Network Architecture

***Networking Concepts and Cyber Security***

HAN22080413

HAN22080031

HAN22080120

HAN22080087

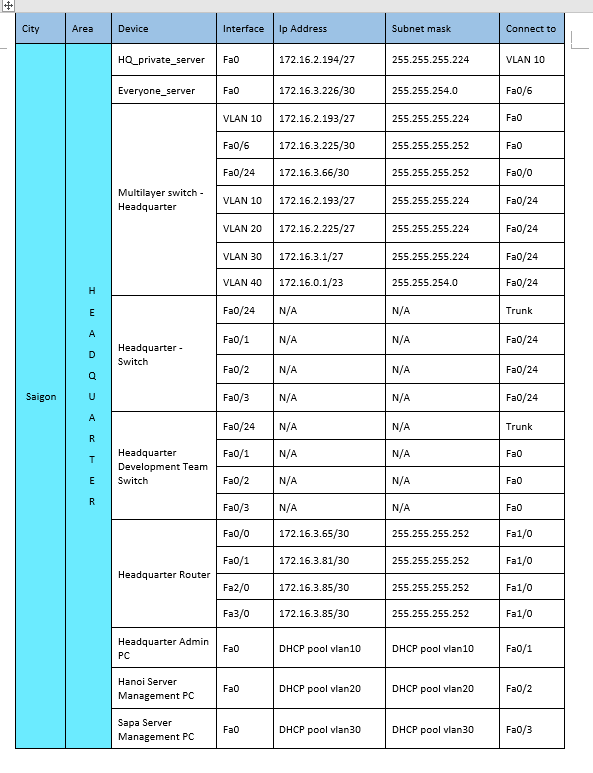
HAN22070067

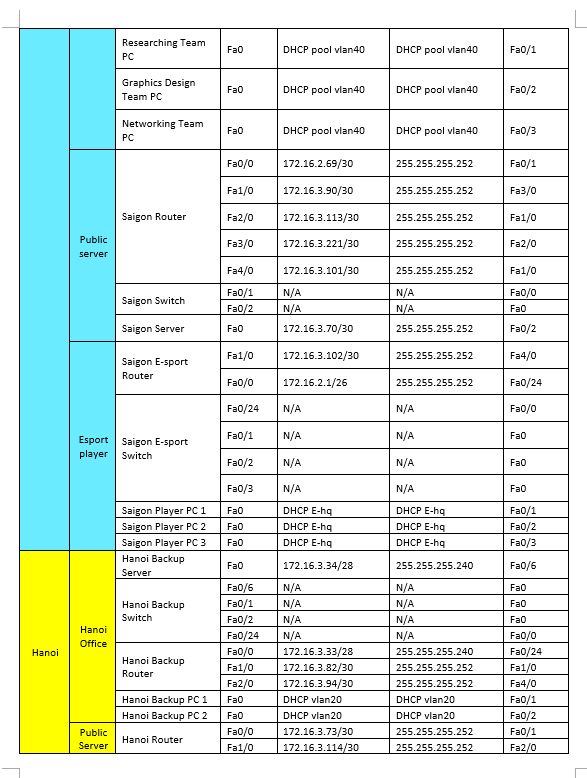
Contents

1. Introduction 0
   1. Scenario 1
   2. How this Book is organized 2
      1. Interpretation of the scenario
      2. Network Devices and their Roles
      3. OSI model and Routing

Protocols of the Model

1. Interpretation of the Scenario 4
   1. Topology 5
      1. Intercity Topology
      2. City Topology
      3. Building Topology
   2. Roles inside the Network System 7
      1. Roles
      2. Developer Role
      3. Server Management Role
      4. Player Role
2. Network Devices and their Roles 9
   1. Network Devices 10
      1. Routers
      2. Switches
   2. Cable Connections 12
      1. Cables
3. OSI Layers and Routing Protocols 14
   1. Physical Layer 15
      1. Explanation of the Layer
   2. Data Link Layer 16
      1. Explanation of the Layer
      2. VLAN
   3. Network Layer 20
      1. Explanation of the Layer
      2. IP
      3. OSPF
   4. Transport Layer 23
      1. Explanation of the Layer
      2. ACL
   5. Session Layer 25
      1. Explanation of the Layer
   6. Presentation Layer 25
      1. Explanation of the Layer
   7. Application Layer 26
      1. Explanation of the Layer
      2. DHCP
      3. DHCP Snooping







# Introduction

**SCENARIO**

A start-up company has released an esports project of a video game owned by a publisher. Therefore, a network system needs to be created to represent the three roles of the publishers, the clans/clubs (esports organizations) and the players. The network system should include a logical network design which prioritizes security, optimal choices of connections and protocols that prioritize connection speed and minimize packet loss and a hierarchy of roles with privileges and limitations needed to achieve an optimal network system. This assignment report will explain the entire system involving the reasoning behind the physical layout and choices of protocols used. All connections will be shown on an address table.

**HOW THIS BOOK IS ORGANIZED**

**Part 1: Interpretation of the Scenario**

The first part of this assignment report is a dissection of the scenario presented and will focus on the broad design of the network system. Firstly, the topology will be explained followed by the involvement of the three roles of publishers, clans/clubs, and players in the system and how they interact with the system and each other.

**Part 2: Network Devices and their Roles**

The second part of this assignment report is going to be focused on network devices and the connections between them. This part does not include protocols but is an in-depth look at all the networks in the network system and an explanation of what each network device does in specific networks.

**Part 3: OSI Layers and Routing Protocols**

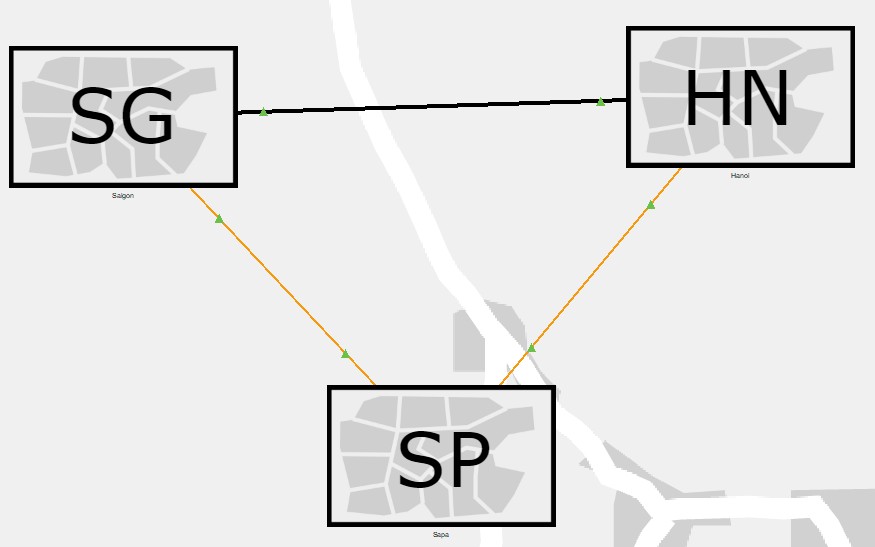
The third part of this assignment report explains all the routing protocols and their OSI model layer. To illustrate the role of each protocol of the network system, only the necessary layers of the OSI model will be discussed, while the TCP/IP model will not be mentioned due the lack of application of the TCP/IP model on the network system and the heavy focus of the OSI model during the making of the network system.

# Iterpretation of the scenario

**TOPOLOGY**

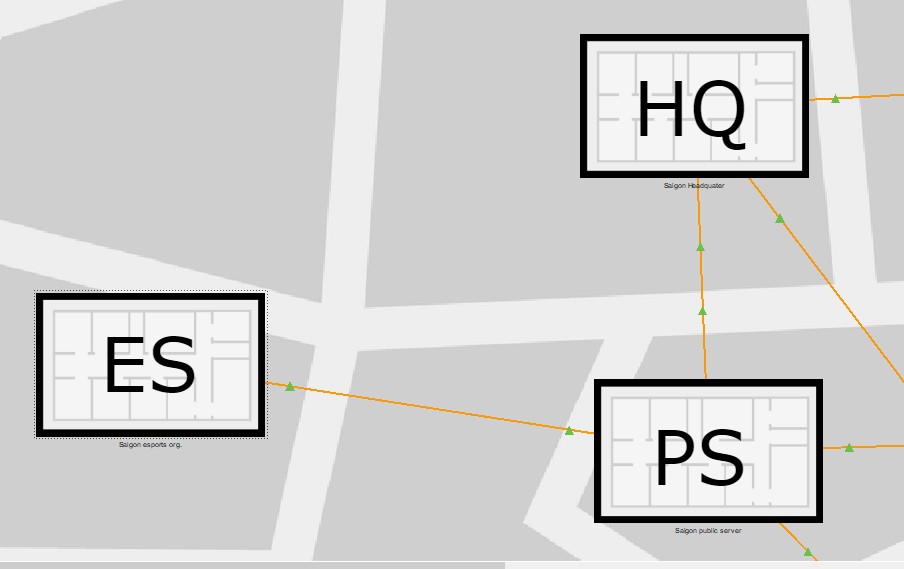
**Intercity Topology**

There are three major cities inside of the intercity, Saigon (Headquarter location), Hanoi and Sapa all connected through a mesh topology. Each city should have a direct connection to other cities to spread out the network traffic and reduce high traffic areas. In case of a power outage resulting in a city not being functional, the network traffic should not slow down or lose access to areas outside of the area that were shut down due to power outage. This network topology is very costly if the network system expands as more connection will be needed when more cities get connected but reduces unwanted latencies which is more important in an esports network that prioritizes speed and efficiency of connections.



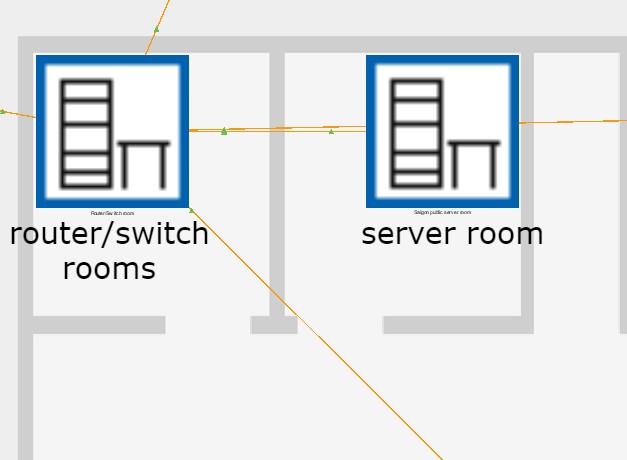
**City Topology**

Inside each city there should be three main buildings present, the headquarters or office building, the public server building and the esports organization building of each city. Each city runs on a star topology with the public server building as the center of the topology which is responsible for connection within the city as well as between cities. With this much traffic going through the public server building, there will be a corresponding headquarters or office building to maintain and update the public server. This topology makes accessing the network system very convenient as an end device or network only need to connect to the public server building to connect with another end device or network, which is crucial as an esports network must be as accessible as possible to user.



**Building Topology**

Due to the cause of each building having different tasks and configuration it is hard to define the topology of each building. With this information it is still crucial to standardize each building for clarity and efficiency. Each building has a Router/Switch room which is responsible for connecting inbuilding end devices and networks with outside connections just like a star topology. All networks connected to the Router/Switch room can be of which desirable topology of choice, which makes the building topology a hybrid network topology.



**Roles inside the Network System**

**Roles**

There are two different subsystems inside of the network system, the publisher system, and the player system. The publisher system contains the developer role and the server management role while the player system only contains the player role. Each system works independently from each other with different goals and tasks.

**Developer Role**

The developer’s main task is to develop the video game and is located inside the game development room inside the headquarters. This role only gives the user access to the headquarter user server (HUS) and the admin room. Due to limited access to the network system, outside connections are reduced which leads to a reduced number of leaks during game development.

**Server Management Role**

The server management role is the most complicated role because the server management role cannot be defined by one activity or goal, but rather varies based on where the user is located. Based on the network system, there must be two types of the server management roles, one located in the headquarter that is responsible for maintaining and looking over the HQ private server (HQPS) and office backup servers (OBS) and one located in an outside office that keeps the backup server and public server of their city in check.

**Player Role**

The player role on the other hand is the least complex role in the network system due to the role having only one simple task. The user’s (players) goal is to connect to other users via the public server network (PSN) which connects any end device or network with another one that is connected to the PSN.

**Network Devices and their Roles**

**Network Devices**

**Routers**

A router is a network device that directs data from one network to another. The data transferred between networks are encapsulated as packets and take place in the network layer of the OSI model.

All routers in the network system are used for connecting local area networks (LAN) to the wide area network (WAN). In this case each building should have one router in a Router/Switch room (RSR) that acts as an interconnection between the LAN and WAN.

Based on which building the router is located, the configuration would differ for example the routers in Hanoi office (HO) and Sapa office (SO) have DHCP and OSPF protocols configured while all other routers only have the OSPF protocol configured (including the HQ router).

**Switches**

A switch is a network device that connects an end device to another end device using MAC addresses which operates in the data link layer of the OSI model. Raw data such as bits that are transmitted as electrical signals from the physical layer and packets from the network layer are converted into frames in the data link layer. Switches that operate on multiple OSI layers are called layer 3 switches or multilayer switches which can operate on the data link layer and network layer.

Each switch in the network system interconnects the end devices in its network and has one connection to a router for WAN connections, which means that each building should only have one switch. In the case of a building having multiple networks or departments, (for example the headquarter) each network/department would still have one switch which would connect to a multilayer switch (acting as secondary router and as a central switch) which is then connected to the primary router for WAN connections.

Aside from the multilayer switch in the HQ which has DHCP and OSPF protocols configured, all layer 2 switches only have DHCP snooping and VLAN configured. The VLAN protocol takes place in the 2nd layer but is configured in and controlled by a router which is why the switch has very little configuration of the VLAN protocol.

**Cable Connections**

**Cables**

There are three types of cables used in the network system, copper straight through cables, copper crossover cables and fiber optic cables. Copper straight through cables, a cable designed to connect two network devices of different type, and copper crossover cables, designed to connect two network devices of the same type are twisted pair cables that send information through electrical signals and are most common and widely used for LAN connections. Fiber optic cables on the other hand use light signals to send information which makes them faster and more efficient but also more expensive than twisted pair cables.

All in building connections were made with either a copper straight through cable or a copper crossover cable due to its low cost compared to fiber optic as information is not being send through large distances. Copper straight through cables are used for end device to switch and switch to router connections and copper crossover cables are used for switch to multilayer switch and public server (PS) to router connections. All interbuilding and intercity connections are made with fiber optic cables due to the long distances between each building/city and the prioritization of s low latency (speed of connection) in an esports environment. In this situation choosing fiber optic cables over twisted pair cables is a design choice that sacrifices low costs to prevent higher latency, caused by slower cable connections between large distances.

**OSI Layers and Routing Protocols**

**Physical Layer**

**Explanation of the Layer**

The physical layer is the lowest layer in the OSI model which focuses on encoding data into bits (1s and 0s) and transmitting the raw data through electrical or optical signals. This includes physical devices like repeaters, hubs and cables which are only responsible for transmitting data to another node. Most notable protocols of this layer include Ethernet, USB and Bluetooth which are a part of IEEE 802 family of standardizations.

**Data Link Layer**

**Explanation of the Layer**

The data link layer is the second layer of the OSI model which lies between the physical layer and network layer and is responsible for node-to-node connections and error and flow control. The data link layer is divided into two sublayers, media access control (MAC) which communicates with the network layer and logical link control (LLC) which communicates with the physical layer. VLAN is the only protocol configured in the network system.

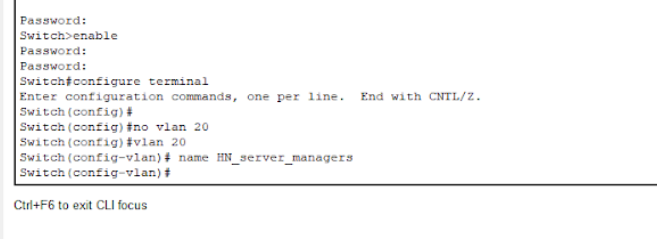
**VLAN**

A virtual local area network also known as the VLAN protocol is a protocol that can divide a network into smaller subnetworks mostly used in large networks to designate specific departments or to block off the connection between specific departments.

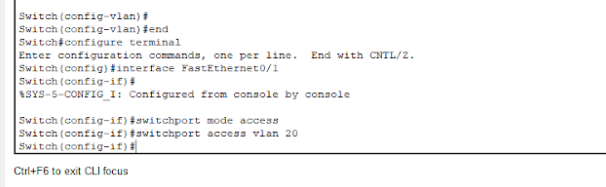
The headquarter building is the only building that has the VLAN protocol implemented due to the number of roles that are present and the need to separate different departments into different networks. Inside of the headquarter building there are four designated VLANs dedicated to six different department, the Hanoi server management (HSM) department, Sapa server management (SSM) department, admin (ADM) department, research (RES) department, game development (GMD) department and the graphic design (GRD) department. All management role departments such as the HSM, SSM and ADM departments have their VLAN as they do not need any connectivity to each other, but only connect to the server they were assigned to manage. The game development roles on the other hand such as the RES, GMD and GRD departments are all put under one VLAN as they need to connect to each other to develop the game. There are also two servers located in the building, one private server (HQPS) which is in the same VLAN as the admin (the server acts like the primary server of the headquarter) while the other server has no VLAN and acts like a temporary save for the development team.

Doing this type of VLAN configuration in the headquarter system reduces traffic from two unrelated departments and gives each VLAN a distinctive network Ip which can be used to configure trafficking protocols like ACL more easily. Creating different VLAN also reduces the need for extra routers and switches which not only simplifies the complicated system but also reduces the overall cost of the system and electricity cost.

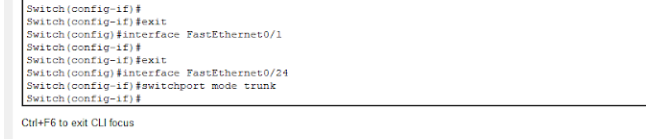
To configure the VLAN protocol, the VLAN must be created and named in the VLAN database which can be configured in the switch.



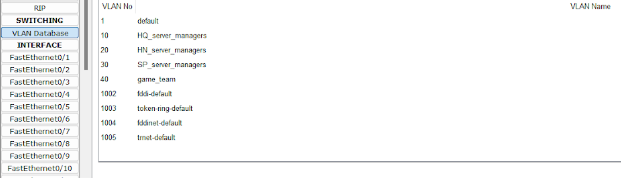
Then configure the switchport access to the interface that connects to the end devices of the VLAN.



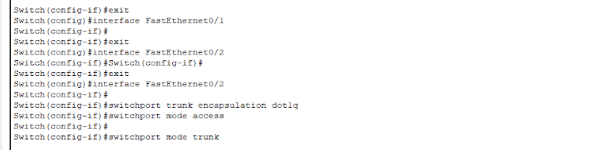
After that, trunk mode must be configured to the interface that connects to the router or multilayer switch.



The different VLAN can be seen in the VLAN database which can be accessed in the router or multilayer switch.



In case two different VLANs need connection to each other, a VLAN interface can be created which acts like a gateway that connects two VLANs in one LAN network.



**Network Layer**

**Explanation of the Layer**

The network layer is the third layer of the OSI model and decides how data goes from the sender to receiver which includes addressing, routing and logical protocols. Data in this layer are encapsulated into data packets which are being routed by specific protocols such as the internet protocol (IP) or open shortest path first (OSPF) protocol.

**IP**

The internet protocol is a network layer protocol which lets end users connect via an Ip address which is made of a network address and a host address. Some Ips such as private Ips are dedicated to private networks and cannot be used for internetwork Ips. A subnet mask determines the separation between the network address and the host address. Changing up the subnet mask to fit a desired number host is called subnetting.

In the network system subnetting is used to limit the amount host that can be inside a network and reduce unused Ip addresses.

**OSPF**

Open shortest path first also know as the OSPF protocol is an interior gateway protocol which is a type of dynamic routing protocol that shares routes inside an autonomous system. This protocol uses Dijkstra’s algorithm to calculate the shortest path from one destination to another. The OSPF protocol can also divide a network system into multiple areas to make routing more efficient, but is not necessary in the case of the network system of this report due to the insufficient amount splitable areas.

To configure the OSPF protocol the OSPF protocol has to be enabled and be given an ID. Each router needs a router-id and a designated area which in this case would be the same area for all routers as the network system only uses one OSPF area. Configuring a passive interface can tell the OSPF protocol not to search for routers in a specific network as it might not have one, in the case of the headquarter building, all individual VLANs inside of the HQ count as a network but do not contain a router.



**Transport Layer**

**Explanation of the Layer**

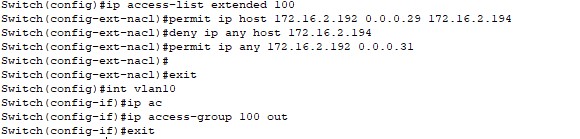
The transport layer is the forth layer of the OSI model which focuses on the end-to-end delivery of a message. If the message contains errors, the transport layer will ensure the message gets resend and if done correctly will send back a signal of confirmation. This layer breaks messages into smaller packets of information which is easier to route as the transport layer is also responsible for flow control of data.

**ACL**

Access control list (ACL) is a layer four protocol that control the flow of information through an access list mostly configured on routers and switches. There are two types of ACL, standard ACL which blocks selected Ip to all destinations and extended ACL which blocks selected Ip to specific destinations or ports.

The network system of this report uses ACL to increase security measures and reduce unwanted outside connections. For example, all access except the ones from the Hanoi office (HO) and Sapa office (SO) has been blocked to the headquarter to ensure that no data leaks or unwanted connections occur. Both offices also do not accept outside connections due to the same reason. There are no direct connections into the headquarter nor both offices which makes the only connection an indirect connection from the public server to the headquarter/offices.

To configure the ACL protocol the ACL protocol must be enabled and given a name on a router or switch that would control traffic. Then the type of traffic control (permit/deny), interface and access-group (in/out) must be configured.



**Session Layer**

**Explanation of the Layer**

The session layer is the fifth layer of the OSI model which is responsible for establishment of connection and maintenance of sessions. This layer allows end devices to establish and terminate sessions in a synchronized manner. Notable protocols of this layer are SIP, PPTP and H.245.

**Presentation Layer**

**Explanation of the Layer**

The presentation is the sixth layer of the OSI model which translates data formats and ensures that data is presented in a readable format before sending the data to the application layer. The data also might need to be encrypted, decrypted, or compressed which would decrease bandwidth allowing for higher level data structures. Notable protocols of this layer are AFP, LPP, NCP and NDR.

**Application Layer**

**Explanation of the Layer**

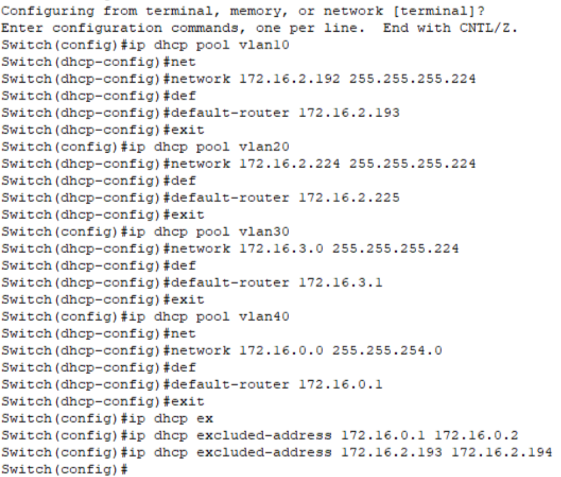
The application layer is the highest layer of the OSI model which deals with user input data such as application.

**DHCP**

The dynamic host configuration protocol (DHCP) is a protocol that assigns local Ip addresses. The protocol enables a network administrator to manage and distribute Ip addresses to end devices connected in one network. The reason why DHCP is not a data link layer protocol is because DHCP is an application that controls the data link layer.

By implementing the DHCP protocol in the network system the cost of static Ips (which are more expensive than dynamic Ips) would be reduced, which in general would improve the overall cost of the system. There are no advantages of having static Ip on end devices like personal computers in the network system which makes the switch from static to dynamic more logical.

To configure DHCP a DHCP pool and its name must be configured on a router or multilayer switch. The DHCP network and gateway must then configured to tell what Ip, and to which end device the Ip must be given to.



**DHCP Snooping**

DHCP snooping is a DHCP security feature that acts like a firewall. A hacker can easily flood the DHCP server by requesting all the Ips available. If a new Ip request came in the DHCP server would deny it due to having no more Ips.

Implementing this DHCP feature decreases the chances of such an occurrence happening.

To configure DHCP snooping DHCP snooping must be enabled, and a trusted port must be assigned. Following that a limit on how many packets can enter the interface has to be configured.

Text

Description automatically generated

Final wordcount: 3094 words without cover page and content table.