VIETNAM NATIONAL UNIVERSITY
HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING

Computer Network

ASSIGNMENT 2 REPORT

BB BANK's COMPUTER NETWORK

LECTURER:	Nguyễn Mạnh Thìn
STUDENTS:	Nguyễn Chí Hiếu - 1952679
	Trương Đăng Quang - 1952940
	Dương Xuân Anh Tú - 1852845
	Nguyễn Nhật Anh - 1852236

Ho Chi Minh City, 2021

Contents

1 REQUIREMENT ANALYSIS 3
1.1 Requirements . . . 3
1.2 Survey Checklist . . . 3
1.2.1 HQ . . . 3
1.2.2 Branches . . . 4
1.3 Network Structure . . . 4
1.4 High Load area . . . 4
1.5 Wireless Coverage . . . 5

2 NETWORK PAPER DESIGN 6
2.1 Equipment Usage . . . 6
2.1.1 Router . . . 6
2.1.2 Switch . . . 8
2.1.3 Multilayer switch . . . 9
2.1.4 Wireless Router . . . 9
2.1.5 Firewall . . . 10
2.1.6 Cable . . . 11
2.2 Physical Design . . . 14
2.3 IP Address Table . . . 15
2.4 Network Throughput, Bandwidth and Safety Parameters Calculation . . . 17
2.4.1 Network Throughput Calculation . . . 17
2.4.2 Bandwidth Calculation . . . 18
2.4.3 Safety Parameters Calculation . . . 18
2.5 Network Design . . . 18

3 PACKET TRACER LOGICAL DESIGN 21
3.1 Theoretical basis . . . 22
3.1.1 Address Resolution Protocol . . . 22
3.1.2 VLAN Trunking Protocol . . . 24
3.1.3 Dynamic Host Configuration Protocol . . . 25
3.1.4 Network Address Translation . . . 27
3.1.5 Access List Control (ACL) . . . 28
3.1.6 Open Shortest Path First . . . 31
3.2 Switch and VLAN configuration . . . 33
3.3 Wireless Router configuration . . . 35
3.4 OSPF Protocol Configuration . . . 36
3.5 Security Configuration . . . 36
3.5.1 Configuring Cisco ASA 5506 . . . 36
3.5.2 Configuring Acess List Control (ACL) . . . 37
3.5.2.a Headquarter Router . . . 37
3.5.2.b Nha Trang Router . . . 38

3.5.2.c Da Nang Router 39
3.5.3 Network Address Translation (NAT) 40
3.5.3.a NAT over PAT 40
3.5.3.b Static NAT 40

4 TESTING AND RESULTS 41
4.1 Test with Ping 41
4.2 Test the system with Tracert 45

5 CONCLUSION 46
5.1 Re-evaluate the designed network system 46
5.1.1 Reliability 46
5.1.2 Easy to Upgrade 46
5.1.3 Diverse Support Software 46
5.1.4 Safety 46
5.2 Expected Cost 47
5.3 Remaining Problems 48
5.3.1 Security 48
5.3.2 Scalability 48
5.4 Future Development 48
5.4.1 Security 48
5.4.2 Scalability 48

1 REQUIREMENT ANALYSIS

1.1 Requirements

- **Three separated local network of BB Bank**: one **headquarter** in HCM city and two branches in Nha Trang and Da Nang.
- **Headquarter:**
  - The building consists of 7 floors, the first floor is equipped with one IT room and Cabling Central Local.
  - Small-scale BBB: 100 workstations, 5 Servers, 10 Network devices.
  - Using new technologies for network infrastructure including 100/1000 Mbps wired and wireless connection.
  - The network is organized according to the VLAN structure.
  - The network connects to outside by 2 leased line and 1 ADSL with a load-balancing mechanism.
  - Using a combination of licensed and open-source software, office application, client-server, multimedia, database.
  - Requirements for high security, robustness when problems occur, easy to upgrade the system.
- **Branches:** also designed similarly to the headquarter but with a smaller scale.
  - The building is about 2 floors high, the first floor is equipped with 1 IT room and Cabling Central Local.
  - BBB Branch: 50 workstations, 3 servers, 5 network devices.
- **Total upload and download** of each Server: 500 MB/day, Workstation: 100 MB/day, Wifi-guest connection: 50 MB/day with the flows and load parameters of the system of about 80% at peak hours (9g-11g and 15g-16g).
- **Growth rate** must be above 20% in 5 years.

1.2 Survey Checklist

1.2.1 HQ

- Check for location of the servers, workstation, network devices and their distribution within the building.
- Check for number of the servers, workstation, network devices and connection within them and connection to the branches.

1.2.2 Branches

- Check for location of the servers, workstation, network devices and their distribution within the building.
- Check for number of the servers, workstation, network devices and connection within them and connection to the other branch, headquarter.

1.3 Network Structure

For convenience and aesthetics, the BB bank's network use the **Star topology** which is a type of network topology in which all the nodes are connected to the central hub or router. For example:

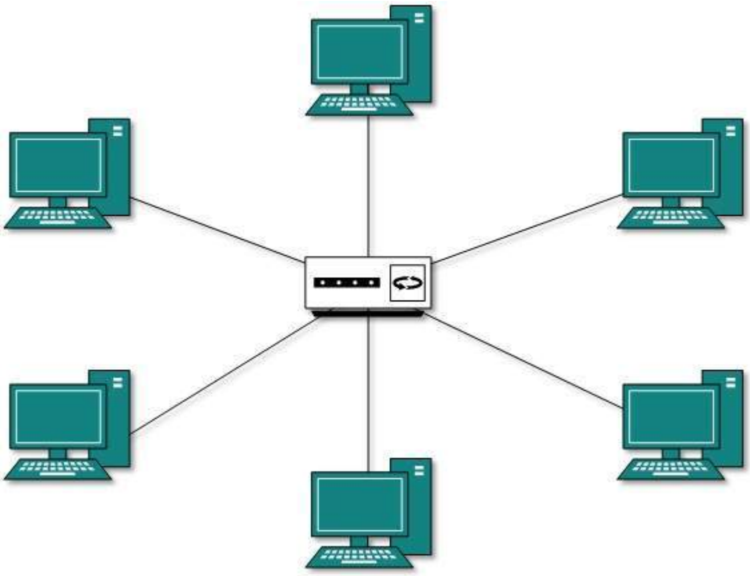


Figure 1: Example for star topology

1.4 High Load area

A large network is typically built by connecting multiple smaller networks together. A network can be as small as two computers in a home or as big as the Internet. When the computers, servers, or devices in a network are in close proximity to each other, such as inside a single office or home, the network is referred to as a local area network (LAN). Connecting multiple LANs, usually across a larger geographical area, yields a wide area network (WAN). The Internet itself can be thought of as a WAN that aggregates many smaller WANs.
To handle large traffic volumes at their websites, companies often place a load balancer in front of a group of servers connected to the same LAN and running the same applications (sometimes referred to as a server farm). For even greater redundancy, a company might distribute requests across the servers on multiple LANs aggregated into a WAN. One of the goals of load balancing is

to maximize application reliability by eliminating single points of failure. Deploying network load balancers to load balance across servers on multiple LANs or even multiple WANs ensures that even if all servers in a LAN fail (or a network partition isolates the LAN), users don't experience failure, because traffic is redirected to accessible LANs where servers are still online.

Typically, we will have load balancing for area with high network load but with our design we only have one connection to the Internet service so it is not require to have load balancer in our system.

1.5 Wireless Coverage

- The wireless design in headquarter is similar to the design in each of the two branches.
- We design the network so that each floor has an access point to the wireless.
- We provide up to 253 users connecting to our wireless with the standard channel of up to 1-2.412GHz.
- All the devices connected to this wireless network can not be ping by other devices which are not in the same subnet area. However, the devices connected to this wireless can ping other devices from different subnet areas.

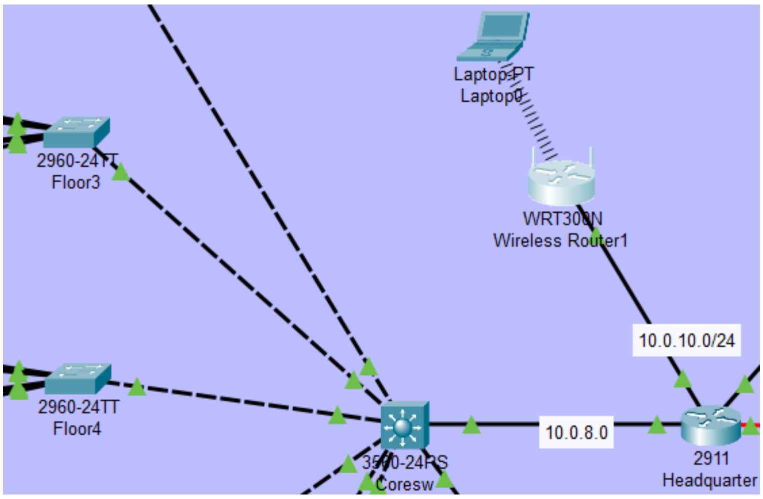


Figure 2: Example of Wireless network in HQ

2 NETWORK PAPER DESIGN

2.1 Equipment Usage

We used various type of network devices which are products of Cisco company. In this section we will describe each of the devices in detail.

2.1.1 Router

Theoretical basis: A router is a networking devices that forwards data packets between different computer networks. Routers guide and direct network data, using packets that contain various kinds of data such as files, communications, and simple transmissions like web interactions. [1]

The data packets have several layers, or sections, one of which carries identifying information such as sender, data type, size, and most importantly, the destination IP (Internet protocol) address. The router analyzes these data packets and decides the most optimal path to use for each transmission. [1]

According to the documentation from ***Cisco***, there are 5 main types of routers: [1]

- ***Core router***: Core routers are generally used by service providers (i.e. AT&T, Verizon, Vodafone) or cloud providers (i.e. Google, Amazon, Microsoft). They provide maximum bandwidth to connect additional routers or switches. This type of router is more suitable for large business that has huge number of employees working in different branches or locations.
- ***Edge router***: An edge router, also called a gateway router or just gateway for short, is a network's outermost point of connection with external networks, including the Internet.
- ***Distribution router***: A distribution router, or interior router, receives data from the edge router (or gateway) via a wired connection and sends it on to end users, typically via Wi-Fi, though the router usually also includes physical (Ethernet) connections for connecting users or additional routers.
- ***Wireless router***: Wireless routers, or residential gateways, combine the functions of edge routers and distribution routers. These are commonplace routers for home networks and Internet access. With this type of router, we can enlarge the performance and connectivity as well as security to a large range of users.
- ***Virtual router***: Virtual routers are pieces of software that allow some router functions to be virtualized in the cloud and delivered as a service. These routers are ideal for large businesses with complex network needs. They offer flexibility, easy scalability, and a lower entry cost. Another benefit of virtual routers is reduced management of local network hardware.

In this assignment, we use router ***Cisco 2911***:

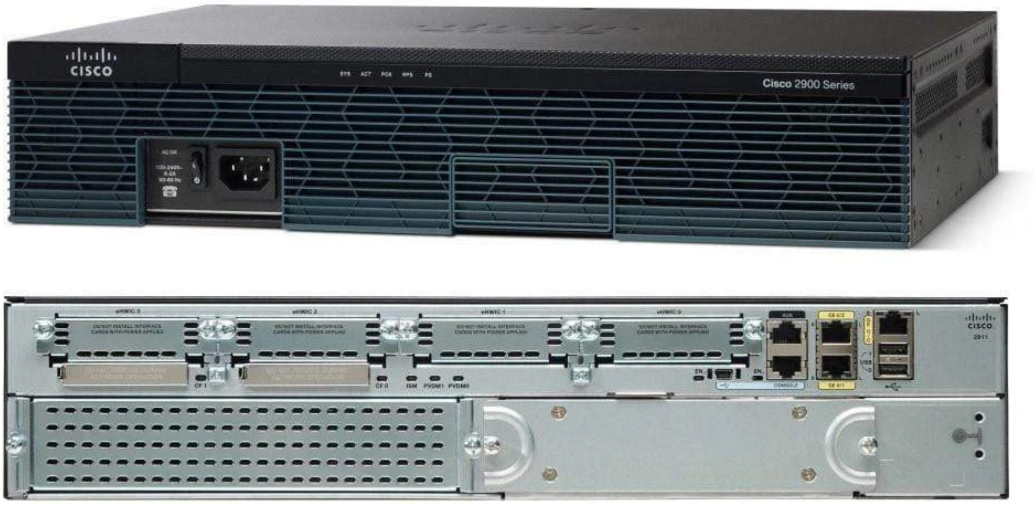


Figure 3: *Cisco router 2911*

- ***CISCO2911/K9***
- ***Port***:
  - 3 integrated 10/100/1000 Gigabit Ethernet ports (RJ-45 only)
  - 4 enhanced high-speed WAN interface card slots
  - 2 onboard digital signal processor (DSP) slots
  - 1 service module slot
  - 1 Internal Service Module slot for application services
- ***Security***:
  - Embedded hardware-accelerated VPN encryption for secure connectivity and collaborative communications Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering.
  - Identity management using authentication, authorization, and accounting (AAA) and public key infrastructure
- ***Quantity***: 3 (one for headquarter and the others for Nha Trang and Da Nang branch each).
- ***Description***: We use gigabit Ethernet ports to connect to the switches and routers in the same area. For connection to other branches over the WAN network, we use Serial port.

2.1.2 Switch

Theoretical basis: Switches facilitate the sharing of resources by connecting together all the devices, including computers, printers, and servers, in a small business network. Thanks to the switch, these connected devices can share information and talk to each other, regardless of where they are in a building or on a campus. Building a small business network is not possible without switches to tie devices together. [2]

There are two main types of switch according to cisco documentation: [2]

- ***Modular switches***: Modular switches let you add expansion modules as needed, giving you flexibility as network requirements change. Expansion modules are application-specific and include those for firewalls, wireless connectivity, or network analysis. They may also allow for additional interfaces, power supplies, or cooling fans. This type of switch provides you with the most flexibility, but at a higher cost.
- ***Fixed-configuration switches***: Fixed-configuration switches provide a fixed number of ports and are typically not expandable, which makes them less expensive overall. Fixed-configuration switches include unmanaged switches, smart switches, and managed switches.

Figure 4: *Cisco Switch 2911-24TT*

- ***Model***: 2960-24TT
- ***Port***:
  - 24 Ethernet 10/100 ports
  - 2 Gigabit Ethernet 10/100/1000 ports
- ***Quantity***: 13
- ***Description***: In the headquarter, there are 7 switches for seven floors from floor 1 to floor 7. All of them are connected to a layer 3 device, which is the multi-layer switch in our case. The switch on floor 1 support 5 servers in the server room. All the other floors from floor 2 to 6 supports a total of 100 workstations.

  In Nha Trang and Da Nang branches, each switch supports 24 ethernet ports, which accounts to a total of 48 workstations. The 2 remaining workstations will be connected directly to the multilayer switch.

2.1.3 Multilayer switch

Theoretical basis: Multilayer switch is a computer networking device that switches on OSI layer 2 like an ordinary network switch and provides extra functions on higher OSI layers. It combines layer 2, 3 and 4 switching technologies and provides high-speed scalability with low latency. Multi-layer switching can move traffic at wire speed and also provide layer 3 routing.

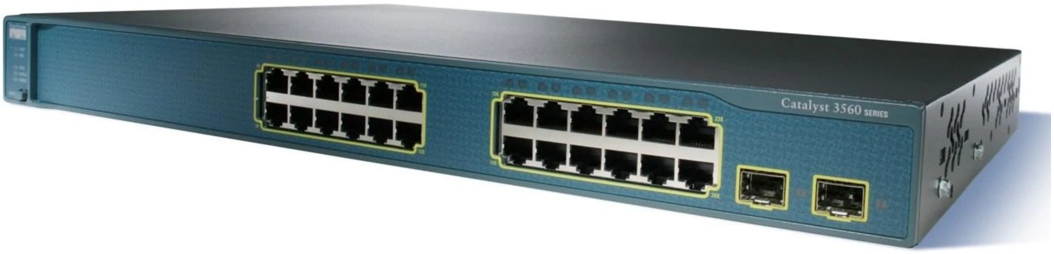


Figure 5: *Cisco Multilayer Switch 3560 24ps*

- ***Model***: 3560 24ps
- ***Port***:
  - 24 Ethernet 10/100 ports
  - 2 Gigabit Ethernet 10/100/1000 ports
- ***Quantity***: 3 (each office has 1)
- ***Description***: The multilayer switch will functions as a central switch connecting all the floor switches at headquarter as well as the branches. This multilayer switch will handle the routing between vlans.

2.1.4 Wireless Router

Theoretical basis: Wireless routers are commonly found in homes – they're the hardware devices that Internet service providers use to connect you to their cable or xDSL Internet network. A wireless router, also called a Wi-Fi router, combines the networking functions of a wireless access point and a router.

Figure 6: *Cisco Wireless router*

- ***Model***: WRT300N
- ***Bandwidth***: 2.4 GHz
- ***Integrated Switch***: 4-port switch
- ***Features***: DHCP support, DMZ port, MAC address filtering.
- ***Description***: Wifi router provides wireless connection to wireless devices with WPA2-PSK authentication. This serves internet service to the guest of each building as well as the staff.

2.1.5 Firewall

Theoretical basis: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. [3]

Types of firewall:

- ***Proxy firewall***: An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network.

- ***Stateful inspection firewall***: A stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed.
- ***Unified threat management firewall***: A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus.
- ***Virtual firewall***: A virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, KVM) or public cloud (AWS, Azure, Google, Oracle) to monitor and secure traffic across physical and virtual networks.

Figure 7: *Cisco Firewall ASA 5506X*

- ***Model***: ASA 5506X
- ***Port***: 8 Gigabit Ethernet, 1 RJ-45 and Mini USB console.
- ***Description***: In this assignment, we use firewall to filter the packets from the internet service provider as well as controlling the input and output of the flow.

2.1.6 Cable

In this system, we use three types of cable to connect our network: Copper straight through, Copper crossover, leased line.

- ***Copper straight through***: A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router.

Both pins on both ends match each other. This type of cable is usually used for connecting different types of devices.

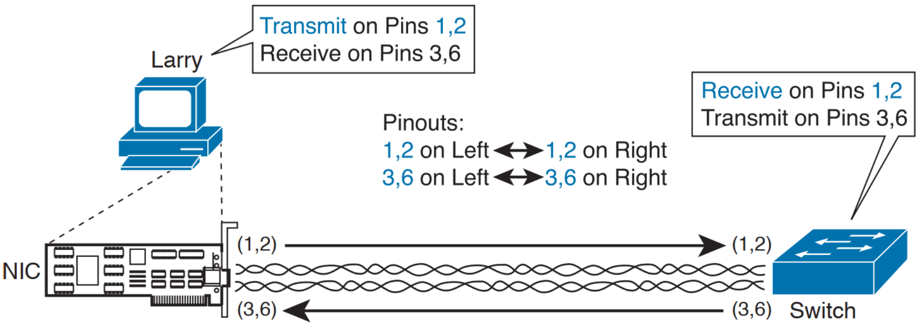


Figure 8: *Copper straight through cable*

- ***Copper crossover cable***: An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. The crossover cable pinout crosses the pair at the transmit pins on each device to the receive pins on the opposite device.

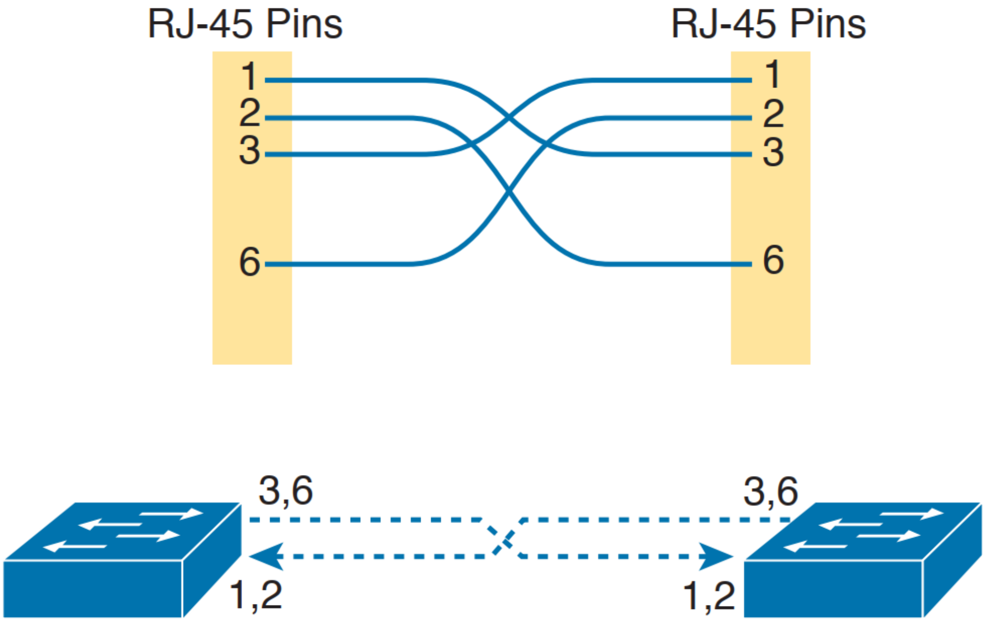


Figure 9: *Copper crossover cable*

- ***Serial cable***:the serial cables normally used between a router and an external CSU/DSU are called data terminal equipment (DTE) cables, plus a similar but slightly different matching data communications equipment (DCE) cable.

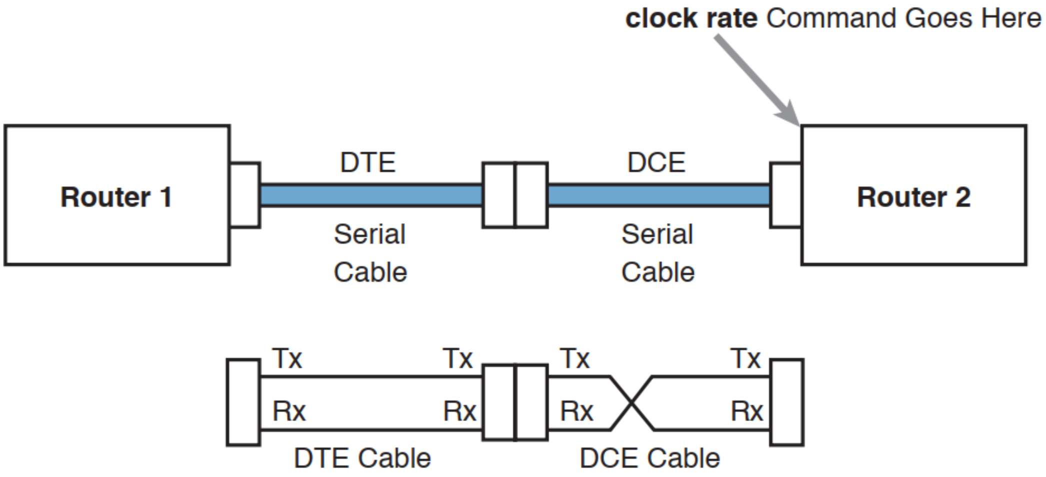


Figure 10: *DTE Cable and DCE Cable*

2.2 Physical Design

Our bank system consists of one headquarter located in Ho Chi Minh city and two branches in Nha Trang city and Da Nang city. These areas transfer information and data by means of WAN links. From the headquarter in Ho Chi Minh city, we use 2 **leased line** to communicate with other branches and one ADSL to the Internet service provider.

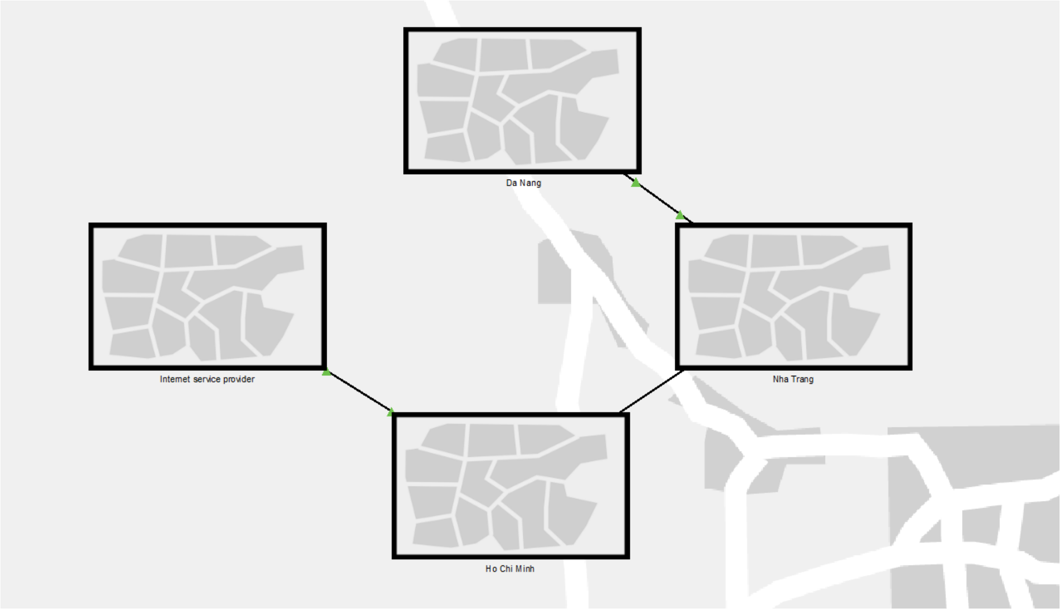


Figure 11: *Physical design of BB Bank*

2.3 IP Address Table

In our design, we use the subnet 10.0.0.0 as our private IP addresses. The public IP address would be in the subnet 200.0.0.0/29. The combination of them would together satisfies the requirement for the bank network.

Location	Department	Subnet	Default Gateway	Public IP	VLAN
HCM	IT	10.0.2.0/24	10.0.2.1	200.0.0.1:1024-65565	20
	HR	10.0.3.0/24	10.0.3.1	200.0.0.1:1024-65565	30
	Maintenance	10.0.4.0/24	10.0.4.1	200.0.0.1:1024-65665	40
	Wireless router	10.0.10.0/24	10.0.10.1	200.0.0.1:1024-65655	-
	Gateway Router	10.0.8.0/24	OSPF	200.0.0.1	-
	Multiplayer Switch	10.0.8.0/24	OSPF	-	-
	DHCP Server	10.0.1.0/24	10.0.1.1	-	10
	Mail Server	10.0.1.0./24	10.0.1.1	200.0.0.3	10
	Database Server 1	10.0.1.0/24	10.0.1.1	-	10
	Database Server 2	10.0.1.0/24	10.0.1.1	-	10
	Web Server	10.0.1.0/24	10.0.1.1	200.0.0.4	10
	Wireless Devices	10.0.10.0/24	10.0.1.2	200.0.0.1:1-65565	-
	ASA 5506	200.0.0.0/29	200.0.1.2	200.0.0.1	-
	ISP Router	200.0.0.0/29	Any	200.0.1.2	-
DN	IT	10.1.2.0/24	10.1.2.1	200.0.0.1:1-65655	20
	HR	10.1.3.0/24	10.1.3.1	200.0.0.1:1-65655	30
	Wireless Router	10.1.10.0/24	10.1.10.1	-	-
	Gateway Router	10.1.4.0/24	OSPF	200.0.0.1:1-65565	-
	Multilayer Switch	10.1.4.0/24	OSPF	-	-
	Service Server	10.1.1.0/24	10.1.1.1	200.0.0.5	10
	Database Server	10.1.1.0/24	10.1.1.1	-	10
	DHCP Server	10.1.1.0/24	10.1.1.1	-	10
	Wireless Devices	10.1.10.0/24	10.1.10.2	200.0.0.1:1-65565	-
NT	IT	10.2.2.0/24	10.2.2.1	200.0.0.1:1-65565	20
	HR	10.2.3.0/24	10.2.3.1	200.0.0.1:1-65565	30
	Wireless Router	10.2.10.0/24	10.2.10.1	-	-
	Gateway Router	10.2.4.0/24	OSPF	200.0.0.1:1-65565	-
	Multilayer Switch	10.2.4.0/24	OSPF	200.0.0.1:1-65565	-
	Service Server	10.2.1.0/24	10.2.1.1	200.0.0.6	10
	Database Server	10.2.1.0/24	10.2.1.1	-	10
	DHCP Server	10.2.1.0/24	10.2.1.1	-	10
	Wireless Devices	10.2.10.0/24	10.2.10.2	200.0.0.1:1-65565	-

We use the subnet 172.16.0.0 as well to illustrate the subnet between three interior router from the headquarter to Nha Trang and Da Nang.

2.4 Network Throughput, Bandwidth and Safety Parameters Calculation

The specification for the upload and download capacity for each type of networking devices is as follow:

- The total upload and download capacity for**server** is **500** MB/day.
- The total upload and download capacity for **workstation** is 100 MB/day.
- WiFi-connected laptop for customers to access about 50 MB/day.

Note that we also take into account the fact that the Bank can grow up to 20% in the next 5 years. Also, The flow of the system reaches its peak with the duration of 3 hours (from 9h to 11h and 15h to 16h)

2.4.1 Network Throughput Calculation

For the headquarter:

- There are 5 servers:
  Throughput: $500 * 5 = 2500$ (MB/day)
- There are 100 servers:
  Throughput: $100 * 100 = 10000$ (MB/day)
- Access points for 100 users:
  Throughput: $100 * 50 = 5000$ (MB/day)
- Total throughput: $2500 + 10000 + 5000 = 17500$ (MB/day)
- Total throughput during peak hours (80% in 3h):
  Throughput: $(17500 * 80\%)/(3 * 3600) \approx 1.2963(MB/s) \approx 10.3704(Mbps)$

For each branch:

- There are 3 servers:
  Throughput: $500 * 3 = 1500$ (MB/day)
- There are 50 servers:
  Throughput: $50 * 100 = 5000$ (MB/day)
- Access points for 50 users:
  Throughput: $50 * 50 = 2500$ (MB/day)
- Total throughput: $1500 + 5000 + 2500 = 9000$ (MB/day)
- Total throughput during peak hours (80% in 3h):
  Throughput: $(9000 * 80\%)/(3 * 3600) \approx 0.667(MB/s) \approx 5.333(Mbps)$

2.4.2 Bandwidth Calculation

For the internal part of each building, Gigabit Ethernet port with capacity of 100/1000 Mbps. All the connections within any office can be handled smoothly.

For the internet connection, we connect from the headquarter router to the Firewall ASA 5506X and from there to the ISP. The ASA 5506X uses gigabit ethernet port 100/1000 Mbps, which means it can handle flow from the isp to provide connection.

Assume we have ADSL2+ standard (ITU G.992.5), which achieves downstream data rates of up to 24 Mbps and upstream data rates of up to 1.5 Mbps.

The total bandwidth for both download and upload: 25.5 Mbps. As we can see, the bandwidth is fully capable of handling the work flow from the bank system.

2.4.3 Safety Parameters Calculation

Within the next 5 years, the bank is going to extend up to 20% for each office (in terms of the number of users, network load, branch extensions, ..). Therefore, we calculate the total amount of throughput with 20% increase to certify if our network would still function as expected.

The throughput with 20% safety parameter:

- ***For the headquarter***: $10.3704 * 1.2 = 12.44448$ (Mbps)
- ***For the branch***: $5.333 * 1.2 \approx 6.34$

2.5 Network Design

The detail design of our BB Bank is described as below:

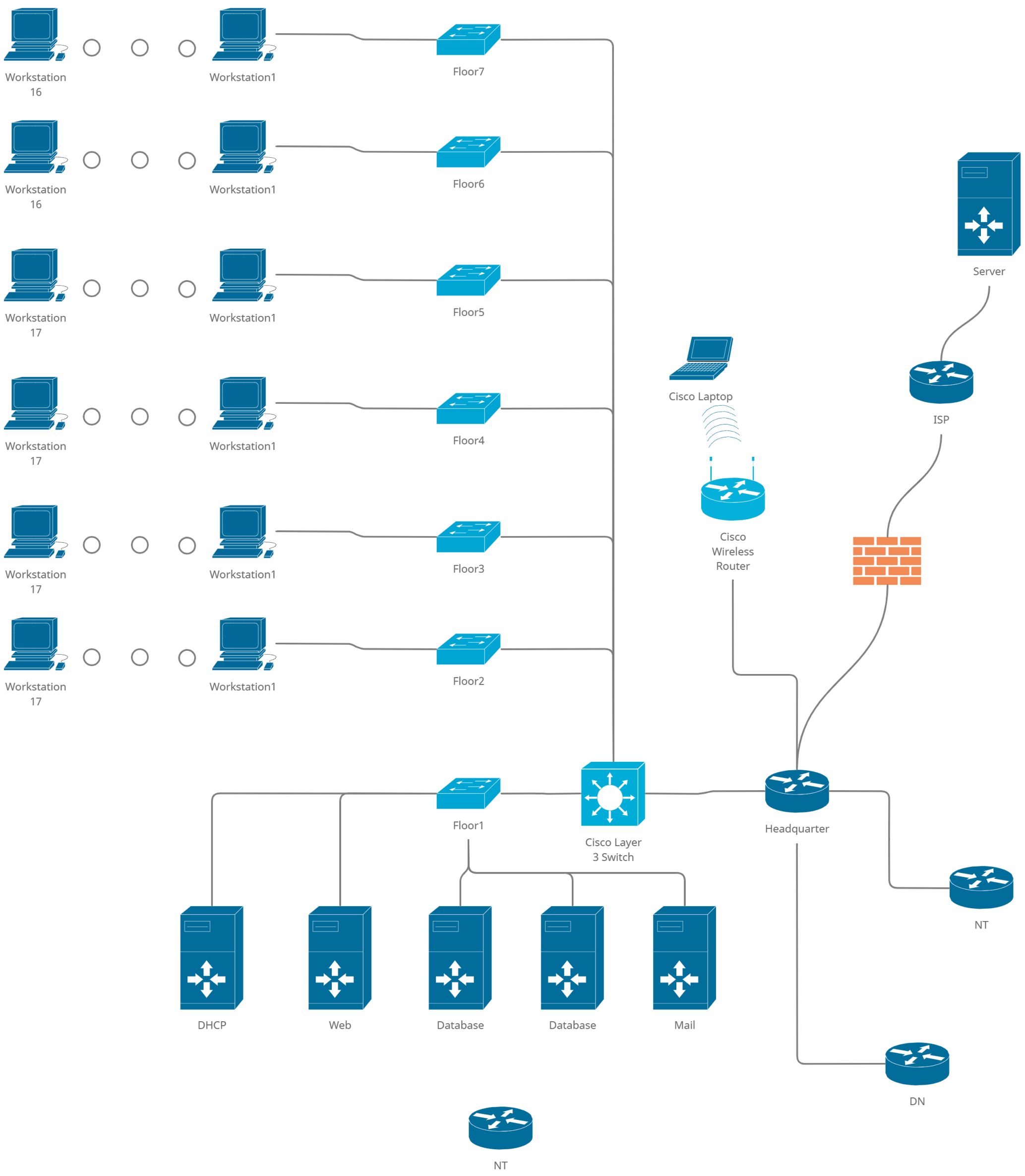


Figure 12: *Headquarter design*

The headquarter consists of seven floors. One the first floor lies the server room where we have 5 servers. One for DHCP, two for internal usage and two for outside service. From floor 2 ti floor 5 there are 17 workstations, the two remaining floors have 16 workstations each. All the workstations add up to the total of 100. Also, we also have wireless connection and establish connectivity to the Internet with the firewall facilitating security measures. If the bank reaches 20% increase in overall size, we still have enough space to fit in 20 more workstations by filling each floor.

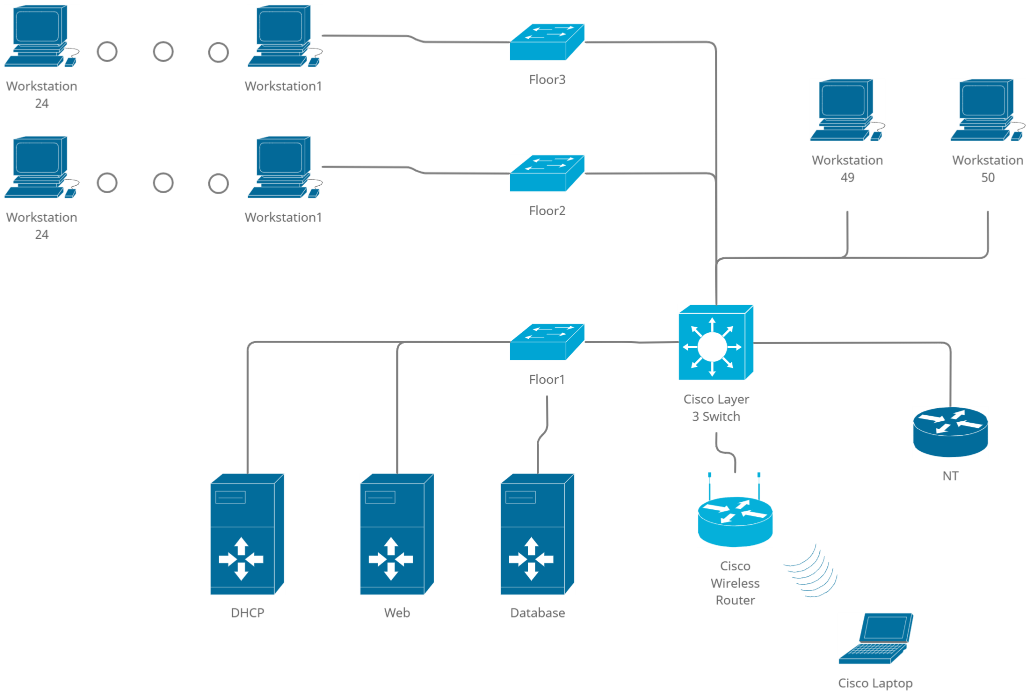


Figure 13: *Branch design*

As for the branch, the design is similar to the headquarter with one minor change. Due to the constraint on the number of networking devices allowed in one branch being only 5, we can only support 48 workstations from two 24-port switches. The remaining 2 workstations are directly connected to the multilayer switch. With this design, if the bank scales up to 20%, we only have to connect more switch to the multilayer switch.

3 PACKET TRACER LOGICAL DESIGN

In the computer network design for a BBB (BB Bank) under construction, three main routers are used to link HCM city headquarter, Nha Trang branch and Da Nang branch together as an WAN. The local network of each building is constructed into multiple VLANs via Floor Switches (FS) and Multilayer Switches (MLS) as follows:

Headquarter: The first floor contains the system of 5 servers, which reside in **VLAN 10**. The 100-workstation system is distributed into the rest 4 floors of 17 workstations each and 2 floors of 16 workstations each. Each floor represents one department of the Headquarter and is further divided into 3 VLANs:

1. **VLAN 20:** For IT function.
2. **VLAN 30:** For HR function.
3. **VLAN 40:** For Maintenance function.

Each floor has its devices connected to a FS, where the 7 FSs are connected to each other via the MLS of the whole building.

NT and DN branches: The first floor contains the system of 3 servers, which reside in **VLAN 10**. The 50-workstation system is distributed into 2 floors of 24 workstations each and the rest 2 workstations are in the first floor. Each floor represents one department of the Branch and is further divided into 2 VLANs:

1. **VLAN 20:** For IT function.
2. **VLAN 30:** For HR function.

Each floor has its devices connected to a FS, where the 3 FSs are connected to each other via the MLS of the whole building.

The reason that we build the VLAN system is to enhance the performance of the whole network. That is when we try to communicate between 2 workstations, without VLANs, the system has to send ARP packets throughout all the building's workstations. This will sometimes make the system overloaded with an excessive number of ARP packets being sent at the same time. However, with VLANs, every time a communication is created, the system will just have to send the ARP packets to the VLANs where the source and destination workstations of the communication belong to. Therefore, the workload of the system is reduced considerably.

As required, we have restricted all the wireless devices from connecting to any local devices except the Service Servers. Besides, wireless devices in one building cannot communicate with wireless devices from another building. Furthermore, the ISP can only communicate with the Service Servers and the wireless devices in the buildings.

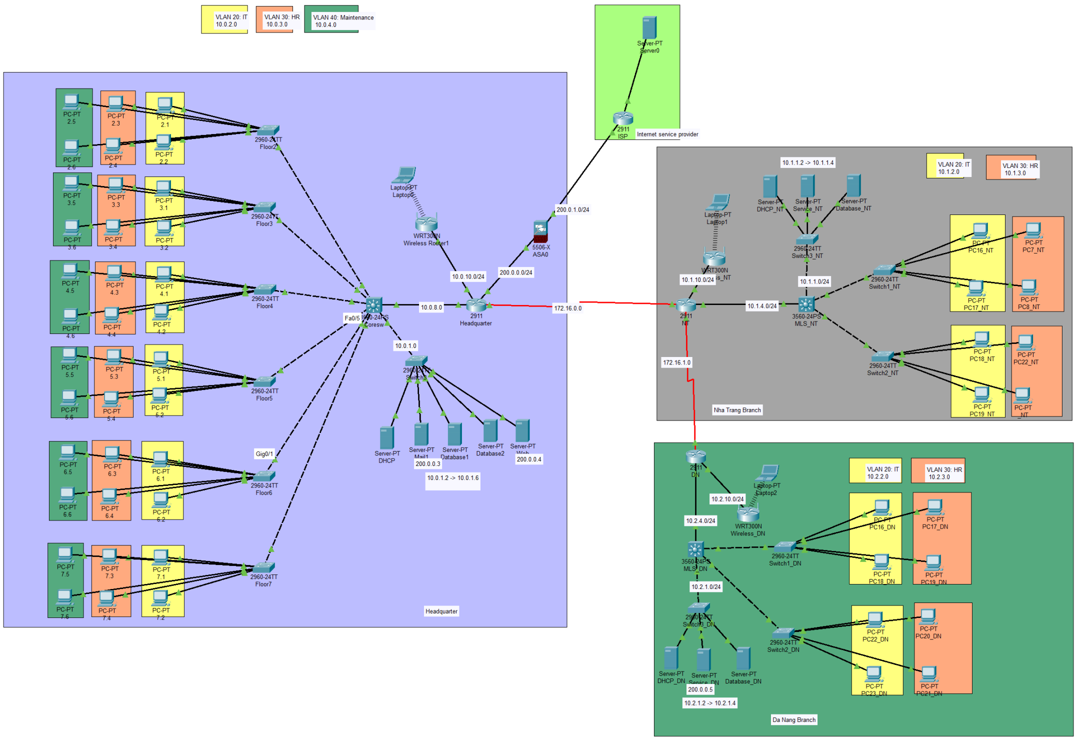


Figure 14: *Packet Tracer Design of BB Bank*

Note: *The Packet Tracer Design doesn't contain all the workstations. However, the working principle and the network structure are still correct.*

3.1 Theoretical basis

The above-mentioned is only raw demonstration of how our Logical Design should look like. However, to fully implement it in Packet Tracer, several theoretical basis need to be grasped:

3.1.1 Address Resolution Protocol

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a Media Access Control or MAC address.

The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa. This is necessary because in IP Version 4 (IPv4), the most common level of Internet Protocol (IP) in use today, an IP address is 32-bits long, but MAC addresses are 48-bits long.

ARP works between network layers 2 and 3 of the Open Systems Interconnection model (OSI model). The MAC address exists on layer 2 of the OSI model, the data link layer, while the IP address exists on layer 3, the network layer.

ARP can also be used for IP over other LAN technologies, such as token ring, fiber distributed data interface (FDDI) and IP over ATM.

ARP works in the following succession of actions:

1. When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address.

2. All operating systems in an IPv4 Ethernet network keep an ARP cache. Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not already exist, then the request for network addresses is sent and ARP is performed.

3. ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

4. Host machines that don't know their own IP address can use the Reverse ARP (RARP) protocol for discovery.

5. An ARP cache size is limited and is periodically cleansed of all entries to free up space; in fact, addresses tend to stay in the cache for only a few minutes. Frequent updates allow other devices in the network to see when a physical host changes their requested IP address. In the cleaning process, unused entries are deleted as well as any unsuccessful attempts to communicate with computers that are not currently powered on.

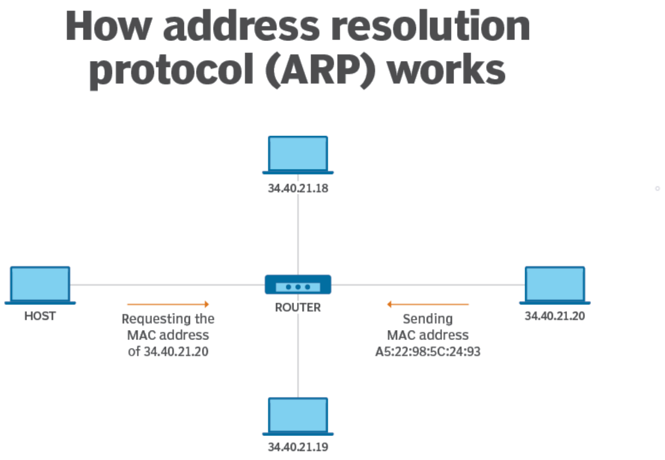

How address resolution protocol (ARP) works
34.40.21.18
HOST
Requesting the MAC address of 34.40.21.20
ROUTER
Sending MAC address A5:22:98:5C:24:93
34.40.21.20
34.40.21.19

Figure 15: *How ARP works*

3.1.2 VLAN Trunking Protocol

VLAN Trunking Protocol or VTP is a proprietary protocol from Cisco that allows networks to send network functionality through all of the switches in a domain. This technique eliminates the need for multiple configurations for VLANs throughout the system.

VTP, which is available with Cisco Catalyst products, provides efficient ways to send a VLAN through every switch. There's also the option of VLAN pruning which will avoid sending traffic through some switches. Users can make these systems pruning eligible or pruning ineligible.

Usually, larger scale networks may need to be limited in terms of which switches will act as the VLAN servers. VTP offers various options for recovery after a crash or for efficiently serving up redundant network traffic.

In general, the idea of VLAN trunking is similar to other kinds of IT trunking. By locating resources in specific arrangements, data has to do less work to get to specific parts of a network system, or administrators need to do less work to accommodate these data transfers. The trunks between switches are part of this efficiency mechanism which allows for faster and more efficient network traffic.

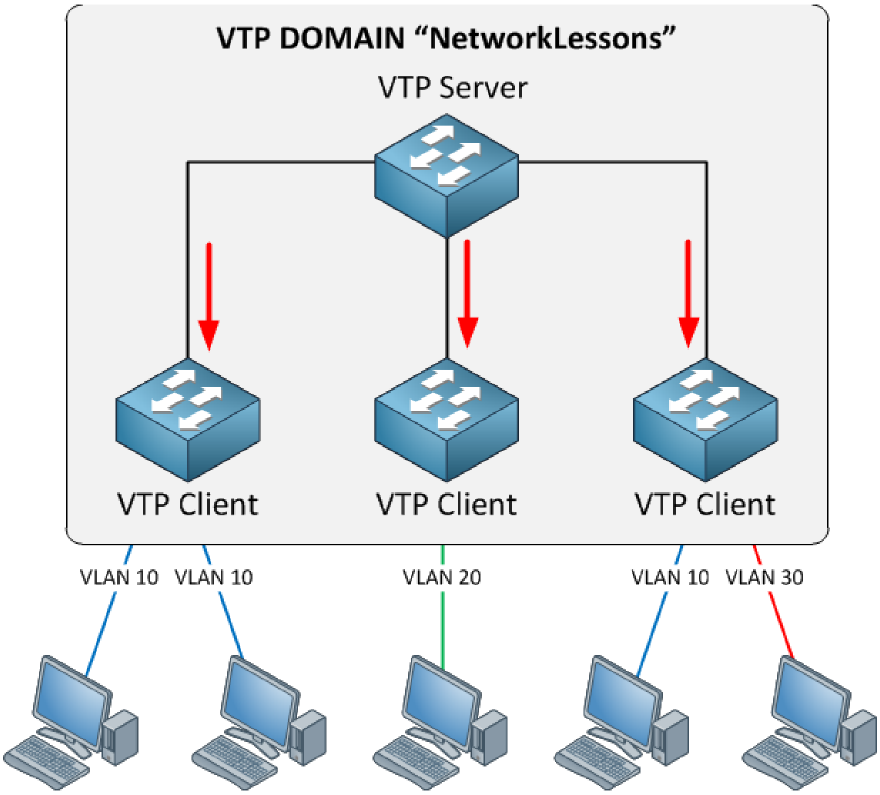


Figure 16: *General switch network for VLAN Trunking Protocol*

3.1.3 Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol or DHCP is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints. The other information includes: subnet mask, default gateway address, domain name server (DNS) and other pertinent configuration parameters.

The primary reason DHCP is needed is to simplify the management of IP addresses on networks. No two hosts can have the same IP address, and configuring them manually will likely lead to errors. Even on small networks manually assigning IP addresses can be confusing, particularly with mobile devices that require IP addresses on a non-permanent basis. Also, most users aren't technically proficient enough to locate the IP address information on a computer and assign it. Automating this process makes life easier for users and the network administrator.

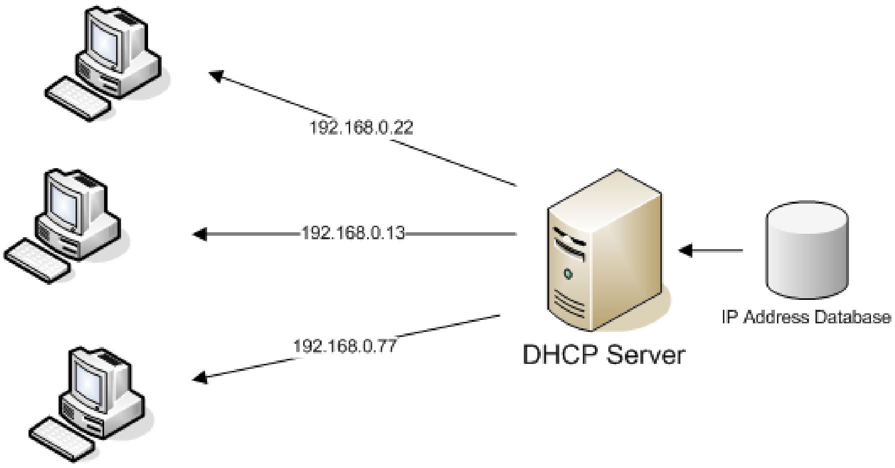


Figure 17: *IP address allocation using DHCP*

When working with DHCP, it's important to understand all of the components:

- **DHCP server:** A networked device running the DCHP service that holds IP addresses and related configuration information. This is most typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** The endpoint that receives configuration information from a DHCP server. This can be a computer, mobile device, IoT endpoint or anything else that requires connectivity to the network. Most are configured to receive DHCP information by default.
- **IP address pool:** The range of addresses that are available to DHCP clients. Addresses are typically handed out sequentially from lowest to highest.
- **Subnet:** IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.

- **Lease:** The length of time for which a DHCP client holds the IP address information. When a lease expires, the client must renew it.
- **DHCP relay:** A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. This can be used to centralize DHCP servers instead of having a server on each subnet.

3.1.4 Network Address Translation

The original design for the Internet required every organization to ask for, and receive, one or more registered classful IPv4 network numbers. The people administering the program ensured that none of the IP networks were reused. As long as every organization used only IP addresses inside its own registered network numbers, IP addresses would never be duplicated, and IP routing could work well.

Connecting to the Internet using only a registered network number, or several registered network numbers, worked well for a while. In the early to mid-1990s, it became apparent that the Internet was growing so fast that all IP network numbers would be assigned by the mid-1990s! Concern arose that the available networks would be completely assigned, and some organizations would not be able to connect to the Internet.

Many short-term solutions to the addressing problem were suggested, but three standards worked together to solve the problem. Two of the standards work closely together: Network Address Translation (NAT) and private addressing. These features together allow many organizations to use the same unregistered IPv4 network numbers internally—and still communicate well with the Internet. The third standard, classless interdomain routing (CIDR), allows ISPs to reduce the wasting of IPv4 addresses by assigning a company a subset of a network number rather than the entire network. CIDR also can allow Internet service providers (ISP) to summarize routes such that multiple Class A, B, or C networks match a single route, which helps reduce the size of Internet routing tables .

NAT achieves its goal by using a valid registered IP address to represent the private address to the rest of the Internet. The NAT function changes the private IP addresses to publicly registered IP addresses inside each IP packet.

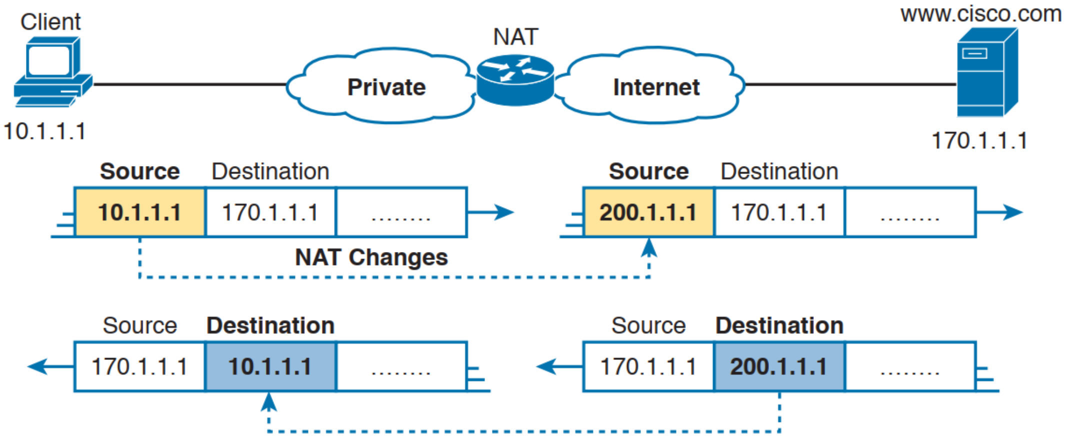
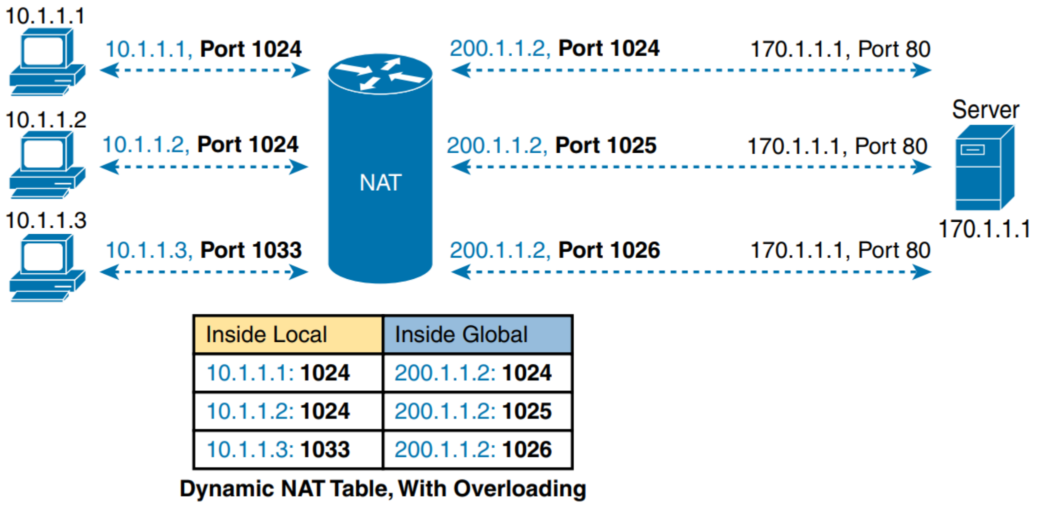


Figure 18: *NAT IP Address Swapping: Private Addressing*

Some networks need to have most, if not all, IP hosts reach the Internet. If that network uses private IP addresses, the NAT router needs a very large set of registered IP addresses. With static NAT, for each private IP host that needs Internet access, you need a publicly registered IP address, completely defeating the goal of reducing the number of public IPv4 addresses needed for that organization. Dynamic NAT lessens the problem to some degree, because every single host in an internetwork should seldom need to communicate with the Internet at the same time. However, if a large percentage of the IP hosts in a network will need Internet access throughout that company's normal business hours, NAT still requires a large number of registered IP addresses, again failing to reduce IPv4 address consumption.

The NAT Overload feature, also called Port Address Translation (PAT), solves this problem. Overloading allows NAT to scale to support many clients with only a few public IP addresses.



Inside Local	Inside Global
10.1.1.1: 1024	200.1.1.2: 1024
10.1.1.2: 1024	200.1.1.2: 1025
10.1.1.3: 1033	200.1.1.2: 1026

Dynamic NAT Table, With Overloading

Figure 19: *NAT Overload (PAT)*

3.1.5 Access List Control (ACL)

IPv4 access control lists (IP ACL) give network engineers a way to identify different types of packets. To do so, the ACL configuration lists values that the router can see in the IP, TCP, UDP, and other headers. For example, an ACL can match packets whose source IP address is 1.1.1.1, or packets whose destination IP address is some address in subnet 10.1.1.0/24, or packets with a destination port of TCP port 23 (Telnet).

Cisco routers can apply ACL logic to packets at the point at which the IP packets enter an interface, or the point at which they exit an interface. In other words, the ACL becomes associated with an interface and for a direction of packet flow (either in or out). That is, the ACL can be applied inbound to the router, before the router makes its forwarding (routing) decision, or outbound, after the router makes its forwarding decision and has determined the exit interface to use.

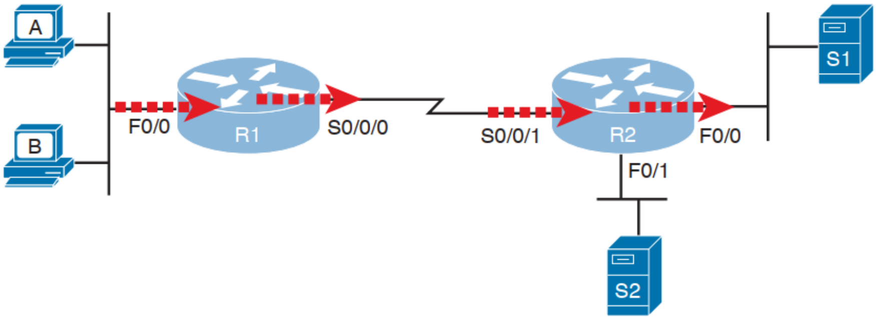


Figure 20: *Locations to Filter Packets from Hosts A and B Going Toward Server S1*

Cisco IOS has supported IP ACLs since the early days of Cisco routers. Beginning with the original standard numbered IP ACLs in the early days of IOS.

- Standard numbered ACLs (1–99).
- Standard numbered ACLs (1–99).
- Additional ACL numbers (1300–1999 standard, 2000–2699 extended).
- Named ACLs.
- Improved editing with sequence numbers.

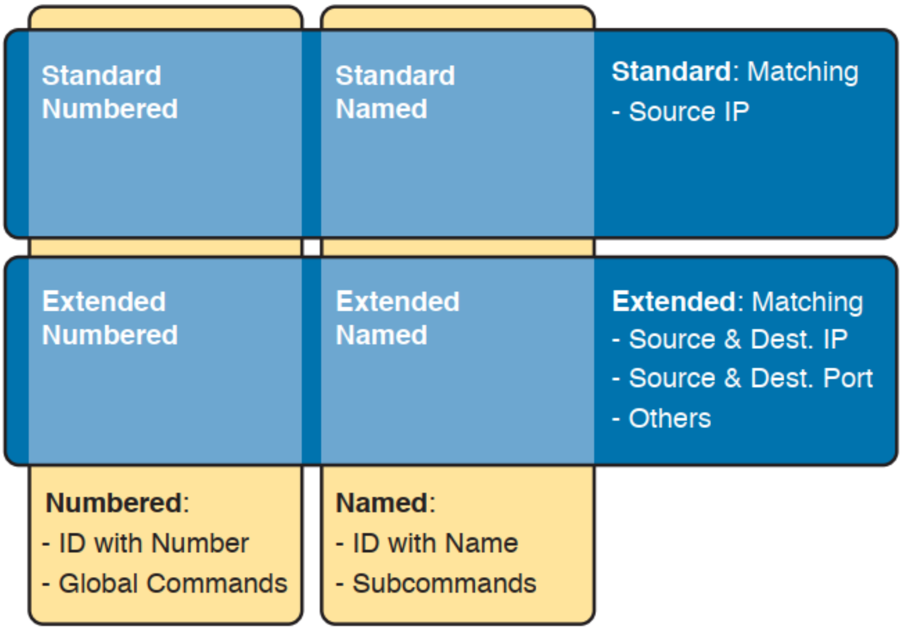


Figure 21: *Comparisons of IP ACL Types*

In this assignment, we will focus on the extended numbered ACL. Extended ACLs differ from standard ACLs mostly because of the larger variety of packet header fields that can be used to match a packet. One extended ACL statement can examine multiple parts of the packet headers, requiring that all the parameters be matched correctly to match that one ACL statement. That powerful matching logic makes extended access lists both more useful and more complex than standard IP ACLs .

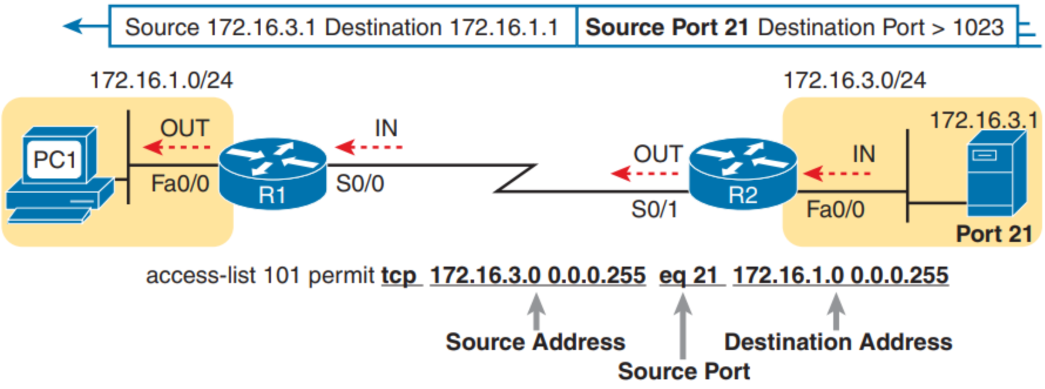
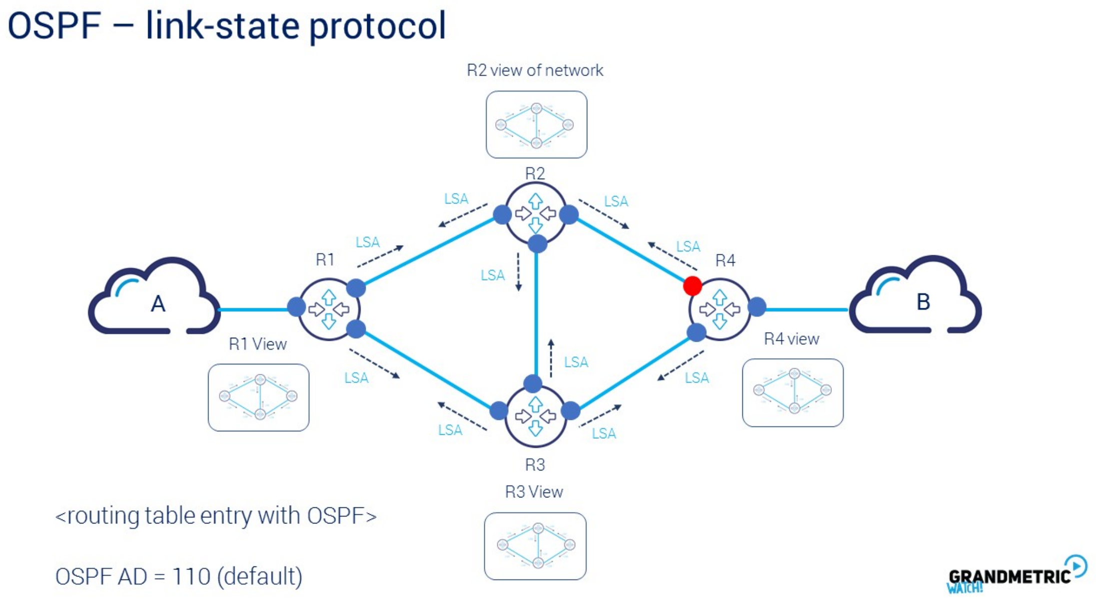

Source 172.16.3.1 Destination 172.16.1.1
Source Port 21 Destination Port > 1023
172.16.1.0/24
172.16.3.0/24
PC1
OUT
Fa0/0
R1
IN
S0/0
OUT
S0/1
R2
IN
Fa0/0
172.16.3.1
Port 21
access-list 101 permit tcp 172.16.3.0 0.0.0.255 eq 21 172.16.1.0 0.0.0.255
Source Address
Source Port
Destination Address

Figure 22: *Filtering Packets Based on Source Port*

3.1.6 Open Shortest Path First

The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.



OSPF – link-state protocol

<routing table entry with OSPF>

OSPF AD = 110 (default)

Figure 23: *OSPF Protocol*

The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link state routing protocol is unsuitable for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS.

Each OSPF router distributes information about its local state (usable interfaces and reach-able neighbors, and the cost of using each interface) to other routers using a Link State Advertisement (LSA) message. Each router uses the received messages to build up an identical database that describes the topology of the AS.

From this database, each router calculates its own routing table using a Shortest Path First (SPF) or Dijkstra algorithm. This routing table contains all the destinations the routing protocol knows about, associated with a next hop IP address and outgoing interface.

- The protocol recalculates routes when network topology changes, using the Dijkstra algorithm, and minimises the routing protocol traffic that it generates.
- It provides support for multiple paths of equal cost.
- It provides a multi-level hierarchy (two-level for OSPF) called "area routing," so that information about the topology within a defined area of the AS is hidden from routers outside this area. This enables an additional level of routing protection and a reduction in routing protocol traffic.
- All protocol exchanges can be authenticated so that only trusted routers can join in the routing exchanges for the AS.

3.2 Switch and VLAN configuration

1. Firstly, we need to create a pool of VLANs in the MLS by applying to each of the VLANs in local network system the following snippet of codes:

```
! In configure terminal of MLS

! For each VLAN to create
vlan VLAN_NUMBER
name VLAN_NAME
exit
```

2. Secondly, we assign IP address to each VLAN:

```
! In configure terminal of MLS

! For each VLAN to assign IP address
interface vlan VLAN_NUMBER
ip address VLAN_IP VLAN_IP_MASK
no shutdown
exit
```

3. Thirdly, we configure VTP and trunk ports so that the MLS can distribute its pool of VLANs to the other FSs. This is done by turning the MLS into an VTP server:

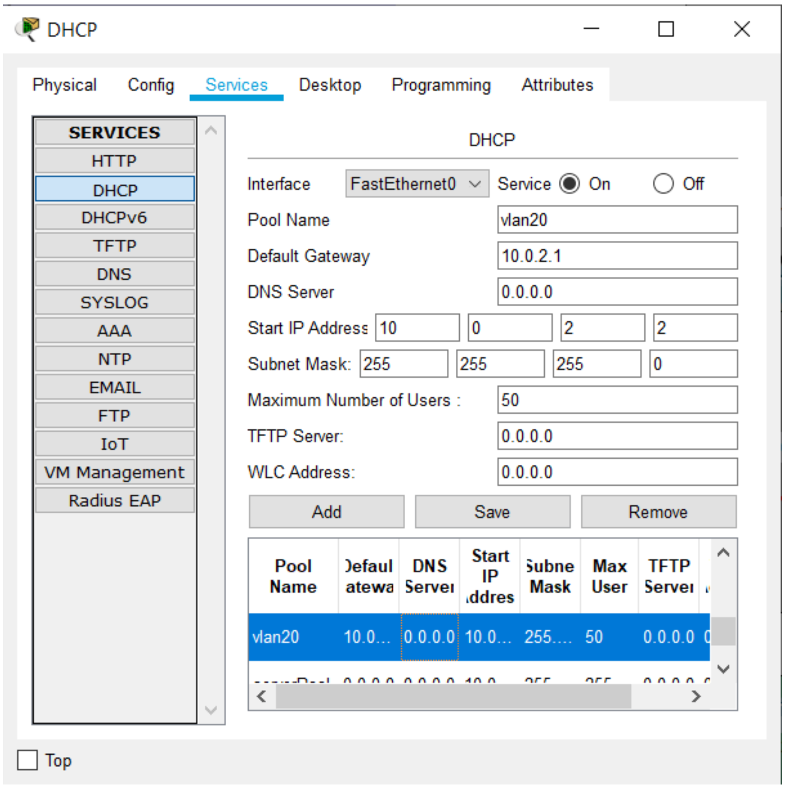
```
! In MLS

! In configure terminal
vtp mode server
vtp domain DOMAIN_NAME


! In each interface that connects to FS.
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. Fourthly, we setup VTP on the FSs and assign VLANs to appropriate ports:

```
! In each FS

! In configure terminal
vtp mode client
vtp domain DOMAIN_NAME

! In the interface that connects to MLS
switchport mode trunk
```

```
! In each interface that connects to each workstation
switchport mode access
switchport access vlan VLAN_NUMBER
```

5. Fifthly, we configure an DHCP server for our local workstations. This is done using GUI provided by Cisco Packet Tracer:



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name: vlan20

Default Gateway: 10.0.2.1

DNS Server: 0.0.0.0

Start IP Address: 10 0 2 2

Subnet Mask: 255 255 255 0

Maximum Number of Users : 50

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	)efaul atewa	DNS Serve	Start IP ddres	Subne Mask	Max User	TFTP Serve
vlan20	10.0...	0.0.0.0	10.0...	255....	50	0.0.0.0

Figure 24: *DHCP server configuration*

6. From step 5, we have obtained a pool of DHCP IP addresses. However, it is not ready to be assigned yet since we must configure DHCP relay on MLS by specifying the server as an IP helper:

```
! In configure terminal of MLS

! In each VLAN interface.
ip helper-address DHCP_SERVER_IP_ADDRESS
```

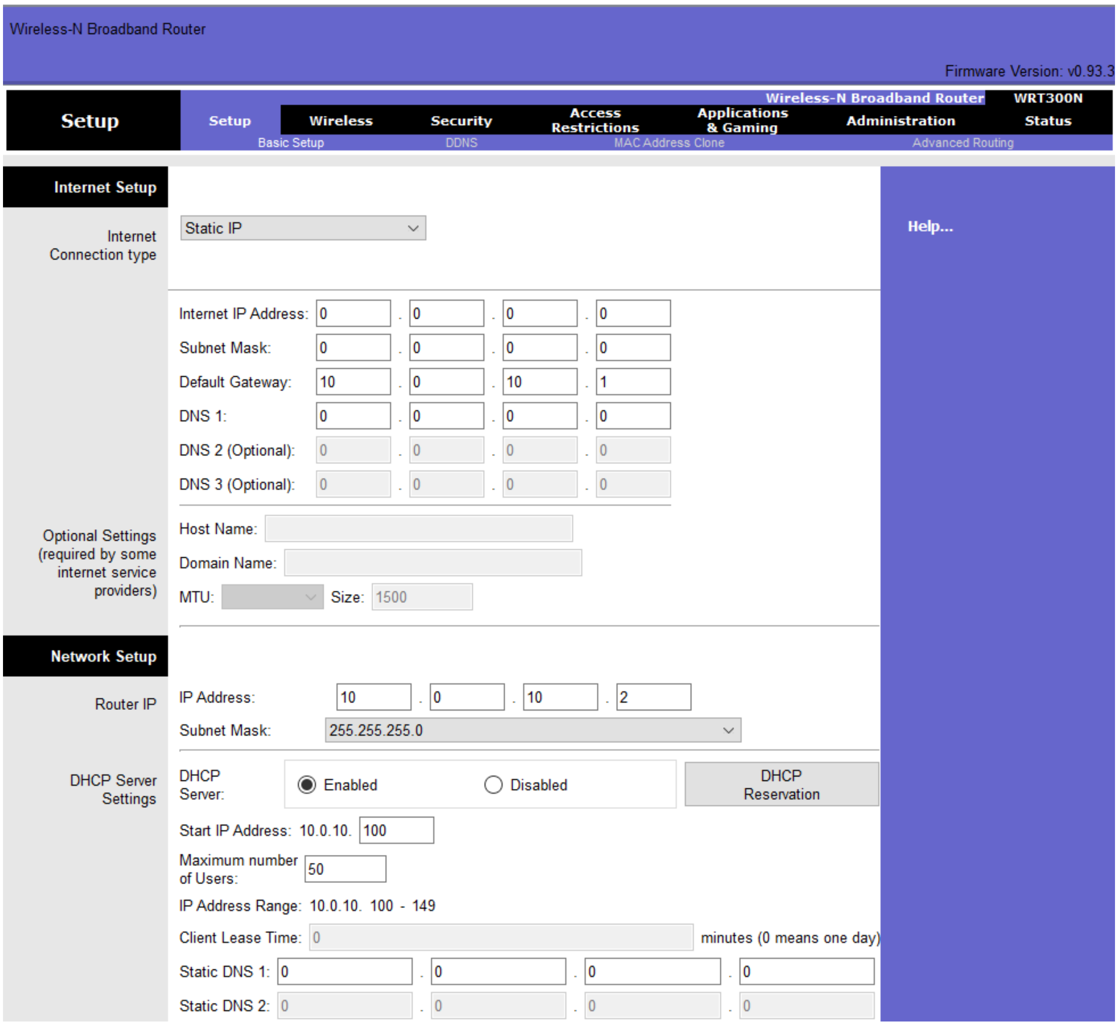
7. Finally, we enable IP routing on the MLS so that the workstations on different VLANs can

communicate to each other. The configuration of IP routing for the MLS will be described in more detail in the OSPF Protocol Configuration.

Providing that the OSPF Protocol of the network is implemented, then our VLANs can communicate to each other freely.

3.3 Wireless Router configuration

The wireless router we are using does not have CLI so we have to configure it on its GUI through uisng Telnet protocol. In the GUI, we set the default gateway, the router IP and alo enabled DHCP. The wifi will use WPA2-PSK standard to set the password for the wifi.



Internet Setup

Internet Connection type: Static IP

Internet IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Default Gateway: 10 . 0 . 10 . 1
DNS 1: 0 . 0 . 0 . 0
DNS 2 (Optional): 0 . 0 . 0 . 0
DNS 3 (Optional): 0 . 0 . 0 . 0

Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU: Size: 1500

Network Setup

Router IP
IP Address: 10 . 0 . 10 . 2
Subnet Mask: 255.255.255.0

DHCP Server Settings
DHCP Server: ● Enabled ○ Disabled
DHCP Reservation
Start IP Address: 10.0.10. 100
Maximum number of Users: 50
IP Address Range: 10.0.10. 100 - 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0

Figure 25: *Wireless Router Configuration*

3.4 OSPF Protocol Configuration

To implement OSPF Protocol, we first register all the routers (including the MLSs) into the OSPF network. For each router to be registered, we have to specify all the sub-networks that are directly connected to that router. This is done via the following snippet of codes:

```
! In configure terminal of Router
router ospf OSPF_NUMBER

! For each network that is directly connected to the router
network SUBNET_ADDRESS SUBNET_WILDCARD area AREA_NUMBER
```

Here, the OSPF number of the whole system is 10 and the area number of all the routers' sub-networks is 0.

Each time a network is specified as a mutual sub-network of the 2 neighboring routers, there should be a notification yielded by Packet Tracer to confirm the setting-up of the OSPF network.

3.5 Security Configuration

3.5.1 Configuring Cisco ASA 5506

1. In our design we use two GigabitEthernet port namedly 1/1 connected to the interior router located in headquarter and 1/2 connected to the ISP router. First we need to set the ip address to each one, nameif and their security level. Traffic from one that with lower security level would obviously not be able to travel to those with higer security level.

```
! In configure terminal of MLS

interface g1/1
ip address 200.0.0.2 255.255.255.248
nameif inside
security-level 100

interface g1/2
ip address 200.0.1.1 255.255.255.254
nameif outside
security-level 100
```

2. Then we need to create the firewall policy and apply its to all the interfaces. In here, we will demonstrate the firewall to allow ICMP packets to pass through the firewall.

```
! In configure terminal of MLS
class-map inspection_default
match default-inspection-traffic

policy-map global_policy
class inspection_default
```

```
inspect icmp

service-policy global_policy global
```

3. Finally we need to enable OSPF route on the firewall and set its default gateway to the ISP router. Be noticed that in the ASA configuration, the network command in here takes a subnet mask not wildcard like in normal router.

```
 ! In configure terminal of MLS
router ospf 10
network 200.0.0.0 255.0.0.0 area 0

ip route 0.0.0.0 0.0.0.0 200.0.1.2
```

3.5.2 Configuring Acess List Control (ACL)

Note: In the access control list, the rules applied from a top-down fashion and there is a hidden deny all ip at the bottom of the list. Therefore if the packets match no rule, they will automatically be dropped.

3.5.2.a Headquarter Router

1. In our design, there will be access list control implemented on three interior routers. First one on the headquarter, we will have 4 access lists namedly 101,102,103,104. 101 will prevent the wifi from reaching local connection but it still can access other service servers and the Internet. Furthermore, as other branches also have wifi connection so we have to ensure that those traffic cannot reach other LANs. The access-list will be implemented on interface GigabitEthernet0/1, router inbound.

```
! In configure terminal of MLS
access-list 101 deny ip 10.0.10.0 0.0.0.255 10.0.2.0 0.0.0.255
access-list 101 deny ip 10.0.10.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 deny ip 10.0.10.0 0.0.0.255 10.0.4.0 0.0.0.255
access-list 101 deny ip 10.0.10.0 0.0.0.255 host 10.0.1.2
access-list 101 deny ip 10.0.10.0 0.0.0.255 host 10.0.1.4
access-list 101 deny ip 10.0.10.0 0.0.0.255 host 10.0.1.5
access-list 101 permit ip any any

interface G0/1
ip access-group 101 in
```

2. Implement access list to block any traffic from the headquarter wifi to going out of the serial interface 0/3/0.

```
! In configure terminal of MLS
```

```
access-list 102 deny ip 10.0.10.0 0.0.0.255 any
access-list 102 permit ip any any

interface S0/3/0
ip access-group 102 out
```

3. Implement access list to block any traffic from the Nha Trang wifi to going in of the serial interface. 0/3/0.

```
! In configure terminal of MLS
access-lsit 103 deny ip 10.1.10.0 0.0.0.255 10.0.0.0 0.0.255.255
access-lsit 103 permit ip any any

interface S0/3/0
ip access-group 103 in
```

4. Implement access list to block any traffic from the Internet to going in of the local network.

```
! In configure terminal of MLS
access-list 104 deny ip any 10.0.0.0 0.255.255.255
access-list 104 deny ip any 172.16.0.0 0.0.255.255
access-list 104 any any (500 match(es))

interface G0/2
ip access-group 104 in
```

3.5.2.b Nha Trang Router

1. As the same logic we use when configuring the router on the headquarter, we apply the same thing to the router on Nha Trang with the rule that the wifi guess cannot reach the local connection but still has the connection to the Internet and service servers.

```
! In configure terminal of MLS
access-list 101 deny ip 10.1.10.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 101 deny ip 10.1.10.0 0.0.0.255 10.1.3.0 0.0.0.255
access-list 101 deny ip 10.1.10.0 0.0.0.255 10.1.4.0 0.0.0.255
access-list 101 deny ip 10.1.10.0 0.0.0.255 host 10.1.1.2
access-list 101 deny ip 10.1.10.0 0.0.0.255 host 10.1.1.4
access-list 101 permit ip any any

interface G0/1
ip access-group 101 in
```

2. Implementing access list 102 to block any traffic from the headquarter wifi reaching other LANs.

```
! In configure terminal of MLS
access-list 102 deny ip 10.1.10.0 0.0.0.255 any
access-list 102 permit ip any any

interface S0/3/1
ip access-group 102 out
```

3. Implementing access list 103 to block any traffic from the headquarter wifi reaching other LANs.

```
! In configure terminal of MLS
access-list 103 deny ip 10.2.10.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 103 deny ip 10.2.10.0 0.0.0.255 10.1.3.0 0.0.0.255
access-list 103 deny ip 10.2.10.0 0.0.0.255 host 10.1.1.2
access-list 103 deny ip 10.2.10.0 0.0.0.255 host 10.1.1.4
access-list 103 deny ip 10.2.10.0 0.0.0.255 10.0.2.0 0.0.0.255
access-list 103 deny ip 10.2.10.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 103 deny ip 10.2.10.0 0.0.0.255 10.0.4.0 0.0.0.255
access-list 103 deny ip 10.2.10.0 0.0.0.255 host 10.0.1.2
access-list 103 deny ip 10.2.10.0 0.0.0.255 host 10.0.1.4
access-list 103 deny ip 10.2.10.0 0.0.0.255 host 10.0.1.5
access-list 103 permit ip any any

interface G0/1
ip access-group 103 in
```

3.5.2.c Da Nang Router

1. As the same logic we use when configuring the router on the headquarter, we apply the same thing to the router on Da Nang with the rule that the wifi guess cannot reach the local connection but still has the connection to the Internet and service servers.

```
! In configure terminal of MLS
deny ip 10.2.10.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 101 deny ip 10.2.10.0 0.0.0.255 10.2.3.0 0.0.0.255
access-list 101 deny ip 10.2.10.0 0.0.0.255 host 10.2.1.2
access-list 101 deny ip 10.2.10.0 0.0.0.255 host 10.2.1.4
access-list 101 permit ip any any

interface G0/2
ip access-group 101 in
```

3.5.3 Network Address Translation (NAT)

3.5.3.a NAT over PAT

As the only public addresses that need to be static and well-known are the service server's IPs. The best practice way is to choose PAT (Port Address Translation). As we have a handful of port numbers ranging from 1 to 65565, we could take advanatage of the unused ones. In our design any host except service server public IP would be using the same public address 200.0.0.1 with different assigned port.
Furthermore, as the ISP router is only connected to the headquarter router, it would be an ideal design to choose the headquarter router as the one that need to do the translation work.

```
! In configure terminal of MLS
interface G0/0
ip nat inside
interface G0/1
ip nat inside
interface G0/3
ip nat inside

interface G0/2
ip nat outside

ip nat inside source list 1 interface G0/2 overload
```

3.5.3.b Static NAT

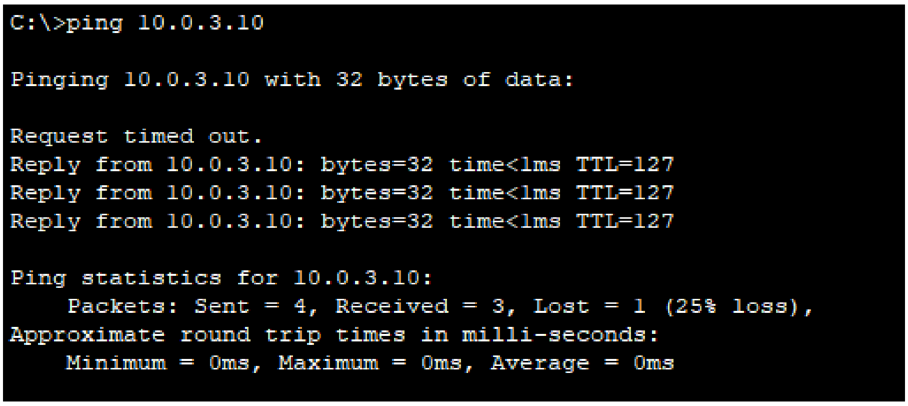
The service servers need static public IP address so that it can be known by outside users. Therefore, we need to have static NATs only for those. In Cisco system, the static NAT is preferred over dynamic ones. So if there are two rules which suit the inside source, Cisco will simply choose the static NAT.

```
! In configure terminal of MLS
ip nat inside source static 10.0.1.3 200.0.0.3

ip nat inside source static 10.0.1.6 200.0.0.4

ip nat inside source static 10.1.1.3 200.0.0.5

ip nat inside source static 10.2.1.3 200.0.0.6
```

4 TESTING AND RESULTS

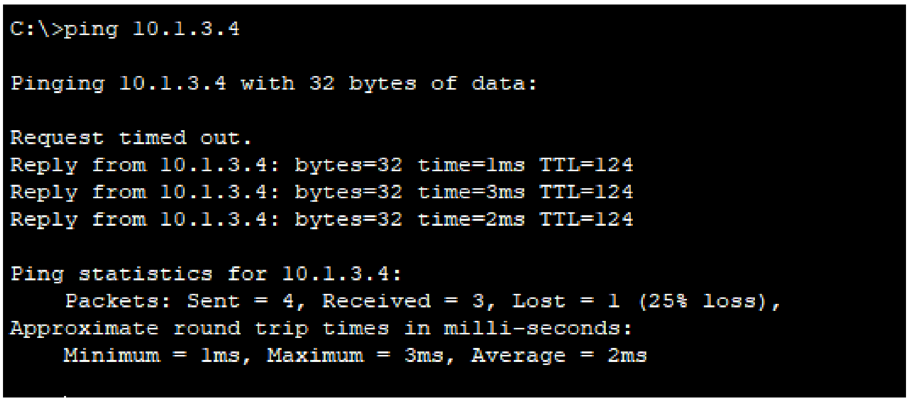
4.1 Test with Ping

As we have implemented various configurations on the router to access and to restrict access. All the status of the ping when we do it for the **first time** can be shown in the figures below:



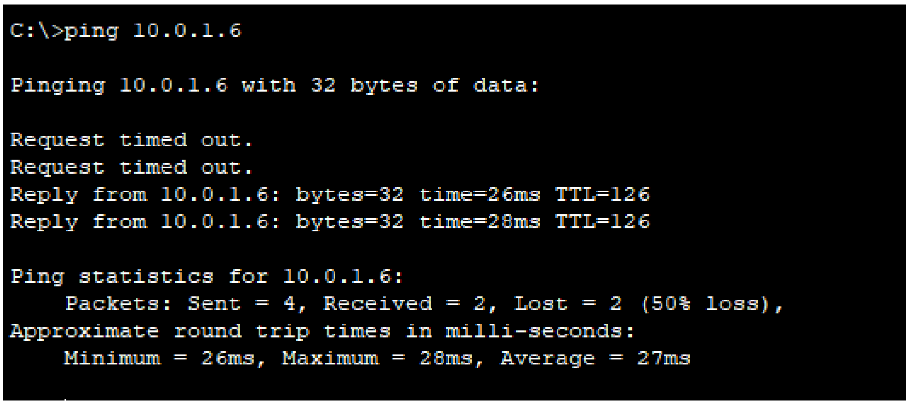
```
C:\>ping 10.0.3.10

Pinging 10.0.3.10 with 32 bytes of data:

Request timed out.
Reply from 10.0.3.10: bytes=32 time<1ms TTL=127
Reply from 10.0.3.10: bytes=32 time<1ms TTL=127
Reply from 10.0.3.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.3.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 26: Ping from a workstation to other workstation with different VLAN



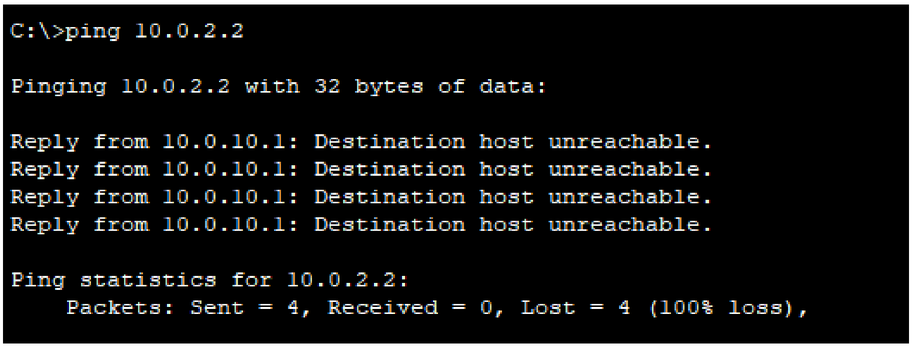
```
C:\>ping 10.1.3.4

Pinging 10.1.3.4 with 32 bytes of data:

Request timed out.
Reply from 10.1.3.4: bytes=32 time=1ms TTL=124
Reply from 10.1.3.4: bytes=32 time=3ms TTL=124
Reply from 10.1.3.4: bytes=32 time=2ms TTL=124

Ping statistics for 10.1.3.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

Figure 27: Ping from a workstation in HCM to workstation in NT with different VLAN



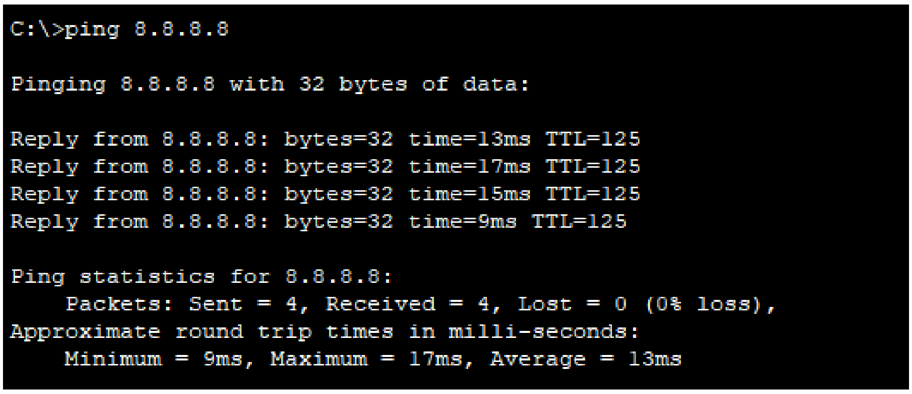
```
C:\>ping 10.0.1.6

Pinging 10.0.1.6 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.0.1.6: bytes=32 time=26ms TTL=126
Reply from 10.0.1.6: bytes=32 time=28ms TTL=126

Ping statistics for 10.0.1.6:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 28ms, Average = 27ms
```

Figure 28: Ping from Guest device to Server service



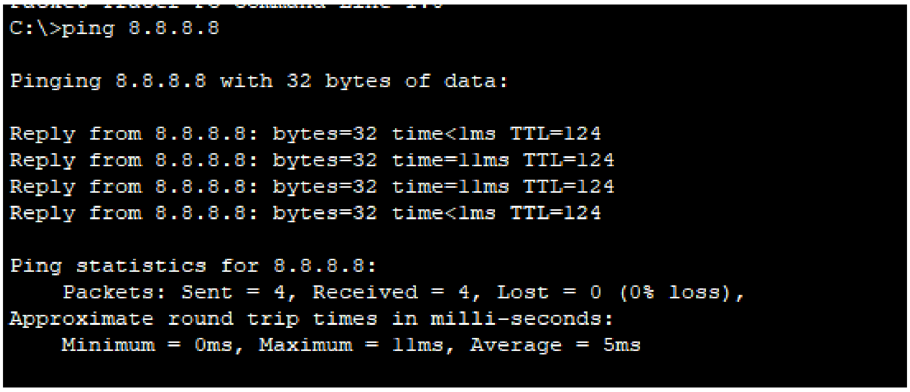
```
C:\>ping 10.0.2.2

Pinging 10.0.2.2 with 32 bytes of data:

Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.

Ping statistics for 10.0.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 29: Ping from Guest device to local network



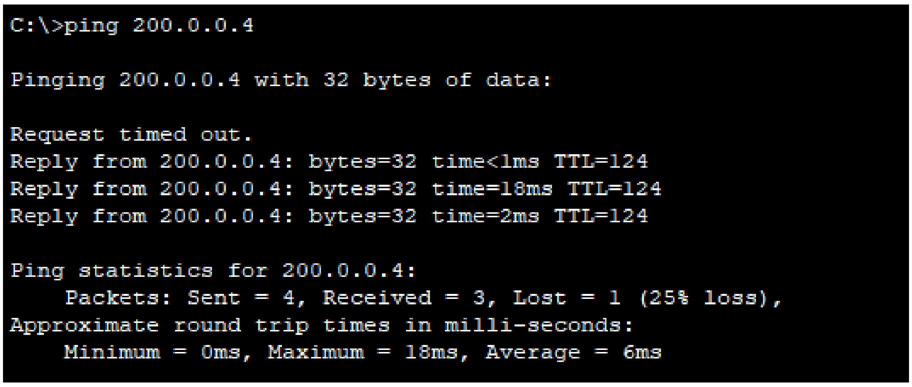
```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=13ms TTL=125
Reply from 8.8.8.8: bytes=32 time=17ms TTL=125
Reply from 8.8.8.8: bytes=32 time=15ms TTL=125
Reply from 8.8.8.8: bytes=32 time=9ms TTL=125

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 17ms, Average = 13ms
```

Figure 30: Ping from Guest device to ISP



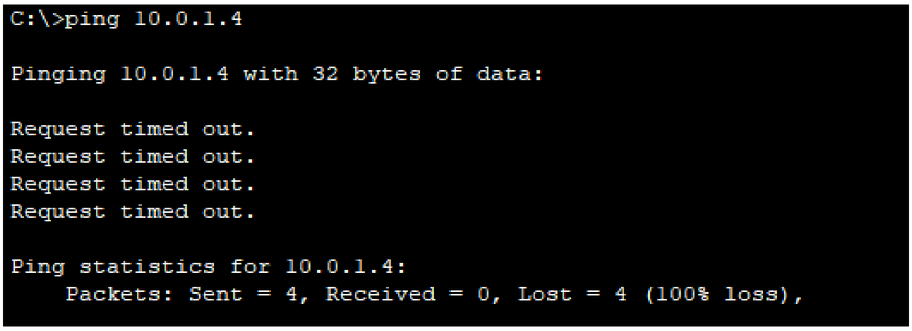
```
Packet Tracer PC Command Line 1.0
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=124
Reply from 8.8.8.8: bytes=32 time=11ms TTL=124
Reply from 8.8.8.8: bytes=32 time=11ms TTL=124
Reply from 8.8.8.8: bytes=32 time<1ms TTL=124

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms
```

Figure 31: Ping from Workstation to ISP



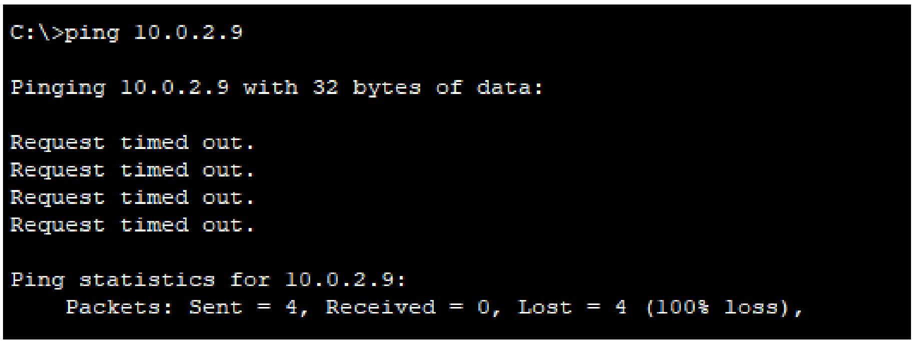
```
C:\>ping 200.0.0.4

Pinging 200.0.0.4 with 32 bytes of data:

Request timed out.
Reply from 200.0.0.4: bytes=32 time<1ms TTL=124
Reply from 200.0.0.4: bytes=32 time=18ms TTL=124
Reply from 200.0.0.4: bytes=32 time=2ms TTL=124

Ping statistics for 200.0.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 6ms
```

Figure 32: Ping from ISP to Server Service



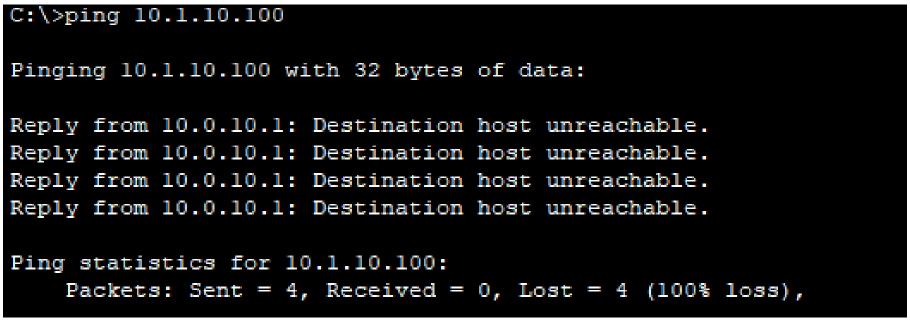
```
C:\>ping 10.0.1.4

Pinging 10.0.1.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 33: Ping from ISP to Server Database



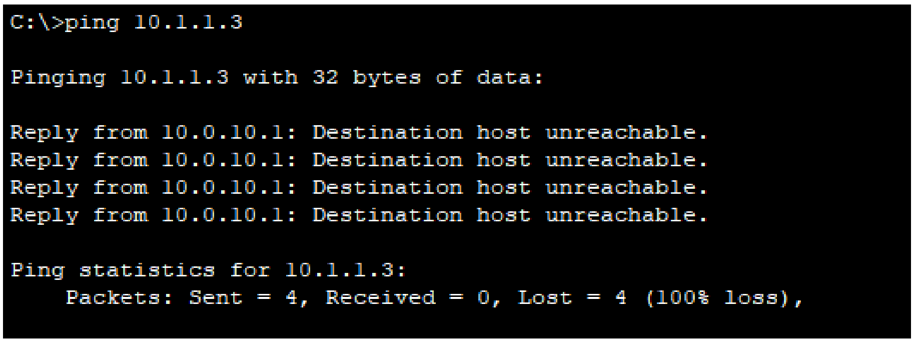
```
C:\>ping 10.0.2.9

Pinging 10.0.2.9 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 34: Ping from ISP to workstation



```
C:\>ping 10.1.10.100

Pinging 10.1.10.100 with 32 bytes of data:

Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.

Ping statistics for 10.1.10.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

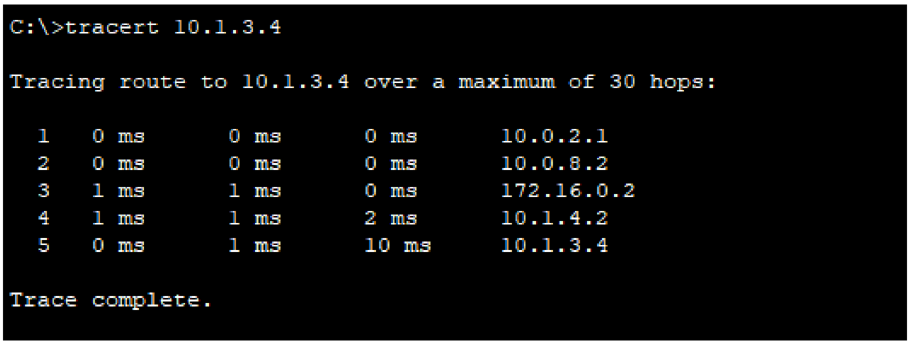
Figure 35: Ping from Guest to Guest in other branch



```
C:\>ping 10.1.1.3

Pinging 10.1.1.3 with 32 bytes of data:

Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.
Reply from 10.0.10.1: Destination host unreachable.

Ping statistics for 10.1.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

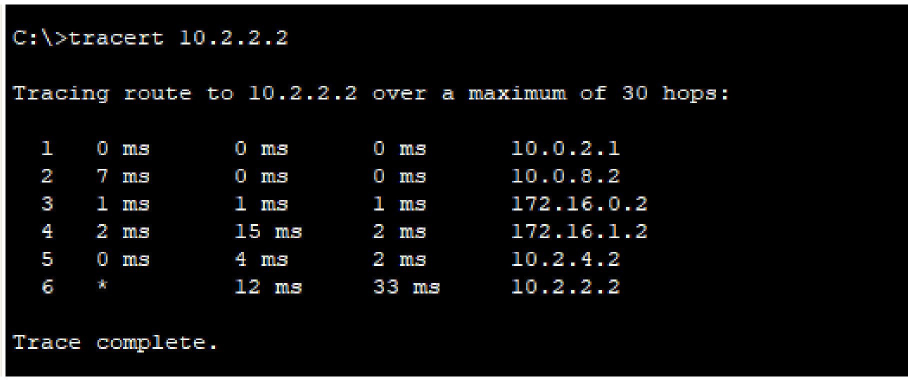
Figure 36: Ping from Guest to Server Service in other branch

4.2 Test the system with Tracert



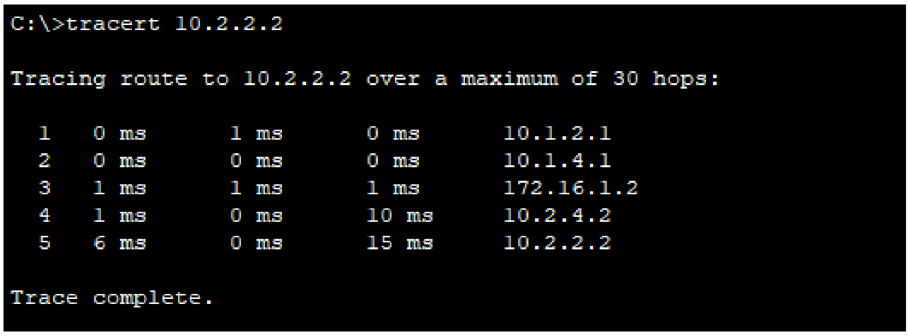
```
C:\>tracert 10.1.3.4

Tracing route to 10.1.3.4 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.0.2.1
  2   0 ms      0 ms      0 ms      10.0.8.2
  3   1 ms      1 ms      0 ms      172.16.0.2
  4   1 ms      1 ms      2 ms      10.1.4.2
  5   0 ms      1 ms      10 ms     10.1.3.4

Trace complete.
```

Figure 37: Tracert from HQ to NT



```
C:\>tracert 10.2.2.2

Tracing route to 10.2.2.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.0.2.1
  2   7 ms      0 ms      0 ms      10.0.8.2
  3   1 ms      1 ms      1 ms      172.16.0.2
  4   2 ms      15 ms     2 ms      172.16.1.2
  5   0 ms      4 ms      2 ms      10.2.4.2
  6   *         12 ms     33 ms     10.2.2.2

Trace complete.
```

Figure 38: Tracert from HQ to DN



```
C:\>tracert 10.2.2.2

Tracing route to 10.2.2.2 over a maximum of 30 hops:

  1   0 ms      1 ms      0 ms      10.1.2.1
  2   0 ms      0 ms      0 ms      10.1.4.1
  3   1 ms      1 ms      1 ms      172.16.1.2
  4   1 ms      0 ms      10 ms     10.2.4.2
  5   6 ms      0 ms      15 ms     10.2.2.2

Trace complete.
```

Figure 39: Tracert from NT to DN

5 CONCLUSION

5.1 Re-evaluate the designed network system

5.1.1 Reliability

- Our system is very reliable, the message sent by every network device always receivable by the receiver devices.
- The loss packets sometimes occur in the first route or ping because the network needed to fill in the MAC table of the switch. After fulfill all the MAC addresses needed it will be much easier to deliver packets without any loss.

5.1.2 Easy to Upgrade

- Our system is relatively easy to upgrade and add devices, because each subnet we provide hundreds of users in a single network. So it will be very easy to add and remove devices in the work space.
- It would also be pretty easy to add another branch to our network. In that case, we just need to add and config the new router represented for that branch and connect through the WAN links to the HQ router just like the other branches.
- We can guaranteed that our system can last for at least 20 years with the growth rate of more than 20% each 5 years.

5.1.3 Diverse Support Software

Our system not only supports Ethernet connection devices but we also have the wireless router to enable the wireless devices (smartphone, laptop,...) to connect to the internet.

5.1.4 Safety

- Our system has supported the mechanism to restrict the IP address to come in and out of the internet.
- The technique NAT is also used to avoid the need to assign a new address to every host when a network was moved, or when the upstream Internet service provider was replaced, but could not route the networks address space.
- We also use many more mechanisms to limit the wireless devices not to ping every other device.
- We provide the security for wireless networks using ACL tables to restrict access from wireless devices to other devices in the network.
- The Servers are placed inside a separate switch in order to make the task of implementing network configurations to make the server more secure very convenient.

- The Firewall monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. In this case, we block the traffic outside from interfere the inside.

5.2 Expected Cost

According to the expected cost from Cisco, we will now evaluate briefly the cost to build up this entire network system.

- ***Router***
  - **Cost:** 885$/unit
  - **Quantity:** 4
  - **Total cost:** 3540$
- ***Switch***
  - **Cost:** 250$/unit
  - **Quantity:** 13
  - **Total cost:** 3250$
- ***Multilayer Switch***
  - **Cost:** 250$/unit
  - **Quantity:** 3
  - **Total cost:** 750$
- ***Wireless Router***
  - **Cost:** 250$/unit
  - **Quantity:** 3
  - **Total cost:** 750$
- ***Firewall***
  - **Cost:** 250$/unit
  - **Quantity:** 1
  - **Total cost:** 250$
- ***Workstation***
  - **Cost:** 1000$/unit
  - **Quantity:** 200
  - **Total cost:** 200000$
- ***Server***

- **Cost:** 2000$/unit
- **Quantity:** 11
- **Total cost:** 22000$

In summary, the total sum for the cost is 230540$.

5.3 Remaining Problems

5.3.1 Security

- Although, we have provided the ACL to restrict the IP from wireless access to ping other devices in the network. However this will also strict the inter Network to receive message from the WebServer when they ping to the Internet.
- There might be lack of defense in depth of security which helps an attacker succeeds in reaching the network security.

5.3.2 Scalability

- Our network system is only tested within small scale so there is no guarantee that it can handle much more branches when the bank expand in the future.
- As the bank grows, the condition bottleneck might happen in the future which is a quite troublesome problem.

5.4 Future Development

5.4.1 Security

- To protect the data of the customer, we will provide some security mechanism in order to protect the system from DDOS, SQL,...
- We will also provide some hashing mechanism so that only customers can know their information, and even the bank does not know the information not provided by the customer.

5.4.2 Scalability

In the future, we can improve the system using latest technique and mechanism so it can support in large scale for a long time.

References

[1] Cisco. What is a router? https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-does-a-router-work (2020/12/31).

[2] Cisco. What is a switch? https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-vs-router.html (2020/12/31).

[3] Cisco. What is a firewall? https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (2020/12/31).

[4] Mark Taub & Jan Cornelssen & Brett Bartow & Sandra Schroeder. *CCENT/CCNA ICND1 100-105*. Cisco Press, oficial edition, 2016.