* Wireless technology that uses radio waves to connect the Internet instead of using any cables
* Maximum speed: 54Mbps
* Can be used in mobile phones to connect to Internet.
* Using type ac can speed up to 3200Mbps
* Ranges can be interfered when there are factors like building designs, glass, irons and electronic devices along the network
* Cannot be limited in a precise area
* Can diffuse outside
* Can be prevented from being hacked by using passwords and encryption or by using secure networks like WPA2
* Has to provide internet for the whole organization
* There might be a bit latency in transferring data and downloading
* Can be connected in everywhere without non limitation
* Some cost around 25$ to 60$ per month
* Some cost around 75$ to $200 per month
* A wired technology using cables to connect with PCs, routers, LANs in order to connect the Internet
* Slightly faster than Wi-Fi
* 100Mbps to 1000Mbps
* More reliable than WIFI since it is plugged with only once PC for each person
* Signals doesn’t drop and performs with consistent speed when the PC is plugged with cable
* Provided for the authorized devices
* No interference and data loss due to being
* Provides the Internet for its plugged device
* Provides the Internet at the fastest speed
* No latency in data transferring or downloading
* Internet is provided only when the device is plugged with the port
* Can be connected according to the length of cable.
* According to the cable categories

For EFA, both Wi-Fi and cable are suitable. Wi-Fi should be applied in remote offices since they have to use tablets, smartphones and desktops etc. In the case of Wi-Fi, they should use type ac because it provides the network with the speed of 1000Mbps for around 1000ft. There might be a bit interference by signal drops but it can be solved by using routers. The security problems can also be solved by using encryption, passwords or pins.

Both cables and Wi-Fi should be applied in the central office since it stores staff data in database servers and uses web servers and email servers. In cables, they should use cat6a cable since it transfers data with the speed of 10Gbps and the bandwidth of 500Mhz so that data can be transferred quickly. Also, it uses copper wire which can lead to greater security. In Wi-Fi, they should use type ac as the remote offices do since they will also use tablets and network printers.

Therefore, both cables and Wi-Fi should be used in both central offices and remote offices.

* Used to connect computers along its network in order to communicate each other
* Comes with 4 to 12 ports.
* The data pass along the hub when the PC is connected to the hub with the cable
* Cannot read the address of the data’s destination
* Sends data to all ports at the same time
* Used in star topology
* Operates at Physical layer.
* Performs the same way as the hub
* Can read MAC address which is used to forward data to correct destination
* Comes with 24 to 48 ports
* Avoids collision along the network
* Used in star topology.
* Controls several data at the same time
* Locks down the network with firewall and authorization
* Operates at Data link layer.
* A hardware networking device used to connect Internet without wire
* Can connect to internet even while moving from one place to another
* Can be connected to internet for dozens of meters
* can connect one building to another
* Works at data link layer.
* Small electronic devices used to connect the network with wire or wireless
* Used to connect different devices (e.g.-phone to PC)
* Can read IP address to forward data to correct
* Provides network security like Firewall
* Operates at Network layer.

-Carries electrical impulses, light or radio signal through the mechanical or electrical level.

-Considers in the case of design such as voltage, connection setting, connection ending and connector requirements.

-Provides transformation of raw data into data that are errorless and passable through the network layer.

-Controls the rate of data between the sender and receiver.

-Divided into MAC layer and LLC layer.

-Provides addressing (IP address) and routing technologies to exchange data through the network.

-Compare differences in addressing, internetworking, error handling and message sizes.

-Deliver messages between the networks and prevents spiting of messages.

-Retransmit messages that are not accepted.

-Controls the flow of messages so that there is no data collision and data loss.

-Responsible for setting up, managing and terminating connections within the network hosts.

-Prevents data transmission at the same time.

-Identifies the translating program that are used by both users to communicate.

-Manages presenting, compression and encryption of the data.

-Transforms the data to a format that the application layer could read.

-Supports the end user services such as email, transferring files and virtual terminal access.

-Offers user interaction, privacy protection and quality certification and translating programs.

# 

This protocol works at application layer. It receives the email when it is sent to the Internet server and allow the users to save it in there for some time.

It works at the network layer. It sets up the network connection, determines the network address and delivers data to the correct receivers.

This protocol works at the transport layer. It enables the network connections to set up and exchange the data and also ensures the data will be delivered at the right time.

This protocol operates at application layer. It sends the mail through the network to a correct receiver or mail box by using “store and forward” process.

It operates at the presentation layer. It encrypts the data which are transmitted along the network and also authenticates the data recipients.

It operates at the application layer. It determines the style and transmission of messages and provide the users to get response from web browsers and servers in a standard way.

It works at the application layer and it is a secure version of HTTP. It is used in transmitting the data through the Internet between the web browser and user more securely than HTTP by using encryption method.

1. A network address is a main technology component in networking that assists in distinguishing a network node or device, that passes over a network. Network components need network addresses in order to define, locate and address other components. It is also distinctive for individual components.

* Distinguishes the Ethernet or network adapters and network interface over a network
* Physical address
* Permanent and cannot be changed
* 48 bits (6 bytes
* Works in data link layer
* NIC card’s manufacturer specifies MAC address
* Can be retrieved by ARP (Address resolution protocol)

* Defines the network hardware connected to a network and network nodes along the network
* Logical address
* Addresses can be changed based on the network
* 32 bits (4 bytes)
* Works in network layer
* Internet service providers
* specify IP address.
* Can be retrieved by RARP (Reverse address resolution protocol)
* Internet protocol version 4
* dotted quad formed
* 32-bit address
* Can’t establish end-to-end connection integrity
* Can’t perform packet-flow identification
* Doesn’t support encryption and authentication facilities.
* Security functions are available based on devices
* Internet protocol version 6
* separated by colons
* 128-bit address
* Can establish end-to-end connection integrity.
* Can perform packet-flow identification
* Supports encryption and authentication facilities
* Provides in-built IP security
* Connected to private network such as LAN
* Can be assigned to routers
* Deliver messages, save files and Print without the Internet
* LAN administrators specify private IP address.
* Unique in LAN
* No cost
* Provides different sets of address individually
* Connected to public Internet network
* Can be assigned to email server, web server or mobile devices and remote accesses
* Internet service providers/INA specifies public IP address
* Globally unique
* Paid version
* Provides same IP address for entire organization

EFA manages all services are managed from Central Office. As private IP address has different sets of address individually, it will limit the users accessing into the important devices. Also, it can continue messaging, file saving and printing without the Internet so that it can reduce a lot of cost. Moreover, it will serve authorization since it limits the users accessing in to the network. Therefore, EFA should use private IPv4 address in Central office.

Staffs and learners in EFA have to use lots of mobile devices that have to use to communicate along the network. Using public IPv4 address, staffs and learners in EFA can access to email servers, web servers and mobile devices. Also, since it provides remote access, the devices can be controlled by Central office. Therefore, public IP address should be used among the staffs, learners and volunteers in remote office.

Class A - 10.0.0.0 to 10.255.255.255

Class B - 172.16.0.0 to 172.31.255.255

Class C – 192.168.0.0

1. DHCP (Dynamic host configuration protocol) is a protocol that distinguishes the IP address, IP host, default gateways and subnet masks automatically.

In central office, DHCP should be used in email servers, web servers since it finds the issues from the IP addresses and distinguish network information from other networks automatically. Also, users can control IP addresses without the involvement of DHCP administrators in which might save time and money consuming. It is also useful for remote offices in delivering messages and files through tablets, smartphones and desktops since users can move easily from one network to another network wirelessly and can also get an IP address automatically. Moreover, in remote office, DHCP may reduce manual IP address configuration errors and IP address conflicts from one or more devices that the staffs use at the same time which might lead to reduce traffic in delivering files and data from many devices at the same time. In addition, all IP address locations can be controlled from Central office which gives Central office a full permission to authorize the network users of the remote office.

A default gateway is an access point or IP router which is used to communicate with other devices on other networks. Default gateway is also a computer with two network adapters in which one is a local area network and the other one is a public network. Using default gateway in EFA might support the remote office by connecting several kinds of devices and deliver same files and data to each device conveniently. This process might save time, money and effort consuming. Moreover, default gateway is suitable for both Central office and remote offices since it provides authentication for users accessing the gateway. This might prevent the sensitive data and files from unauthorized users. In addition, it performs like firewall in network security and separates the Intranet and public network. This might lead to prevent critical information in the central office from spreading into the public.

A subnet mask is a 32-bit number that identifies the network range, covers the IP address component and separates them into network address and host address. Using subnet mask in EFA’s remote office will prevent unnecessary broadcasts in which the messages are sent to every computer along the network. This will facilitate the staffs in remote office to deliver messages and files to the right person. Moreover, it will also perform like firewall in the case of security and authorize the users in accessing into the network. Therefore, there is no need to be worry about security threats in both central office and remote office. In addition, subnet mask also increases the network performance and speed by removing the traffics along the network. Hence, data and files can be delivered quickly from one device to another in both central office and remote office.

According to these following reasons, both default gateway and subnet mask are required for both central office and remote office.

There are various kinds of network security countermeasures to prevent the security threats. To recommend 7 of them, these include as follows.

# 

EFA must use Firewall in the central office, where all services are managed from it in There are various kinds of network security countermeasures to prevent the security threats in order to protect the hardware and software at there from traffics, viruses and worms and also to detect, block and prevent all these threats.

# 

In EFA, they should use anti-virus software in order to protect the networks from virus, trojans, worms and malwares in which they can enter the networks of EFA through email servers and webservers.

Since EFA store important sources like client information, email servers and web servers, authentication is important to identify the network accessors and to permits only the authorized users to access in the protected sources, networks and devices.

This process is important for EFA since there are so many staff in there. This process might help EFA to reduce staff thefts and physical deliberate threats.

EFA should use vulnerability scanners in order to scan the issues and weaknesses which can be get rid by hackers. It will also find those vulnerabilities launching or spreading along the networks and protect them from hackers.

This policy is particularly important for EFA since it sets the rules for people who will access into the networks, services and devices in the purpose of preventing them from cyber-attacks, intruders and staff thefts. These people must follow the rules such as not to enter the unknown websites, sources and messages, to use the authorized devices and to agree all the responsibilities if they break the rules.

This software must be used in EFA since they use Intranet accesses and remote accesses in which the intruders can enter through these accesses. IDS may protect these threats by detecting the traffics along the network and warn admins when they found these destructive activities.

The biggest threat for network security system of EFA might be Ransomware. It may enter to the network of EFA through some phishing emails with destructive attachments or by auto downloading the malicious software without the user’s allowance. They will lock all the sources of EFA or encrypt them to interrupt the users from accessing them. When the network is infected by Ransomware, EFA will lose their sources temporarily or permanently, can impact on financial loss to restore their sources and sometimes, they can get harm on reputation. The hackers threaten the organization for payment if EFA want their sources back after the sources are hacked. Sometimes, although the payment is done, they may not give the organization’s sources back. However, EFA can back-up their files in The Cloud, can educate the employees not to open the files from unknown sources and can protect by using Firewalls or anti-virus software in order to prevent this threat.

(c) In central office, EFA has to use 8 network computers which are connected to switch with the use of cables in order to transfer data within the office. Also, the access point, which enables wireless private network is connected to switch in order to connect with the devices such as phones, tablets and whithin the office wirelessly. The domain controller is also put in the central office and connected to the switch in order to authenticate the users who will enter into the resources and networks of the central office, stores the users’ informations and promulgate the security policy rules to the accessors. The two network printers are also used in central office of which one of them is connected to the switch with the connector while the another one is connected to the access point wirelessly.

DMZ (Demilitarised Zones) which separates the private network in the central office from other public networks is also located in the central office. The email servers, web servers and data base servers, which are connected to switch are also put in there in order to access from the Internet and to remain the private network prevented from untrusted sources.

All of this componets in the central office are protected by firewall, which is a hardware device or program that will protect the informations in the central office from hackers, threats, vituses and intruders. Following, firewall will connect with the router which will connect to the public Internet network through VPN. VPN will provide the encryption and decryption systems which will make EFA secure in data transfering system. Through these processes, the private network in central office can able to connect with the public Internet harmlessly and securely.

Also, the two remote offices are connected to the router through the firewall in order to connect with the public Internet network with the use of VPN tunnel. The tablets, phones and other moblie devices in the remote offices are also connected to the access point wirelessly which is connected to the Firewall in order to transfer data within the office safely and harmlessly.

1. Since staffs of EFA has to access email, client records and intranet through laptops and smart phones, they need a secure remote access in this system. In this case, EFA should use VPN (virtual private network). It is a private network created virtually on a public network (like WIFI or Internet) to protect the information transferred through the network. VPN will provide EFA with the components like protocols (IP security, PPTP and L2TP). VPN routers and network security functions like authentication, encryption, access control, data integrity and firewall. By using VPN, it will hide the actual IP address of EFA, confirm the correct receivers and senders of information, protect the network from unauthorized users, encrypt the conversation along the network and prevent the network from hackers and viruses.
2. Since staffs from EFA use remote accesses through mobile devices like laptops and smartphones, there will be a bit impact on security according to the following reasons:

Most of the remote access systems require only simple logins and passwords. If EFA uses single sign on methods to access into various organizational systems, it may lead to staff thefts and hacking. In this case, EFA can protect their network by using different sign in system, encrypting the network and using authentication to access into the system.

Most remote access can’t checkup the virus or malwares of the devices. This may lead the hackers to put viruses into the network and hack all the organization critical data. This can be protected by using IDS, antivirus software and firewall.

Since EFA has multiple of staffs accessing into the remote access system, EFA should specify authorization and authentication system in this system. Without it, it might lead to staff thefts and technical impacts.

1. VOIP is a technology which uses packet switch network protocols in order to enable traditional telephone services through the internet. VOIP uses codecs to convert the voice signals into data packets while sending along the network and reconvert the data packets into voice signals when they are sent.
2. Using VOIP system will fulfil EFA’s expectations in communication and training among staffs and learners. To implement VOIP system in EFA, they need to figure out the number of users, the Internet speed and accessing VOIP providers and devices. EFA will need components such as VOIP servers and provides, VOIP compatible phones and VOIP software. Using VOIP, EFA can give training classes to the learners and staffs through video conferencing only using the mobile devices which might lead to save time and money. Also, using VOIP can help EFA in delivering learning schedules and exercises to the learners through voice mails and emails only in one click and hence, there will be no separation in voice and message delivery. According to these reasons, EFA should implement VOIP system in their organization.

* Provides cost- effective features and functions
* Provides communication around the world using Internet connection
* Supports video conferencing which can access directly to training, teaching or monitoring
* More touchy than traditional telephone service
* Easy installation, configuration and maintenance
* Must use Internet connection
* Can have issues like latency or packet loss when the signal is low
* Can have security issues like hacking, eavesdropping or denial of service