**Networking report**

As a networking consultant, it is my job to help design and explain in detail about the equipment and how the network work. This report aim is to do into deep detail of each equipment that are present in the network and their role, the overview of the network, threat that may harm the network and how to prevent such threat, and lastly the recommend security module.

1. **The network equipment**

* The end-user device: These type of devices include computer that employee use, the printer, phone, laptop, smartphone, tablet. These type of devices is to help the user to connect to the network.

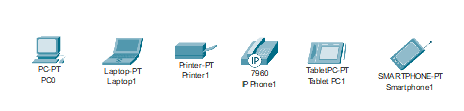


Figure 1: the icon of the end-user devices

* Access-point/Wi-Fi router: This device help connects the wireless devices to the network by entering the right id and password of the Wi-Fi.

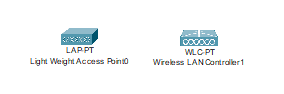


Figure 2: The Wi-Fi modem and Wi-Fi controller

* Switch: Switch is a device that help end-user communicate in a local network by forwarding packet to a single device. This communication happens in layer 2 of the network where these end-users communicate thought MAC address, which is a permanent address of a device.



Figure 3: Switch icon

* Router: Router help selected path for data packet to travel across the network to reach their destination. It job is to connect other local network together so it acts like a bridge between network. This communication work in layer 3 of the network, where instead of MAC, the network communicates thought IP address, which is a temporary address.



Figure 4: Router icon

* Multi-layer Switch: This device is a combination of switch and router which give the device both the ability to communicate in layer 2 and layer 3.

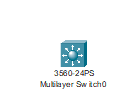


Figure 5: Multi-layer Switch icon

* Firewall: This device id mainly uses for security purpose in the network, it main job is to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules



Figure 6: Firewall icon

* Server: This is where all the service such as web, mail is hosted, it provides resources, data, services, or programs to other computers, known as clients, over a network



Figure 7: Server icon

1. **Overview of the network**

This network is consisting of 4 branch: Ha Noi, HCM (Ho Chi Minh), SaPa, Da Nang, which each branch has 1 server room and 3 departments: Marketing, I.T, Finance. Out of these 4 branch, Ha Noi is the main branch and also act as a data center of all the network and the host of the DMZ zone, 3 other branch will be sub-branch that work independently and all of the branch will communicate thought the internet. In this section of the report, the design of main and sub branch will be discussing, this include: the architecture of the network, the DMZ zone, how the network communicates internally and externally, what service each network use.

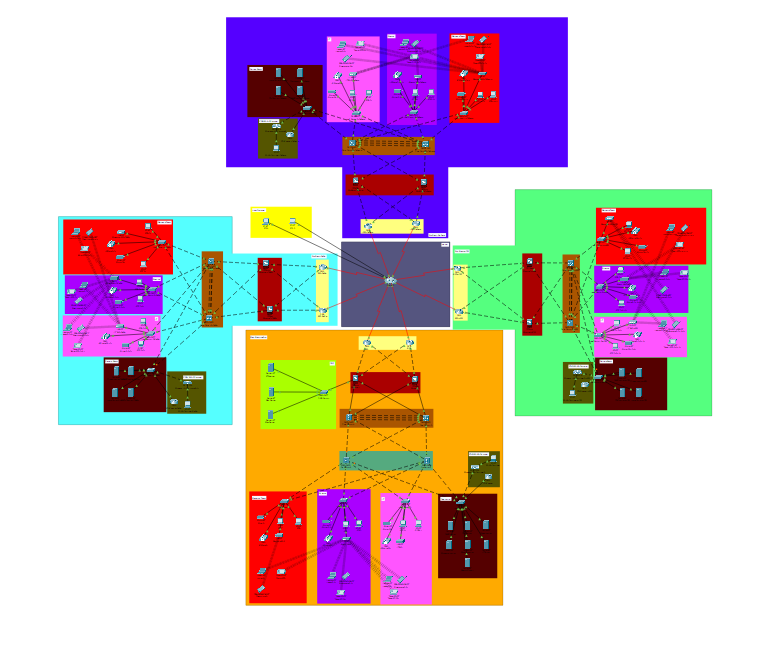
****

Figure 9: the overview of all 4 branch

1. **The architecture of the main and sub branch**

Both the main and sub branch use leaf and spine architecture for end-users and servers to communicate, while as the main branch use tier 3 architecture for outside communication and sub branch use tier 2 architecture for the same purpose. Both branch have redundancy for each switch and multilayer switch, this is also true for ISP (internet service provider), which mean that if any switch/multilayer switch or 1 of the ISP stop working, the network can still function.

* Spine and leaf architecture: This is a two-layer network topology composed of spine and leaf switch. This topology priorities east-west network traffic, which reduce network latency and improve network efficiency. This also help scalability and redundancy, this mean that other end-user devices can be added later on and help the availability of the network even if a switch die.

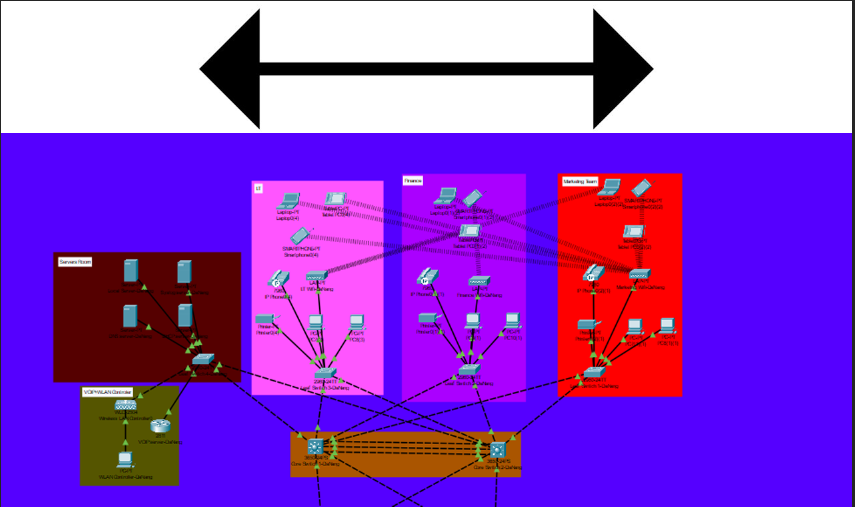


Figure 10: the direction of Spine and leaf architecture communication

* Tier 2 architecture (sub branch architecture): The tier 2 architecture consist of 2 layer: access and distribution layer. The access layer is where the end-users connect to the switch, where as the distribution layer are where the switch connect to the multilayer switch so LANs can connect with each other. The distribution layer also has another job is to connect to the router for outside communication. This architecture is use on the sub branch due to it cheaper cost and efficiency.

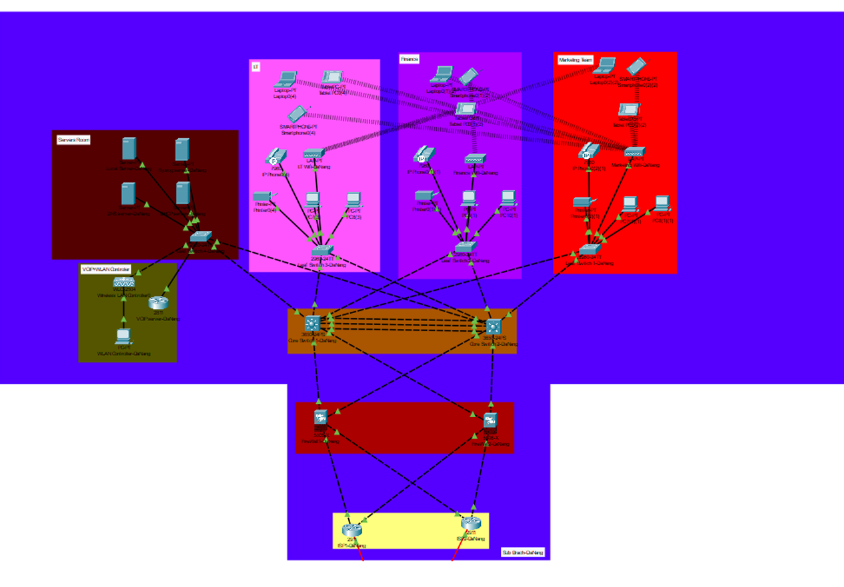


Figure 11: the 2 tier architecture/ sub branch architecture

* Tier 3 architecture (main branch architecture): Similar to the tier 2 efficiency, the tier 3 efficiency also consist of access and distribution layer, but also include core layer which consist of 2 more multilayer switch. In this architecture, the core layer will be handling the outside communication so the distribution layer can focus on inter connection of the network, this make the network much faster, which is needed for the main branch as it also acts as the data center for the entire network and the host of the DMZ zone.

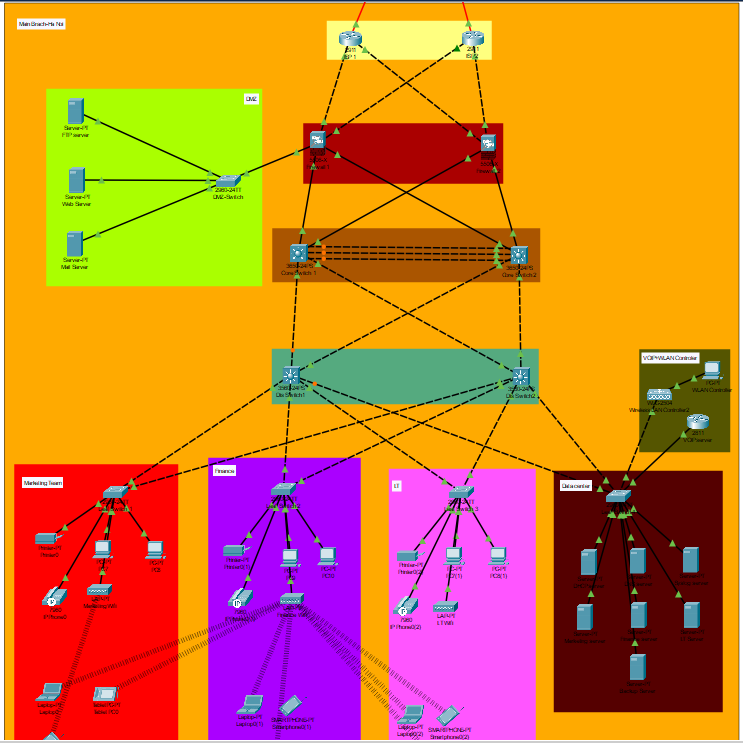


Figure 12: the 3 tier architecture/ main branch architecture

1. **The DMZ zone**

DMZ zone or demilitarized zone is a subnetwork that contain public-facing resources, which is resource that public could access to such as web service. The main purpose of a DMZ is to isolate the public resource from the private one with some factor of security.

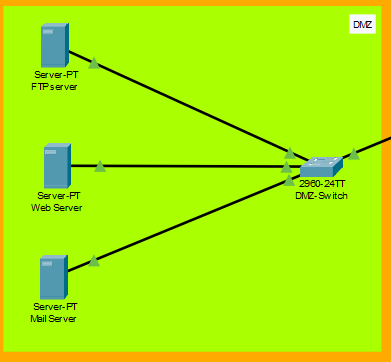
****

Figure 13: The DMZ zone

1. **Network internally and externally communication**

For the network able to communicate internally, the OSPF routing protocol have been selected, and the same go for BGP routing protocol for external communication.

* + OSPF routing protocol: OSPF or Open Shortest Path Frist is a routing protocol that use link state, which where the protocol will have all device to show their location to form a topology map. Using this map, the protocol will be able to calculate the shortest path to the destination even if there a disconnect switch or topology change.
  + BGP routing protocol: Border Gateway Protocol (BGP) is the postal service of the internet. When a packet is send via the internet, BGP is responsible for looking at all of the available paths that data could travel and picking the best route, which usually means hopping between autonomous systems.

Other than those 2 routing protocol, the network also got divide into 3 different VLAN, which each VLAN represent different type of end-user devices that communicate within the network.

* + LAN: This VLAN is where all the company end-devices belong to, which include to company computer and printer.
  + WLAN: Wireless LAN is where all the devices that connect to the company Wi-Fi belong to, which let some devices have the ability to connect to the network.

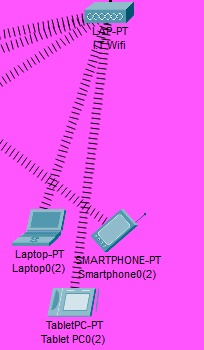


Figure 14: Other devices connect via the Wi-Fi modem

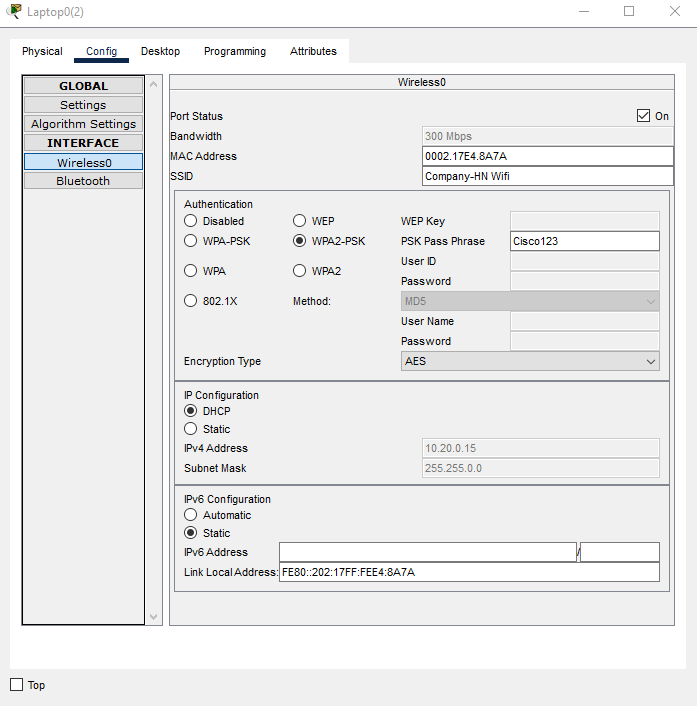


Figure 15: A laptop connects to Ha Noi Wi-Fi by id and password

* VOIP: This is where all the phone in the network connect to, which help employees to communicate within the branch.

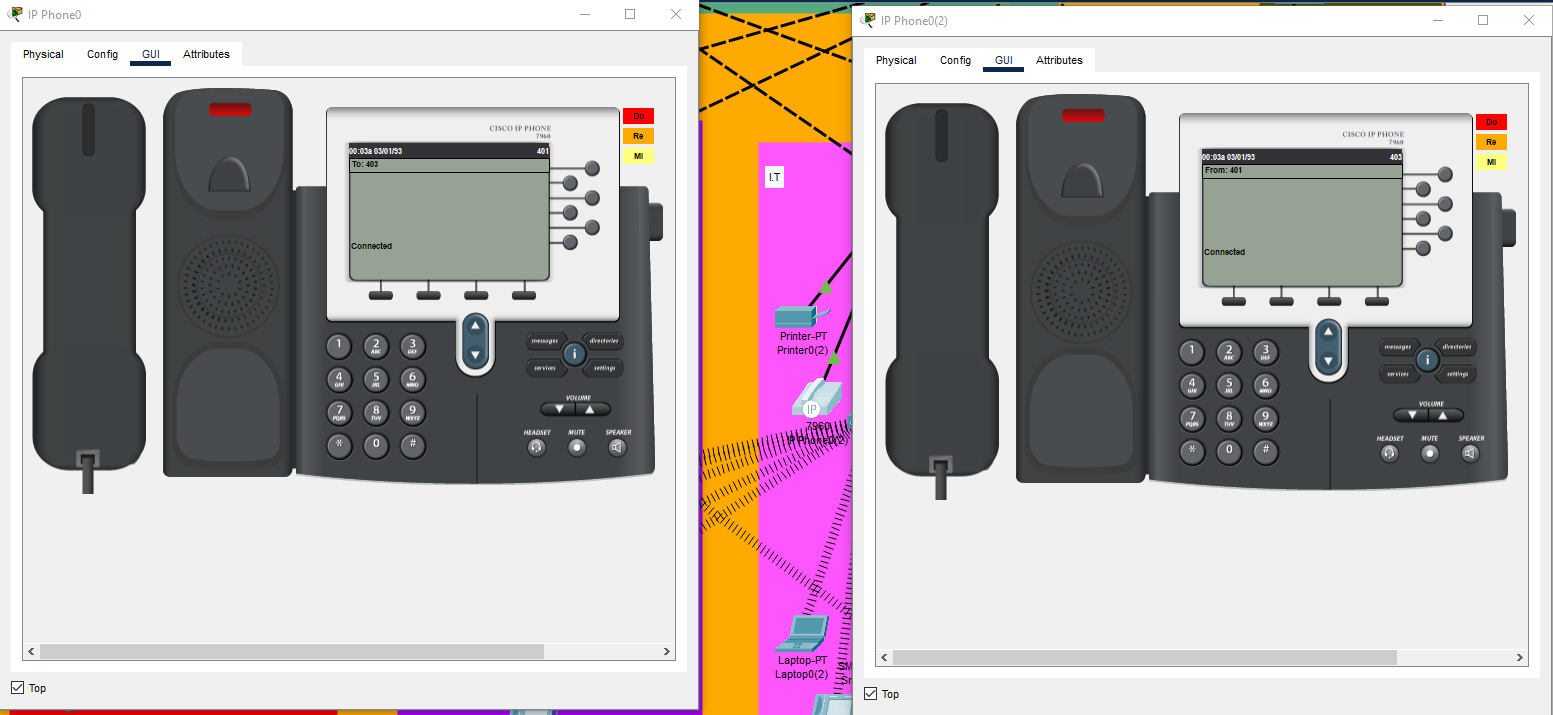


Figure 16: phone 403 is connect/call phone 401

|  |  |  |
| --- | --- | --- |
| VLAN | IP | Branch |
| LAN | 172.16.0.0 / 255.255.0.0 | Ha Noi |
| 172.17.0.0 / 255.255.0.0 | HCM |
| 172.18.0.0 / 255.255.0.0 | SaPa |
| 172.19.0.0 / 255.255.0.0 | Da Nang |
| WLAN | 10.20.0.0 / 255.255.0.0 | Ha Noi |
| 10.21.0.0 / 255.255.0.0 | HCM |
| 10.22.0.0 / 255.255.0.0 | SaPa |
| 10.23.0.0 / 255.255.0.0 | Da Nang |
| VOIP | 172.30.0.0 / 255.255.0.0 | Ha Noi |
| 172.31.0.0 / 255.255.0.0 | HCM |
| 172.32.0.0 / 255.255.0.0 | SaPa |
| 172.33.0.0 / 255.255.0.0 | Da Nang |

Figure 17: The IP table of all the VLAN of each branch

1. **Network services**

There are 4 different type of services in each branch and 3 in the DMZ zone, these services are: HDCP server, DNS server, syslog server, data server, web server, FTP server, mail server.

* DHCP server: This server main job is to assign IP to company computer, each computer will receive a IP that belong to a IP pool/range.

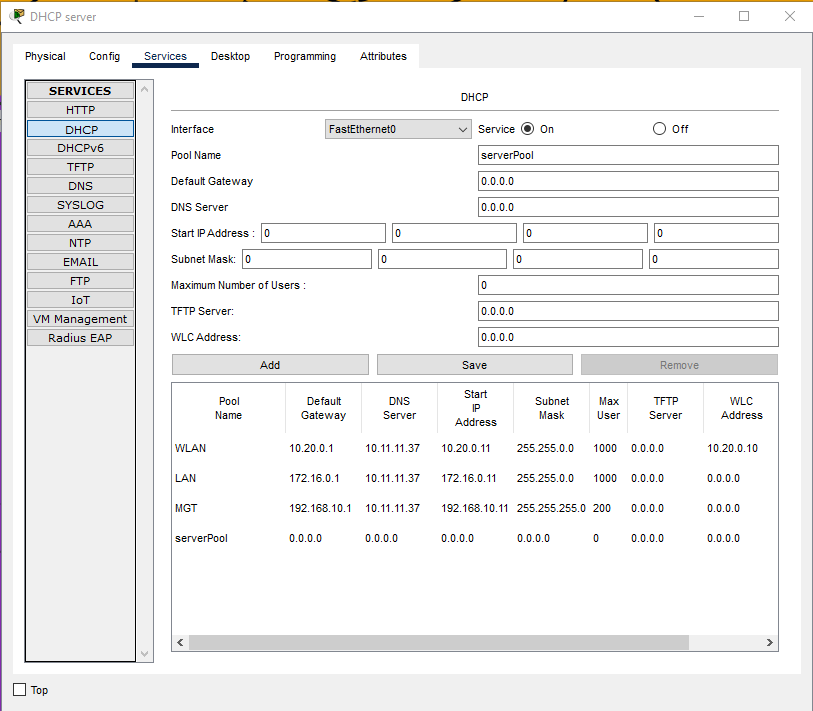


Figure 18: The DHCP server of Ha Noi branch

* DNS server: Similar to the DHCP, the DNS server assign name to an IP, which is more user friendly. For example, to access 10.11.11.11 (company website), user do not have to enter the whole IP, but just need to enter “https://cisco.com”.

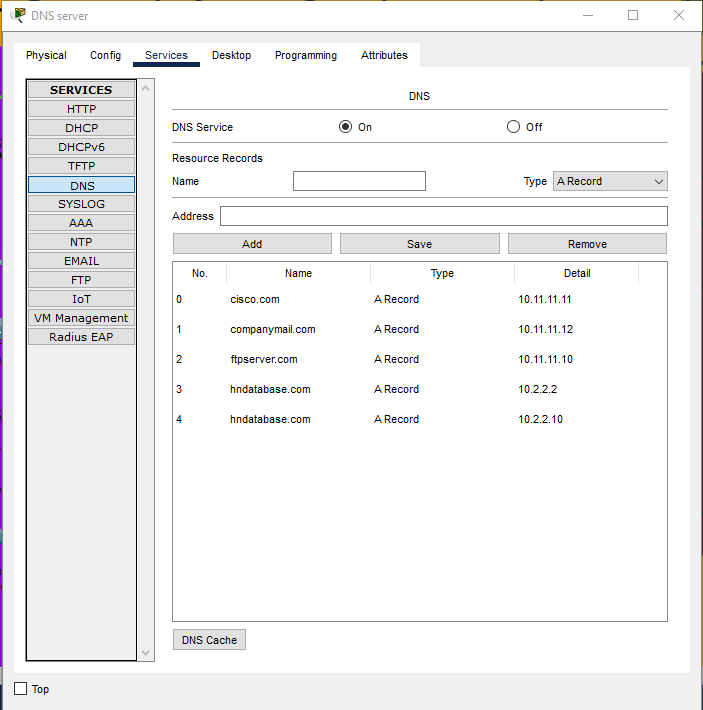


Figure 19: The DNS server of Ha Noi branch

* Syslog server: This server role is to log any change of the network and activity of the company website, this log will be display as time of action and the action itself.
* Data server: This is where the company data is store. In Ha Noi, which is the main branch and data center, each department have their own data server, whereas the sub-branch department share 1 data server. To access the data server for both inside and outside the network need a username and password to access it.

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Password | Data server | Data access |
| Head-Marketing | Cisco123 | https://hanoidata.com | Ha Noi marketing server |
| Head-I.T | Cisco123 | https://hanoidata.com | Ha Noi I.T server |
| Head-Finance | Cisco123 | https://hanoidata.com | Ha Noi finance server |
| HCM | Cisco123 | https://hcmdata.com | HCM main server |
| HCM-Marketing | Cisco123 | https://hcmdata.com | HCM marketing server |
| HCM-IT | Cisco123 | https://hcmdata.com | HCM I.T server |
| HCM-Finance | Cisco123 | https://hcmdata.com | HCM finance server |
| SaPa | Cisco123 | https://sapaoidata.com | SaPa main server |
| SaPa-Marketing | Cisco123 | https://sapadata.com | SaPa marketing server |
| SaPa-IT | Cisco123 | https://sapadata.com | SaPa I.T server |
| SaPa-Finance | Cisco123 | https://sapadata.com | SaPa finance server |
| DaNang | Cisco123 | https://danangdata.com | DaNang main server |
| DaNang-Marketing | Cisco123 | https://danangdata.com | DaNang marketing server |
| DaNang-IT | Cisco123 | https://danangdata.com | DaNang I.T server |
| DaNang-Finance | Cisco123 | https://danangdata.com | DaNang finance server |

Figure 20: List of all accounts for data server of all 4 branch

* Web server: This is where the company website is host, it located in the DMZ so the user can access the web without enter the company network.

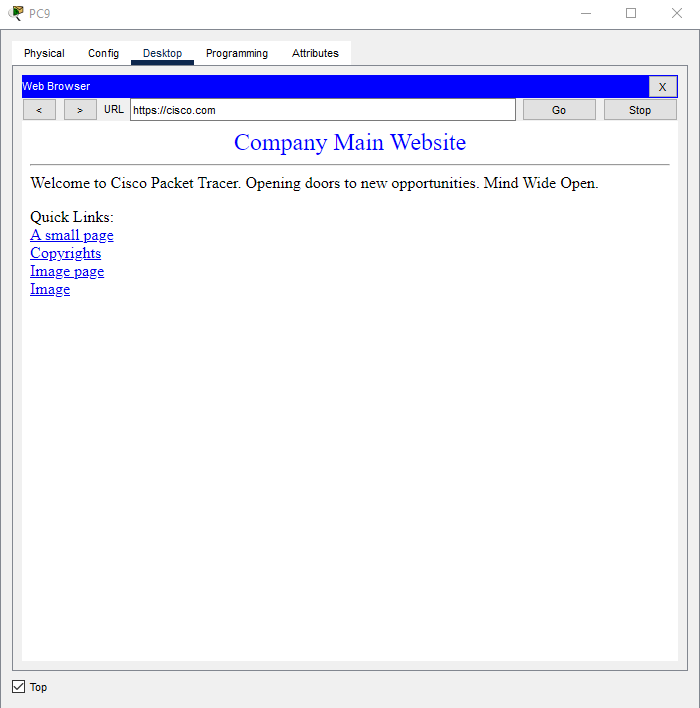


Figure 21: Accessing the company website

* FTP server: File Transfer Protocol server is to let all 4 branch share file within one server, which help centralize the data to the main branch and update the company website. To access FTP, a username and password that is resign in the server is required.

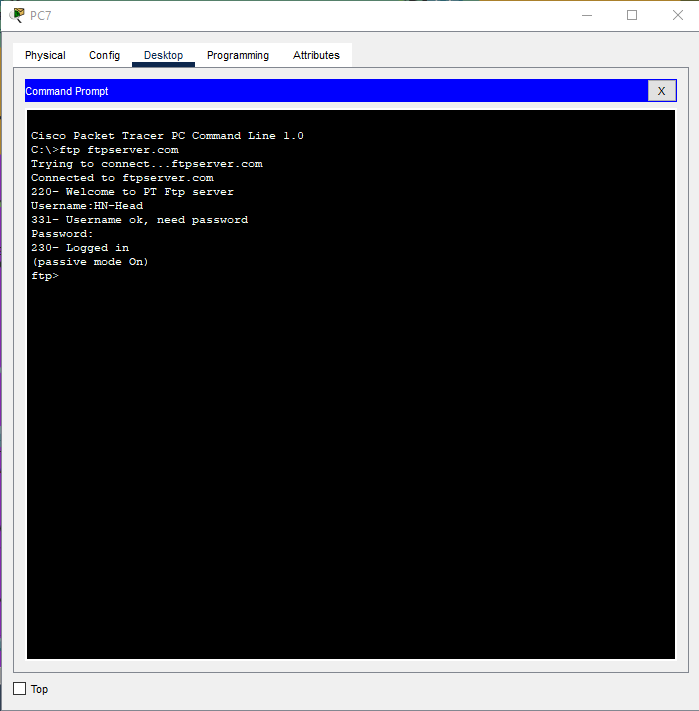


Figure 22: Logging in to ftp server

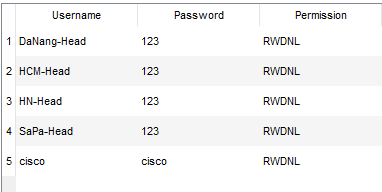


Figure 23: List of accounts in the ftp server

* Mail server: Similar to the FTP server, mail server main role in the network is to help employee communicate all over 4 branch by exchange mail. To able to exchange mail, an account that resign in the server is required.

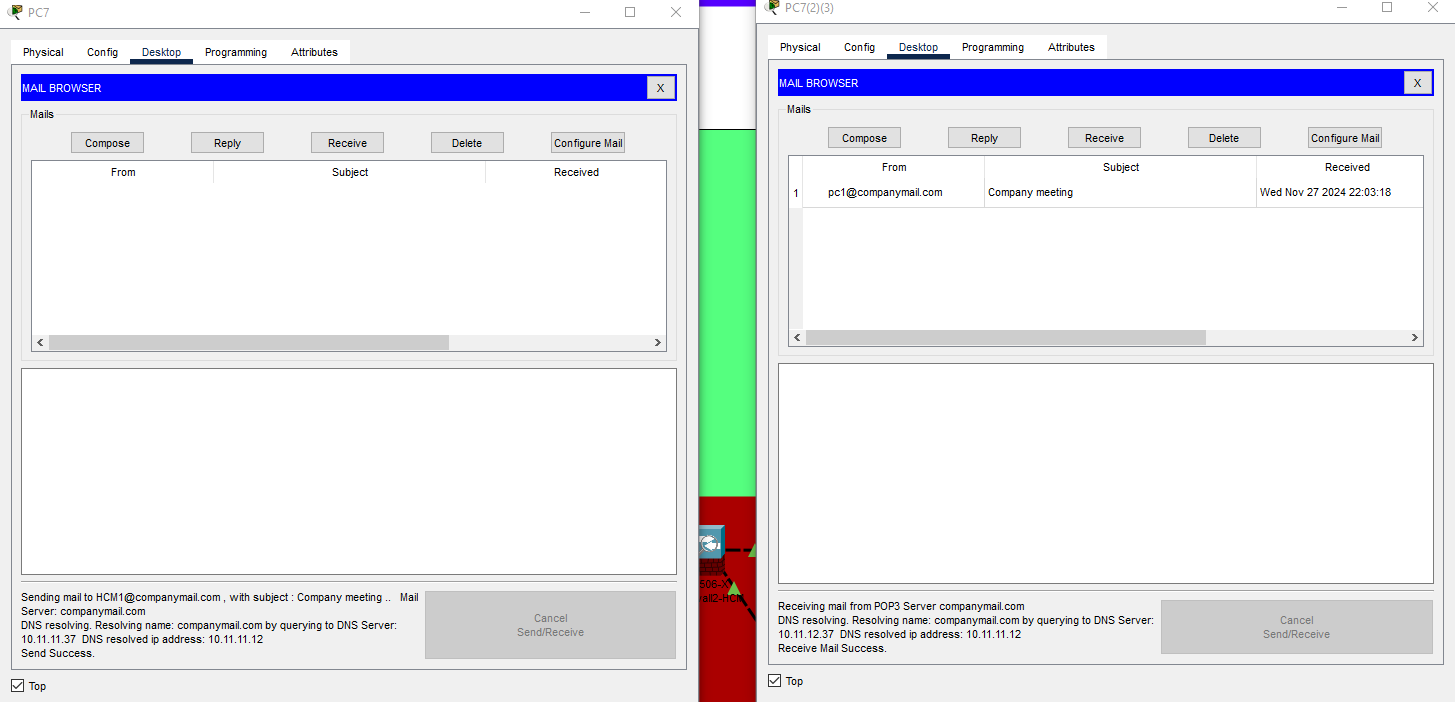


Figure 24: pc1(HaNoi1) sending mail to HCM1 and HCM1 received the mail

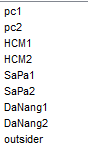


Figure 25: List of email account in the mail server (password for all:123)

1. **Threat and solution**
2. **Network security and threat that have been prevent**

To able to protect the network from potential threat, some security protocol has been impairment in the network. The table below will show what part of the network that the protocol is in and the detail and threat haven been prevented by the protocol.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Security protocol | Detail | Threat prevented |
| Layer 2 | DHCP snooping | Monitoring packet from untrusted interface(end-user) when requested IP from the trusted port(DHCP server) | -DHCP starvation  -DHCP spoofing  -DHCP poisoning |
| ARP inspection | Monitoring packet from untrusted interface(end-user) when forwarding ARP packet to the trusted port(server) | -ARP poisoning  -ARP spoofing |
| Port-security | Prevent unknown end-user device connect to the network by learning their MAC address | -Unknown devices accessing the network |
| BPDU guard | Prevent unknown switch to connect to the network | -Unknown devices accessing the network |
| Switch/multilayer switch password (password: Cisco) | Require password to modify switch/router configure | -Unauthorized access to the switch/ multilayer switch |
| Layer 3 | Firewall security level | This create security level for each zone and lower security zone can not enter higher level without permission. The security level divide are: outside (0%), DMZ (70%), inside (100%) | -Outside devices accessing the inside network  -Malware attack  -DoS/DDoS |
| Server | FTP allowed IP | Only company devices which belong to IP range of LAN VLAN can access the ftp server | -Unknown devices accessing FTP server by stealing FTP account  -Malware attack |
| Mail allowed IP | Only company devices which belong to IP range of LAN VLAN can access the mail server | -Unknown devices accessing mail server by stealing mail account  -Fishing attack |
| Using https in web sever | Using https port number instead of http for more security due to http have minimal security built in | -Eavesdropping between web browsers and web servers |
| Use AAA for accessing the data server | When accessing the data server for both inside or outside the network, an account is needed. Each account have their own permission in the data server and the action of these account will be log in the syslog server | -Each department accessing each other department database  -Stealing/modifying data |

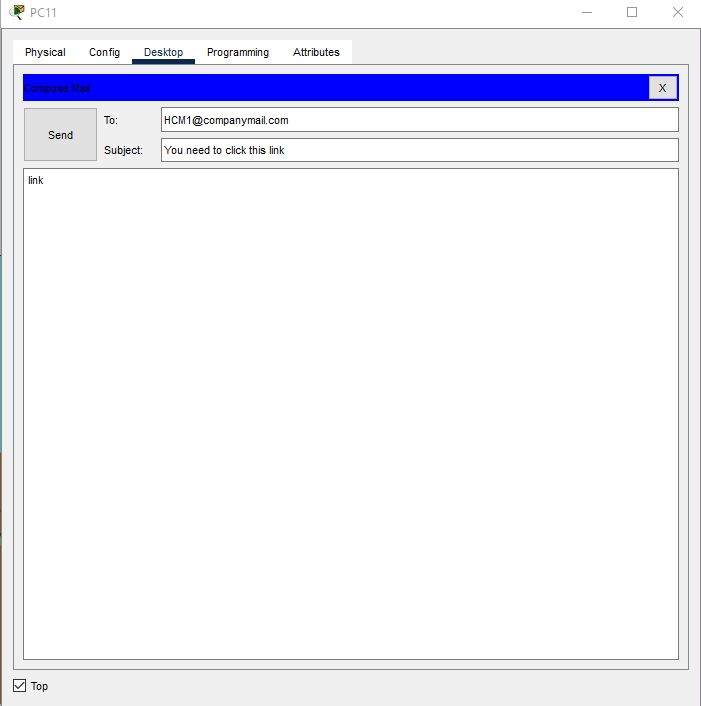
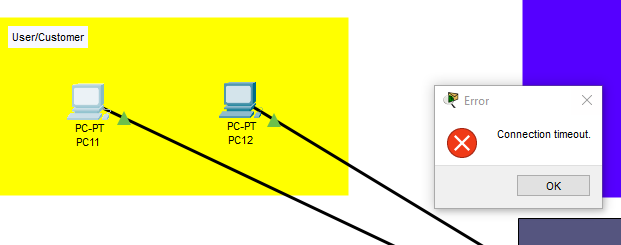
 

Figure 26: outsider use company mail to send mail but got blocked

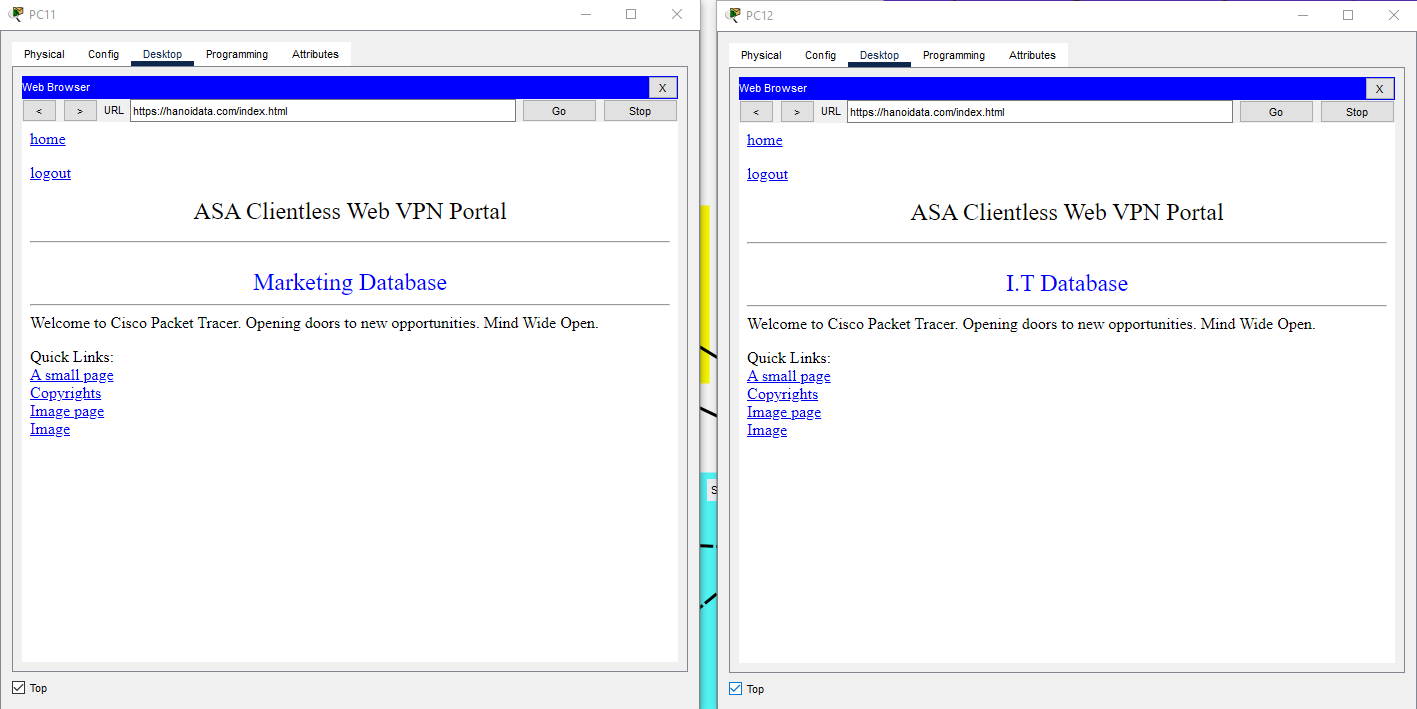


Figure 27: 2 user access “https://hanoidata.com” with different account

1. **Potential threat and it solution**

Despite the network security protocols, some potential threats still exit within the network. The table below will display some of these threat and how to avoid them.

|  |  |  |
| --- | --- | --- |
| Threat | Detail | Prevention |
| Ransomware | Hacker/attacker encrypting data and ask for money for decryption | Make backup for data server daily |
| Malware | Attacker can use company computer inside the network to send the malware | Install malware protection program and check the syslog for any danger of malware |
| Fishing | Attacker can use company computer inside the network to send the fishing mail | Check the mail before clicking any link in the mail |
| SQL injection | Using SQL command to stole or implant the malware into the system/server | -Make a black list of which input should not be enter  -Use website with SQL protection  -Monthly check the website for vulnerability  -Check syslog for any sign of attack |
| Brute force attack | Trying to guess username and password of an account to steal the it | Make strong password and change password monthly |
| Directory Traversal | Attacker try to access unauthorized files or directories outside the targeted folder by changing the directory in the web link | -Make a blacklist of what path user can not access  -If any user tries to access data server directory, ask for authentication  - Check syslog for any sign of attack |

1. **Recommended security module**

To ensure a secure working environment, 3 common security module is recommended, these modules are: CIA, AAA and zero-trust

* + CIA: Confidentiality, Integrity, and Availability (CIA) is a module which ensure that the network is protected, the data is not being modify between communication and the network is always accessible by both user and employee at all time.
  + AAA: Authentication, authorization, and accounting (AAA) module required user to provide a credential to enter, each account only able to access the data that the account is assign and each action need to be log.
  + Zero-trust: This module makes all access in the network require credential no matter the role of the user, which provide an extra layer of protection.

Word count: 1609