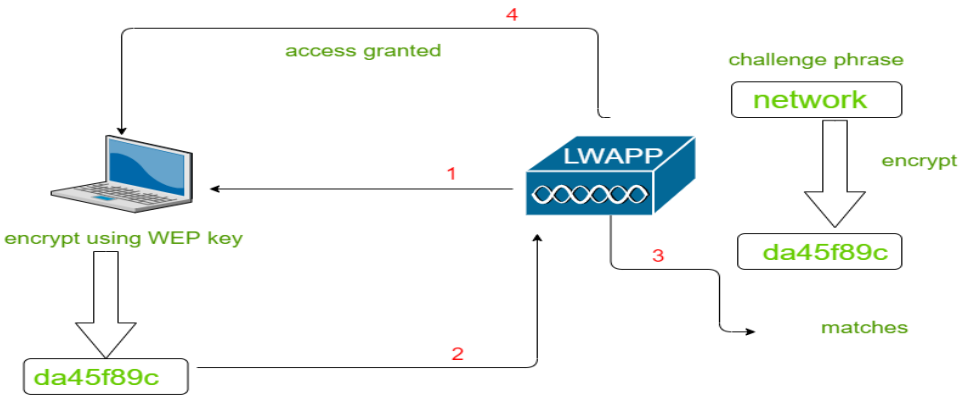
Wireless security is ensured by following methods-

- Authentication
- Privacy and Integrity
- In this article, we talk about Authentication. There are broadly two types of Authentication process: Wired Equivalent Privacy (WEP), and Extensible Authentication Protocol (802.1x/EAP).

These are explained as following below.

Wired Equivalent Privacy (WEP) :

- For wireless data transmitting over the air, open authentication provides no security.
- WEP uses the RC4 cipher algorithm for making every frame encrypted. The RC4 cipher also encrypts data at the sender side and decrypt data at the receiving site, using a string of bits as key called WEP key.
- WEP key can be used as an authentication method or encryption tool. A client can associate with AP only if it has the correct WEP key. AP tests the knowledge of the WEP key by using a challenge phrase. The client encrypts the phrase with his own key and send back to AP. AP compares the received encrypted frame with his own encrypted phrase. If both matches, access to the association is granted.



Working of WEP Authentication

Extensible Authentication Protocol (802.1x/EAP) :

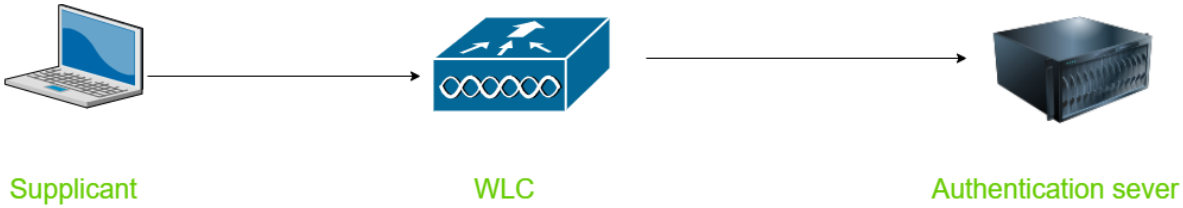
In WEP authentication, authentication of the wireless clients takes place locally at AP. But Scenario gets changed with 802.1x. A dedicated authentication server is added to the infrastructure. There is the participation of three devices –

.Authenticator –

Device that provides access to network usually a Wlan controller (WLC).

Authentication Server –

Device that takes client credentials and deny or grant access.



EAP is further of four types with some amendments over each other –

- LEAP
- EAP-FAST
- PEAP
- EAP-TLS

CHAPTER 11

Intelligent Networks and Interworking

11.1 Call processing

A fundamental of mobile architecture is the ability to manage a connection when a device moves out of a cell tower's range. Therefore, understanding mobile architecture requires knowing how call transfer, routing, and back-end processing work.

The basics of call transfer

Initially, when cellular networks started, they used an architecture in which base stations were pretty dumb. They could receive and transmit radio signals, but all other activity was handled by an independent device called a base station controller (BSC), which evolved into a Radio Network Controller (RNC).

These devices had the smarts required to negotiate and monitor caller access to and among the network. Also, these controller devices knew all the base stations in the network. This enabled the controller to manage handing off a cellphone among base stations as the mobile

device goes in and out of range. Figure 1 below illustrates the essential principle behind call handoff management using a central Radio Network Controller.

Image

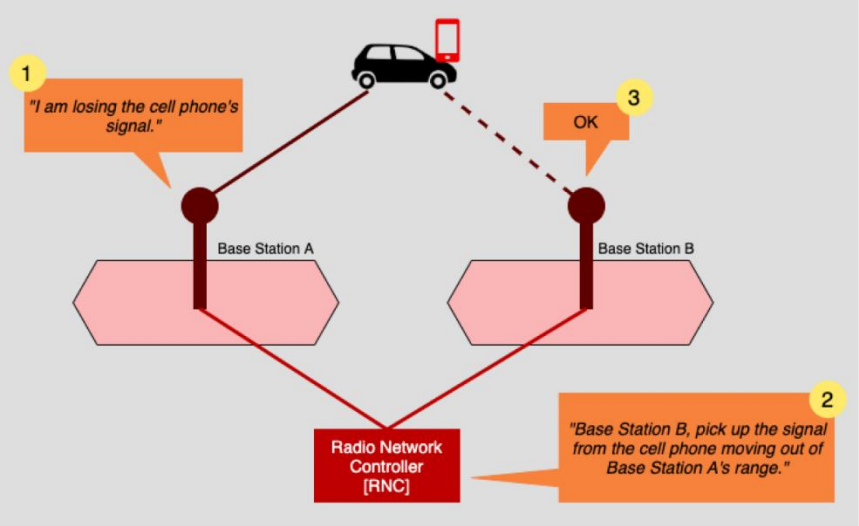


Figure 1: In earlier mobile networking architecture, the central RNC knew about all the base stations in the network and handed off calls accordingly. (Bob Reselman, CC BY-SA 4.0)

Eventually, controlling call and user activity moved directly onto the base station with the release of 4G LTE technology. Thus, a base station became aware of the other base stations in its vicinity. This effectively put handoff activity under the control of the base station.

Image

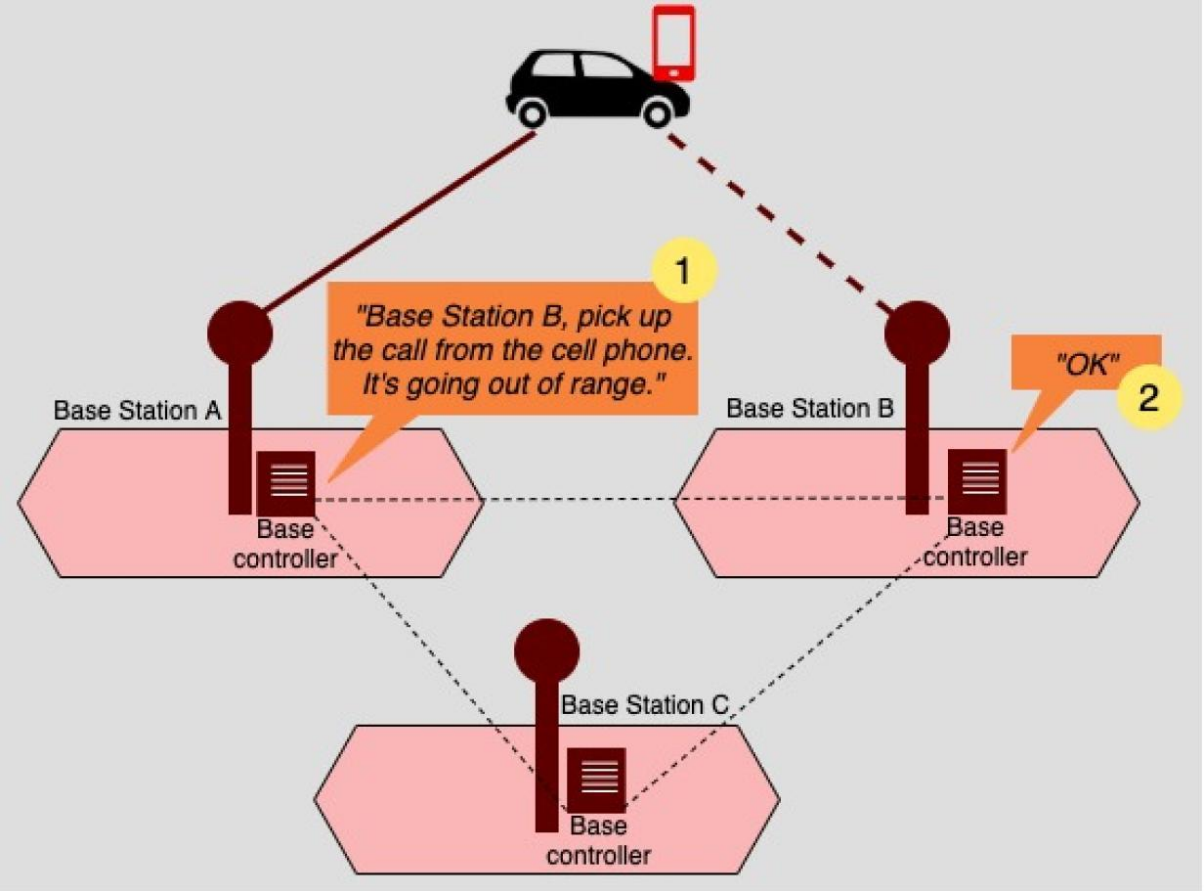


Figure 2: LTE technology pushes managing call handoff behavior down to the base stations. (Bob Reselman, CC BY-SA 4.0)

Transferring handoff activity from a central, all-knowing controller to individual base stations might seem like a minor point, but it's quite the opposite. Granted, from the user's point of view, nothing is really different. A caller can still make a call and travel about without any interruption in service. But, behind the scenes, a dramatic shift has occurred.

First, moving from a centrally controlled system to a decentralized system using Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) technology required a complete equipment overhaul. As Figure 2 above shows, each E-UTRAN-powered base station needs to have its own device to facilitate call management activities.

Moving to E-UTRAN was a significant undertaking in terms of technological transformation and financial cost. Given that there were nearly a quarter-million base stations in the United States in 2009, which is the year that introduced LTE technology, you can easily imagine that upgrade costs went into the tens of millions of dollars, if not more.

Understanding Control and User Plane Separation (CUPS)

Handoff management is only one aspect of the processing activity that takes place in a mobile computing architecture. Other vital elements are authenticating and connecting mobile

devices to the carrier network. Connecting to the carrier network's backend gives the caller access to the internet. In addition, connecting to the backend facilitates monitoring a customer's usage behavior, which, in turn, allows the carrier to bill the customer according to the monitored usage.

When you're exchanging information on your cellphone in the form of voice, text, or even listening to your favorite podcast, that interaction has two sets of functions. One set of functions is part of the user plane; the other is part of the control plane. This separation is formally called Control and User Plane Separation (CUPS).

User-plane functionality encompasses user behavior around the call such as signal handoff activity. Control-plane functionality is about the operational specifics of the call, for example, giving your phone an IP address, recording the time and place of your location as you travel, and keeping track of the amount of data you're using.

In the early days of cellular communication, user- and control-plane activity was coordinated in a central location. This approach was an inefficient use of the network. For example, if the central server is far away from the mobile device, a lot of time can be wasted doing user-specific tasks, such as a call handoff. That user behavior is better handled closer to the user at the base station. This is the reason behind the separation inherent in CUPS.

Today, user-plane and control-plane functionality are separated. User-plane activity is executed as close to the user as possible, while control-plane behavior is executed back at central servers on the core network. Behaviorally, this means handoff behavior is handled in the user plane, while viewing your account activity on your carrier's website is what's reported from the control plane.

Image

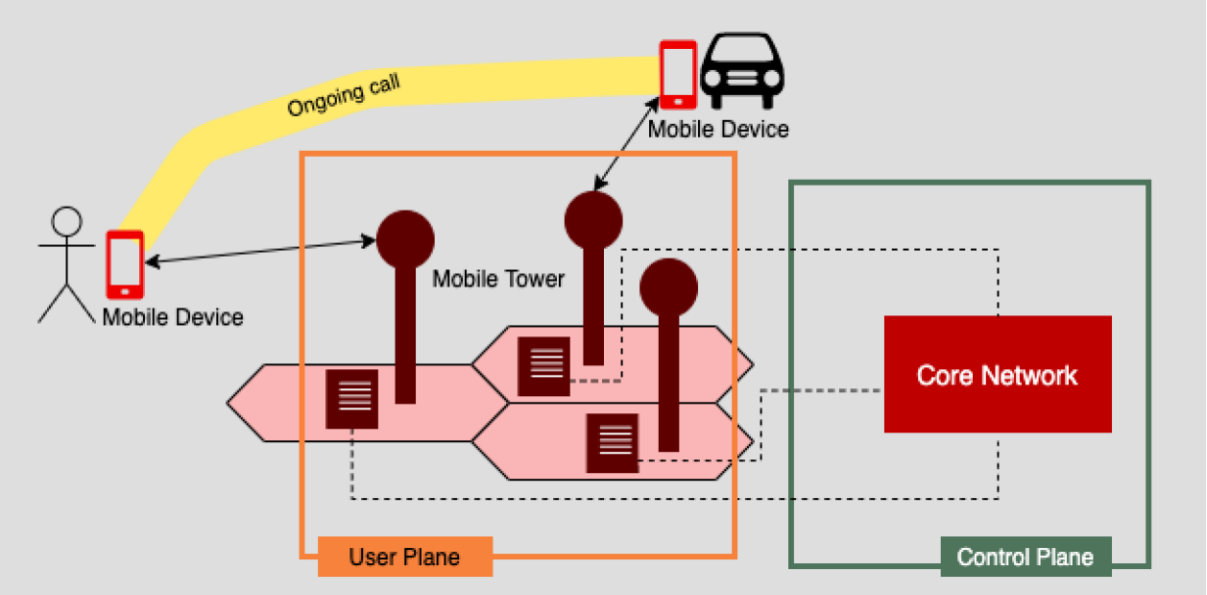


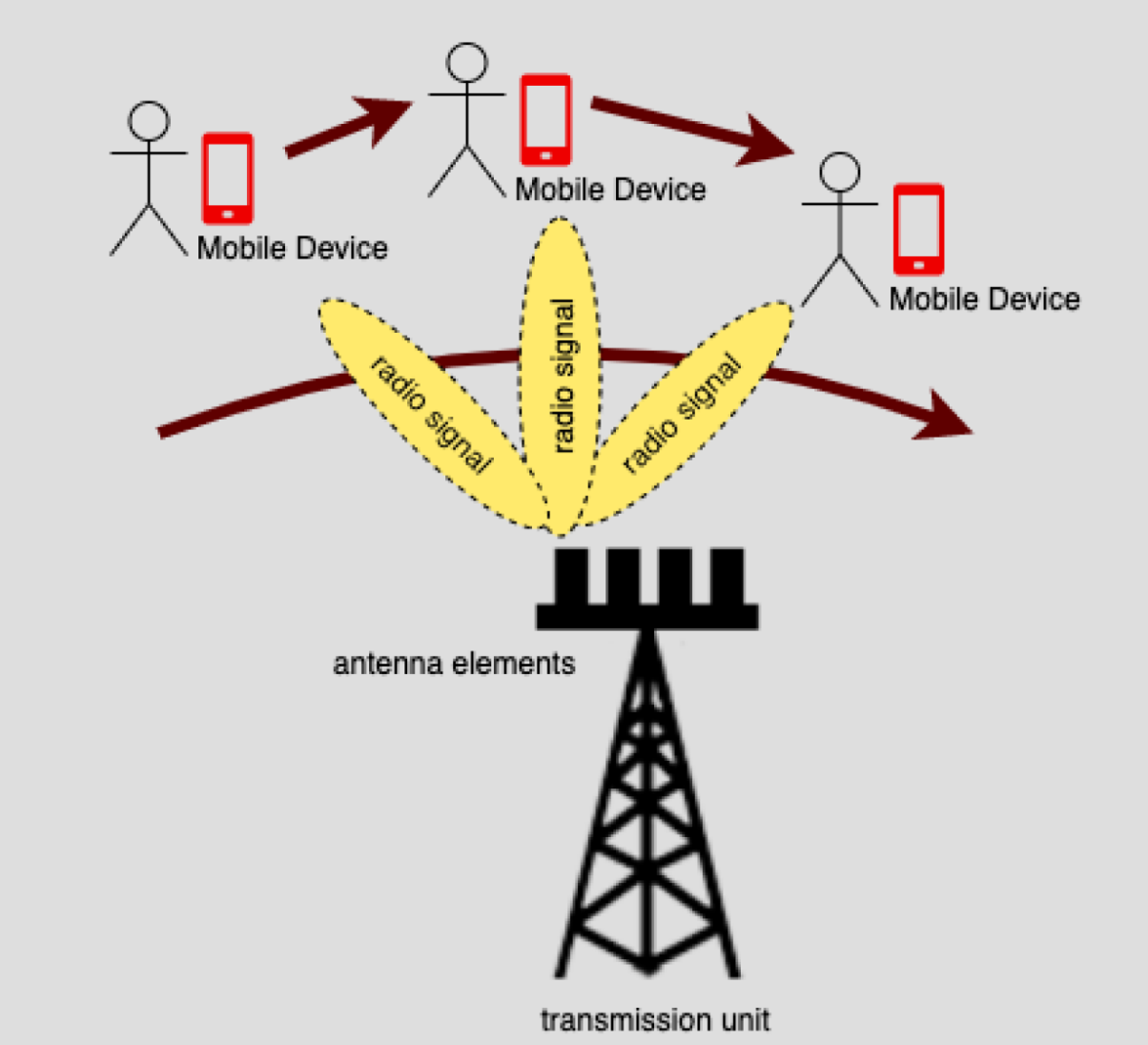
Figure 3: Separating the user plane from the control plane increases the efficiency of the mobile network. (Bob Reselman, CC-BY SA 4.0)
The important thing to understand about CUPS from an architectural perspective is that separating the user plane from control-plane activities increases network efficiency. Data only goes as far across the network as it has to, and overall performance increases.

CUPS plays a major role in decreasing the time a signal takes to get to a mobile device (lower latency) and increasing data throughput velocity on the network. In short, CUPS satisfies mobile customers' basic desire: getting more data at faster rates of exchange, which leads us to 5G.

Putting 5G into the mix: The need for speed

5G is the latest generation of technology on the cellular landscape. The motivating force driving its adoption is speed. Some of 5G's promises to mobile users are more data at faster rates, reduced latency for communication sessions, and better support for a high density of IoT devices in a particular physical location. More data at lower latency translates into 4K Ultra HD movies on your cellphone, higher fidelity in audio broadcasting, and fast access to data that changes in millisecond increments.

While there are an enormous number of technical details underlying 5G technology, at the most refined level, the way that 5G intends to satisfy the planet's ever-increasing need for speed is to push the frequencies that mobile carriers transmit signals higher up the frequency spectrum while also modifying the design of the physical architecture of mobile base stations.



5G beamforming enables wireless antennas to focus connections more directly toward mobile devices. A transmission tower or unit that implements beamforming has multiple radiating elements transmitting the same signal to a caller at an identical wavelength and phase in a reinforced manner.

The radiating element will steer the beam to follow a particular mobile device. When the device goes out of range, the signal is handed off, and beamforming continues to steer the new signal toward the mobile device of interest.

The important thing about 5G from an architectural perspective is that it will broaden the scope of cellular activity, particularly as 5G technology moves beyond cellphones and mobile tablets. The lower latency 5G offers is expected to make it an essential part of autonomous vehicle safety.

Also, the faster download times should enable edge computing devices to absorb a lot more data much more quickly, thus making them more independent of the network to do commonplace work. Imagine it taking only seconds for a doctor to download to a smartphone the gigabytes of current data and algorithms required for AI to do complex medical analysis. That doctor can then go into an area that's not connected to the internet or a wireless network and have that data and AI capability readily available to do the work of saving lives.

11.2 SS7

What is Signaling System Seven (SS7)

SS7 is a critical component of modern telecommunications systems. SS7 is a communications protocol that provides signaling and control for various network services and capabilities. Being a layered protocol, SS7 provides various protocol levels for connection oriented and connectionless (database) signaling in fixed and mobile networks.

- Transaction Capabilities Application Part (TCAP): TCAP is the portion of the SS7 protocol stack utilized for transport of the payload of other application processes
- ISDN User Part (ISUP): ISUP is a form of connection oriented signaling used for call set-up

While the Internet, wireless data, and related technologies have captured the attention of millions, many forget or do not realize the importance of SS7. Every call in every Public Switched Telecommunications Network (PSTN) system is dependent on SS7.

Likewise, every mobile phone user is dependent on SS7 to allow inter-network roaming. SS7 is also the "glue" that sticks together circuit switched (traditional) networks with packet-switched (IP based) networks.

Origins of SS7

Common Channel Signaling Network (CCSN) technology was introduced in the mid-1970s to improve trunk signaling (e.g.signaling for call set up involving inter-office facilities). Prior to CCSN, trunk signaling was performed via multi-frequency. After the introduction of CCSN, this form of signaling would be referred to as "in-band" signaling.

The early form of CCSN was known as Common Channel Signalingnumber Six (CCS6) and was used within the AT&T toll network for trunk signaling. It was also used by AT&T to provide great efficiency for their In-WATS (incoming Wide-Area Telephone Service) offering, the original version of toll-free calling, which at the time was available only to AT&T prior to portability of 800 numbers.

In the 1980s, a new CCSN protocol known as Signaling System number Seven (SS7), was developed and deployed. Telephone companies soon realized the advantages in SS7 that surpassed improvements in trunk signaling and it became the vehicle for signaling to databases and other platforms associated with enhanced services enabling the advent of intelligent networking. Variations of SS7 are now the standard through the world.

SS7 Network Elements
Networks elements involved in SS7 include the following examples:

- Service Control Point (SCP): SCPs are usually deployed in pairs. They are the brains of the SS7 network – where service logic resides
- Signal Transfer Point (STP): STPs are always deployed in pairs. They are the backbone of the SS7 network – routes signals to network nodes.
- Service Switching Point (SSP): By definition, an SSP is a switch that is intelligent network capable, meaning that they have software logic and triggering necessary to invoke SS7 messages based on events as well as respond to SS7 messages received to affect call control.

Inter-system Signaling

There are two major types of inter-system signaling for mobile/cellular database signaling: GSM Mobile Application Part (MAP) and ANSI-41. GSM MAP is the standard utilized for GSM and ANSI-41 is the inter-system standard for other mobile networks including CDMA. Both ANSI-41 and GSM MAP rely upon SS7 as a signaling protocol and both support intelligent network operations in terms of subscriber registration, roaming, and service profile portability.

Intelligent Network Standards for Cellular

The two recognized global standards for IN in mobile/cellular networks are Wireless Intelligent Network (WIN) and Customized Applications for Mobile Enhanced Logic (CAMEL). WIN and CAMEL are the standards used to provide network intelligence in ANSI-41 and GSM networks respectively. The two standards are similar in the sense that they achieve the same high-level technical and business goals. Both WIN and CAMEL rely upon SS7 as a signaling protocol.

Wireless Intelligent Network (WIN)
As WIN standards have been introduced, accepted and evolved, they have become part of the core ANSI-41 standards. In contrast, the GSM CAMEL Application Part (CAP) represents that portion of the GSM standard that uses CAMEL, and will remain a separate yet associated standard to the core GSM networking standard, GSM MAP.

WIN is based on an open industry standard that enables equipment from different suppliers to interoperate successfully, and allows automatic roaming between various networks. The WIN standard is part of the ANSI-41 family of standards, which allows additional capabilities to any existing ANSI-41-based network within an open vendor environment, to ensure full interoperability with third-party products and services.

11.3 Softswitch

What is Softswitch and How Does it Work

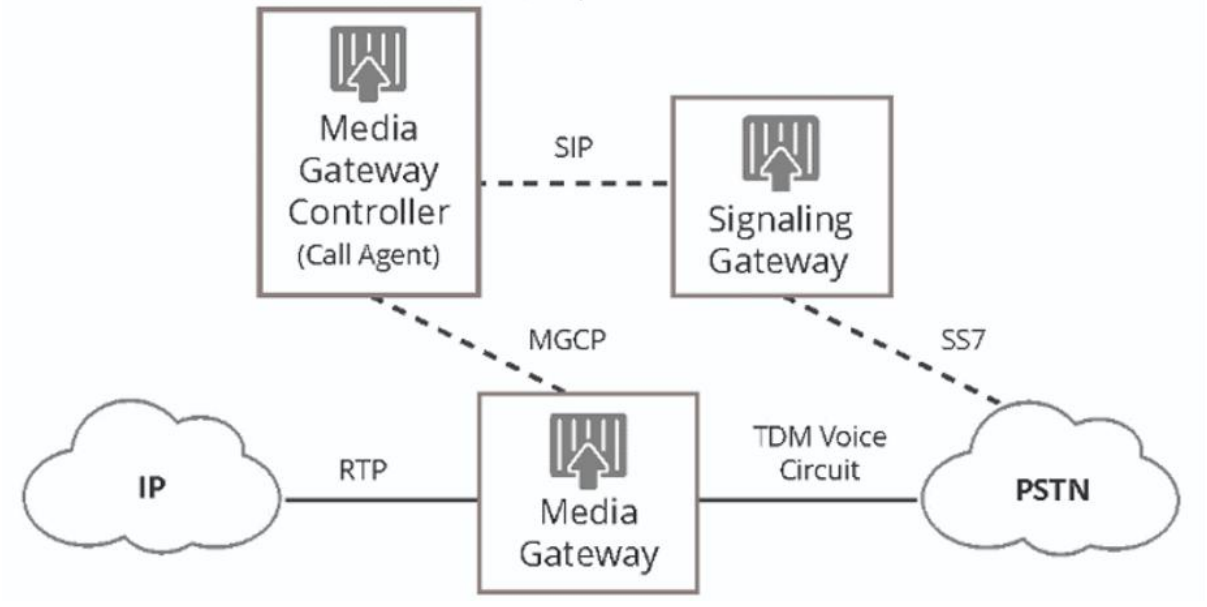
Switchboard operators, who initially routed telephone calls manually, replace automatic switchboards towards the end of the 1800s with the development of technology. Over the years, technology has progressed as follows; Strowger Switch and Crossbar Switch which use electromagnetic energy to open and close switches, single processor SPCs (Stored Program Control) to manage 10-100 calls per second, Digital Switches that transfer calls with WAN (Wide Area Network) and the latest VoIP Softswitch we use nowadays.

Softswitch (Software Switch) is a software-based telephone switchboard in a telecommunications network that is not based on the special switching hardware of a traditional telephone exchange but runs on a general-purpose computer platform. Shortly, it directs IP packets (VoIP) to reach their destination. This software has the potential to make incoming and outgoing calls over which infrastructure, line, or media gateway, to perform various operations on the phone numbers dialed, to direct emergency lines, and to support various platforms.

The most commonly used switches to route calls over different networks are Class 4 and Class 5 Softswitches.

Class 4 Softswitch ensures safe sound traffic over long distances. When a call is made, this switch chooses the most efficient route, delivering it to the recipient designated by the other party.

Class 5 Softswitch is there to reach the end-user in the system. Featuring call forwarding, conference calls, and voicemail, this switch also enables cost-effective scaling of voice services. The PBX system you choose to route voice traffic is also a Class 5 switch.



VoIP software switches provide coordination with other VoIP or PSTN software switches. A software key is needed to make a search, the software key starts by searching the recipient's IP address database. In the address database, it transmits to other software switches until the IP address of the recipient is found. The call is then transferred to the PSTN. Thanks to this transmission, we can hear the voices of our loved ones instantly.

11.4 Programmable networks

An abridged history of network programmability We'll provide a brief overview of the history of network programmability. A more detailed version of this history can be found elsewhere What's the simplest way to build a router that can take packets coming in on one port and send it to another port? Let's assume we are provided with a mechanism to receive packets on any given port and a mechanism to send packets on any given port.

This mechanism could concretely take the form of a peripheral that you can plug into your computer; your computer would then communicate with this peripheral to send and receive packets. Assuming the existence of this peripheral, how would you build a router? One simple solution is to take a general-purpose processor and implement the router's functionalities as a program on this general-purpose processor.

These functionalities include: 1. Running the routing protocol (e.g., link-state or distance-vector routing) to compute routing/forwarding tables for each router 2. Receiving packets 3. Looking up a packet's destination address in the routing/forwarding tables we just computed to find an output port for this packet 4. Sending the packet to that output port 5. Queueing the packet either at the input or output depending on whether the router is input/output queued 6. Dequeueing the packet from its queue and sending it

Software-defined networking

The first move towards a more programmable network in the era of hardware routers (by which we mean routers with data plane chips) was a movement that later came to be called software-defined networking (SDN). SDN has its roots in internet service provider networks such as AT&T's backbone network [8]. The need for a more programmable network arose from a desire to control the exact path taken by different packets that went beyond vanilla destination-address-based forwarding One example of policy routing is traffic engineering.

the ability to split traffic volume in some ratio across different paths in the network. Another example is to make sure one tenant's traffic does not cross over into the part of a network that belongs to a different tenant, a use case that is common in multi-tenant networks such as those found in cloud computing. The standard practice then was to somehow coerce a distributed routing protocol (such as a link-state or distance-vector routing protocol) to achieve these policy routing objectives using some unintuitive knobs in the routing protocol.

Programmable data planes Soon enough, people started noticing shortcomings with OpenFlow. OpenFlow was developed as the common minimum denominator across existing router functionality. In other words, OpenFlow did not add any new router functionality nor

did it provide a way to do so. All OpenFlow did (and this was a pretty big step forward) was to standardize an interface to existing router chips so that the route computation servers could communicate with different router chips in the same manner once these chips supported the OpenFlow standard. Put differently, the hardware within the data-plane chip was still rigid and fixed function. if you did not already have a particular feature in the data plane such as the ability to support different priorities for different traffic classes, you were still out of luck. One place where this need was felt was in the standardization of new protocol formats. The protocol format is a specification of which bits in the packet belong to which packet header, e.g., the first 48 bits of an Ethernet packet correspond to the Ethernet source MAC address header. Existing routers hardcoded the set of protocol formats and could not be tweaked to support a new protocol format that a network operator may have found useful.

11.5 Virtual Private Network (VPN)

An Introduction

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual “private network” i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

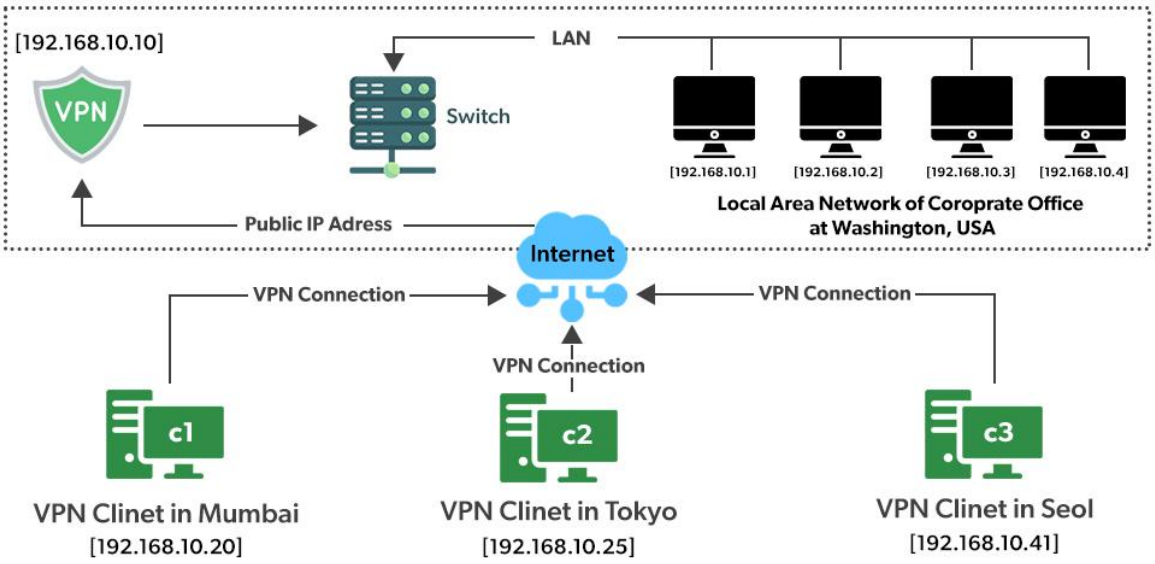
VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual “private network” i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).

The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.

Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.

So this is the intuitive way of extending the local network even across the geographical borders of the country.



Suppose the Ip address is 101.22.23.3 which belongs to India. That's why our device is not able to access the Spotify music app.

But the magic begins when we used the Psiphon app which is an android app and is used to change the device IP address to the IP address of the location we want(say US where Spotify works in a seamless manner).

The IP address is changed using VPN technology. Basically what happens is that your device will connect to a VPN server of the respective country that you have entered in your location textbox of the Psiphon app and now you will inherit a new IP from this server.

Now we typed "what is my IP address"? Amazingly the IP address changed to 45.79.66.125 which belongs to the USA And since Spotify works well in the US, so we can use it now being in India (virtually in the USA). Is not that good? obviously, it is very useful.

VPN also ensures security by providing an encrypted tunnel between client and VPN server.

VPN is used to bypass many blocked sites.

VPN facilitates Anonymous browsing by hiding your ip address.

Also, most appropriate Search engine optimization(SEO) is done by analyzing the data from VPN providers which provide country-wise stats of browsing a particular product. This method of SEO is used widely my many internet marketing managers to form new strategies.

VPN and its legality

Using VPN is legal in most of the countries,. The legality of using a VPN service depends on the country and its geopolitical relations with another country as well. A reliable and secure VPN is always legal if you are not intended to use it for any illegal activities like committing fraud online, cyber theft, or in some countries downloading copyrighted content.

China has decided to block all VPN(Virtual private network)s by next year, as per the report of Bloomberg. Many Chinese Internet users use VPNs to privately access websites that are blocked under China's so-called "great firewall". This is done to avoid any information leakage to rival countries and so as to tighten the information security.

This article is contributed by Shivam Shukla. If you like GeeksforGeeks and would like to contribute, you can also write an article using write.geeksforgeeks.org or mail your article to review-team@geeksforgeeks.org. See your article appearing on the GeeksforGeeks main page and help other Geeks.