Network Architecture Design Report

Module: Networking Concepts and Cyber Security (COMP40002)

Lecturer: Dr. Anchit Bijalwan

Cohort: CS2210

Semester: 1st Year 1st Semester

Group report by

HAN22080358

HAN22080119

HAN22080236

HAN22080381

HAN22080226

Submitted to

British University Vietnam in collaboration with Staffordshire University

**Abstract**

A new start-up company launched their E-sport project with a vision to create a multi-sites business capable of providing fundamental infrastructure for casual and competitive gaming. We – as an IT team, tasked with the responsibility to evaluate network operations requirements – have designed a network architecture that can satisfy the needs. Our primary goal is providing network design, network configuration, network equipment specifications and internal communications. The design utilizes OSPF protocol, LAN, VLAN, WAN, and routing protocols used for synchronization and communication. In addition to elaborate the design and implementation of said protocols, we investigate the layers of technology within the network and its security risks.

The network consists of a main headquarters (which located in Hanoi) in charge of providing basic departments needed to facilitate a business and three collaborative venues (Ba Dinh, Cau Giay and Ha Dong) for players in various locations.

Keywords: protocols, communication, synchronisation, security

Contents

[1. Network Overview 4](#_Toc122095228)

[2. Network Devices 4](#_Toc122095229)

[2.1. Routers 4](#_Toc122095230)

[2.2. Switches 5](#_Toc122095231)

[2.3. Multi-layer switches 6](#_Toc122095232)

[2.4. PCs 6](#_Toc122095233)

[3. OSI Layers and Network Architecture Applications 7](#_Toc122095234)

[3.1. Physical layer 7](#_Toc122095235)

[3.2. Data link layer 7](#_Toc122095236)

[3.3. Network layer 9](#_Toc122095237)

[3.4. Transport layer 15](#_Toc122095238)

[3.5. Session layer 15](#_Toc122095239)

[3.6. Presentation layer 16](#_Toc122095240)

[3.7. Application layer 16](#_Toc122095241)

[References 18](#_Toc122095242)

## Network Overview

This topology describes a network of a game company with one headquarters and three branches (or collaborative venues), located in three different cities.

The headquarter is located in Hanoi, contains multiple VLANs to separate the network into various departments (Marketing department, Finance department, Analyst department, Manager department, and a database server). Additionally, we design multiple switches that can be used as fail-safe. These four local networks connect to the public network made of four routers connected. The public network used OSPF protocol to utilize the traffic. Also, one of four routers in public network is used to loop back 8.8.8.8 as a replacement for the internet.

Each of the three collaborative venues (located in Ba Dinh, Cau Giay and Ha Dong) contains 5 different personal computers (PCs) for players to taking part in competitive events that hosted in these venues.

## Network Devices

### Routers

#### Models

* IRS4331
* 2811

#### Configuration

This is the configuration of our Router in the headquarters, and it goes the same with the other 3 routers in the OSPF section.

Table

Description automatically generated with medium confidence

### Switches

#### Models

* 3650-24PS: 24 ports, Ipv4, Static IP Routing
* 2960-24TT:
  + 24 ports
  + 100% throughput: 28W
  + Built in security features

#### Configuration

This is the configuration of our switch in the headquarters, and it goes the same with the other 2 switches.

Text

Description automatically generated Text

Description automatically generated

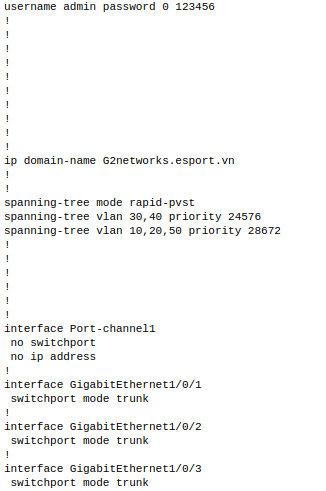
### Multi-layer switches

#### Models

* 3650-24PS

#### Configuration

This is the configuration of our multi-layer switch in the headquarters, and it goes the same with the other 2 switches.



### PCs

In sub venues Ba Dinh, Ha Dong, Cau Giay, each has 5 PCs connected to the network through cables

## OSI Layers and Network Architecture Applications

### Physical layer

The physical layer includes and defines the connector, physical cable, or wireless connection between network nodes. The physical layer is also responsible for the transmission of raw data (series of 0s and 1s) and control the bit rate. Our architecture’s physical layer includes:

* Cables: Copper Cross-over, Copper Straight-through
  + Fast Ethernet: 100 Mb/s
  + Gigabit Ethernet: 1 Gb/s
* Interfaces: GigabitEthernet, FastEthernet
* Transmission mode: Full duplex

### Data link layer

Data link layer concerns the connection between two physical nodes in a network, includes initiating and ending a connection. Network packets from the network layer are divided into frames and sent from the source node to the nominated node. This layer has two functions: Logical Link Control (LLC), identifies any involving network protocols, checks for transmitting error and synchronizes frames; and Media Access Control (MAC), which connect devices and set permissions to send/receive data via MAC addresses.

#### STP

**STP – Spanning Tree Protocol** is a data link layer network protocol, used to prevent looping within a network topology. STP was created to avoid the problems that arise when computers exchange data on a local area network ([LAN](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN)) contains redundant paths. If the flow of traffic is not carefully monitored and controlled, the data can be caught in a loop that circles around network segments, affecting performance and bringing traffic to a near halt. (Sheldon, 2021)

The redundant link connection is provided between each layer 2 switches in headquarters to the 2 Core switches. The purpose of having an extra link is that, if one link goes down still the network components can communicate with each using the redundant link. So, there will be less down time on the network. But there is a concern of adding an extra link between network switches is that it will create a broadcast storm (loop). To avoid this problem, STP protocol is used with switches in this network. So, at a time one active link will be present and another link will be in blocked mode. Once the active link fails, the redundant link comes into active mode from blocked mode.

#### VLAN Configuration

VLANs are created across departments to control traffic, stopping data from reaching another network. VLANs also create a layer of security. Additionally, VLANs help reduce cost by separating hosts logically under one switch (no need for investing in additional switches).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN | Network address | Subnet Mask | Range | Broadcast |
| VLAN 10: Marketing/PR | 192.168.10.3/24 | 255.255.255.0 | 192.168.10.4 - 192.168.10.204 | 192.168.10.205 |
| VLAN 20: Manager/Owner | 192.168.20.3/24 | 255.255.255.0 | 192.168.20.4 - 192.168.20.204 | 192.168.20.205 |
| VLAN 30: Legal/Finance | 192.168.30.3/24 | 255.255.255.0 | 192.168.30.4 - 192.168.30.204 | 192.168.30.205 |
| VLAN 40: Analyst | 192.168.40.3/24 | 255.255.255.0 | 192.168.40.4 - 192.168.40.204 | 192.168.40.205 |
| VLAN 50: Servers | 192.168.50.3/24 | 255.255.255.0 | 192.168.50.4 - 192.168.50.204 | 192.168.50.205 |

##### VTP

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol used by Cisco switches to exchange VLAN information. With VTP, you can synchronize VLAN information (such as VLAN ID or VLAN name) with switches inside the same VTP domain. A VTP domain is a set of trunked switches with the matching VTP settings (the domain name, password and VTP version). All switches inside the same VTP domain share their VLAN information with each other.

In this network, VTP is used on Core-1 switch with server mode. Others switches in headquarters are also using VTP but in client mode. This means when we want to make some adjustments on VLAN, it just needs to be done in Core-1 switch rather than adjusting again and again in other switches. It would save time as the configuration will not have to be repeated on every switch.

#### Access Control List (ACL)

Cisco ACLs are characterized by single or multiple permit/deny statements. The purpose is to filter inbound or outbound packets on a selected network interface.

In this scenario, ACL is used mainly to block others computer from accessing 2 Core switches and 2 routers (Active and Backup) in headquarters. Only the Manager or the Owner can access those devices through their computer or laptop in VLAN 20. Also, we used SSH to secure this connection between VLAN 20 and those 4 devices.

### Network layer

This layer has two main functions: the first is turning “segments” in transport layer into network packets and reassembling these packets on the receiving end; and the second is discovering the best path across a physical network (routing packets). Network layer uses network addresses (IP addresses) to guide packets to a determined node. For this scenario, there are two aspects of network layer that we will further discuss about: routing and IP configuration.

#### Routing

There are three main ways to setup the routing: static routing (setting up static IP on separate PCs, configuring on core routers of each branch and then routing the traffic from main network to outside network), dynamic routing (setting IP configuration on core routers so the traffic from inside network can communicate with ISP router for internet or other unknown traffic) and inter VLAN routing (configuring core routers to route the traffic between different VLAN in the network).

For this scenario, we use all three kinds of routing: static routing for both core and branch routers, dynamic routing for sub-router level devices (as all players' PC and 2 core switches) and inter VLAN routing for PCs related to the headquarter branch.

#### IP Configuration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Area | Device | Interface | IP Address | Connects to |
| OSPF | R1 | Fa0/0 | 2.2.2.1/24 | Fa0/0 |
| Fa0/1 | 1.1.1.1/24 | Fa0/1 |
| R2 | Fa0/0 | 2.2.2.2/24 | Fa0/0 |
| Fa0/1 | 3.3.3.2/24 | Fa0/0 |
| Fa1/0 | 113.171.2.2/24 | Gig0/0/0 |
| Fa1/1 | 113.171.3.2/24 | Gig0/0/0 |
| R3 | Fa0/0 | 3.3.3.3/24 | Fa0/1 |
| Fa0/1 | 4.4.4.3/24 | Fa0/0 |
| Fa1/0 | 113.171.1.3/24 | Gig0/0/0 |
| Fa1/1 | 113.171.5.3/24 | Gig0/0/1 |
| R4 | Fa0/0 | 4.4.4.4/24 | Fa0/1 |
| Fa0/1 | 1.1.1.4/24 | Fa0/1 |
| Fa1/0 | 113.171.4.4/24 | Gig0/0/0 |
| Hanoi - Headquarter | R-Active | Gig0/0/0 | 113.171.1.1/24 | Fa1/0 |
| Gig0/0/1 | 10.0.0.1/24 | Gig1/0/24 |
| R-Backup | Gig0/0/0 | 113.171.2.1/24 | Fa1/0 |
| Gig0/0/1 | 113.171.2.1/24 | Gig1/0/24 |
| CORE-1 | Gig1/0/24 | 10.0.0.2/24 | Gig0/0/1 |
| Gig1/0/21 |  | Gig1/0/21 |
| Gig1/0/22 |  | Gig1/0/22 |
| Gig1/0/1 |  | Gig0/2 |
| Gig1/0/2 |  | Gig0/2 |
| Gig1/0/3 |  | Gig0/2 |
| CORE-2 | Gig1/0/24 | 10.0.1.2/24 | Gig0/0/1 |
| Gig1/0/21 |  | Gig1/0/21 |
| Gig1/0/22 |  | Gig1/0/22 |
| Gig1/0/1 |  | Gig0/1 |
| Gig1/0/2 |  | Gig0/1 |
| Gig1/0/3 |  | Gig0/1 |
| ACC-3 | Gig0/1 | N/A | Gig1/0/1 |
| Gig0/2 | Gig1/0/1 |
| Fa0/1 | Fa0 |
| Fa0/3 | Fa0 |
| Fa0/4 | Fa0 |
| Fa0/5 | Fa0 |
| Fa0/6 | Fa0 |
| Fa0/2 | Fa0 |
| ACC-4 | Gig0/1 | N/A | Gig1/0/2 |
| Gig0/2 | Gig1/0/2 |
| Fa0/1 | Fa0 |
| Fa0/3 | Fa0 |
| Fa0/4 | Fa0 |
| Fa0/5 | Fa0 |
| Fa0/6 | Fa0 |
| Fa0/2 | Fa0 |
| ACC-5 | Gig0/1 | N/A | Gig1/0/3 |
| Gig0/2 | Gig1/0/3 |
| Fa0/1 | Fa0 |
| Fa0/2 | Fa0 |
| Server DHCP + FTP | Fa0 | 192.168.50.254 | Fa0/1 |
| Server DNS | Fa0 | 192.168.50.253 | Fa0/2 |
| PC Marketing PR 1 | Fa0 | DHCP VLAN 10 | Fa0/1 |
| PC Marketing PR 2 | Fa0 | DHCP VLAN 10 | Fa0/3 |
| PC Marketing PR 3 | Fa0 | DHCP VLAN 10 | Fa0/4 |
| Laptop Manager Owner 1 | Fa0 | DHCP VLAN 20 | Fa0/5 |
| PC Manager Owner 1 | Fa0 | DHCP VLAN 20 | Fa0/6 |
| PC Manager Owner 2 | Fa0 | DHCP VLAN 20 | Fa0/2 |
| PC Legal Finance 1 | Fa0 | DHCP VLAN 30 | Fa0/3 |
| PC Legal Finance 2 | Fa0 | DHCP VLAN 30 | Fa0/1 |
| Laptop Legal Finance 1 | Fa0 | DHCP VLAN 30 | Fa0/4 |
| PC Analyst 1 | Fa0 | DHCP VLAN 40 | Fa0/5 |
| PC Analyst 2 | Fa0 | DHCP VLAN 40 | Fa0/2 |
| Printer Analyst 1 | 0 | DHCP VLAN 40 | Fa0/6 |
| Ba Dinh | Router (BD) | Gig0/0/1 | 113.171.5.1/24 | Fa1/1 |
| Gig0/0/2 | 172.16.2.1/24 | Gig0/1 |
| SW (BD) | Gig0/1 | N/A | Gig0/0/2 |
| Fa0/1 | Fa0 |
| Fa0/2 | Fa0 |
| Fa0/3 | Fa0 |
| Fa0/4 | Fa0 |
| Fa0/5 | Fa0 |
| PC BD 1 | Fa0 | DHCP - BD | Fa0/1 |
| PC BD 2 | Fa0 | Fa0/2 |
| PC BD 3 | Fa0 | Fa0/3 |
| PC BD 4 | Fa0 | Fa0/4 |
| PC BD 5 | Fa0 | Fa0/5 |
| Cau Giay | Router (CG) | Gig0/0/0 | 113.171.4.1/24 | Fa0/1 |
| Gig0/0/1 | 172.16.3.1/24 | Gig0/1 |
| SW (CG) | Gig0/1 | N/A | Gig0/0/1 |
| Fa0/1 | Fa0 |
| Fa0/2 | Fa0 |
| Fa0/3 | Fa0 |
| Fa0/4 | Fa0 |
| Fa0/5 | Fa0 |
| PC CG 1 | Fa0 | DHCP - CG | Fa0/1 |
| PC CG 2 | Fa0 | Fa0/2 |
| PC CG 3 | Fa0 | Fa0/3 |
| PC CG 4 | Fa0 | Fa0/4 |
| PC CG 5 | Fa0 | Fa0/5 |
| Ha Dong | Router (HD) | Gig0/0/0 | 113.171.3.1/24 | Fa1/1 |
| Gig0/0/1 | 172.16.1.1/24 | Gig0/1 |
| SW (HD) | Gig0/1 | N/A | Gig0/0/1 |
| Fa0/1 | Fa0 |
| Fa0/2 | Fa0 |
| Fa0/3 | Fa0 |
| Fa0/4 | Fa0 |
| Fa0/5 | Fa0 |
| PC HD 1 | Fa0 | DHCP - HD | Fa0/1 |
| PC HD 2 | Fa0 | Fa0/2 |
| PC HD 3 | Fa0 | Fa0/3 |
| PC HD 4 | Fa0 | Fa0/4 |
| PC HD 5 | Fa0 | Fa0/5 |

#### HSRP

HSRP stands for **Hot Standby Router Protocol**, it allows you to configure two or more routers as standby routers and only a single router as an active router at a time. All the routers in a single HSRP group share a single MAC address and IP address, which acts as a default gateway to the local network. The *Active router* is responsible for forwarding the traffic. If it fails, the *Standby router* takes up all the responsibilities of the active router and forwards the traffic.

HSRP is configured by combining the 2 core routers in this network. Therefore the 2 core routers will act as a single virtual router for the internal hosts. Core-1 router will assume the responsibility as active router for VLAN 10, VLAN 20 and VLAN 50 and work as standby router for VLAN 30, VLAN 40 while Core-2 will take responsibility as active router for VLAN 30, VLAN 40 and be standby for VLAN 10, VLAN 20, VLAN 50. If a router fails, the other router assumes the role of the failed router. Since the new forwarding router uses the same MAC and IP addresses, the hosts can communicate without any disruption even if 1 core router fails.

#### NAT

NAT stands for **Network Address Translation** is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table.

Class C private range IP addresses are used inside this network. But the hosts cannot communicate with this private IP address over the Internet because private IP addresses are not routable on the Internet. Therefore, they must be converted to public IP addresses for communication over the Internet. So, NAT becomes an essential part of this network design. PAT (Port Address Translation) is used in the core router to map one/two public IP addresses provided by ISP to map the private IP address used inside the network. By using PAT, we can save the number of public IP addresses used for the translation. Static NAT will be used for communication of server over the Internet. By using NAT, public IPv4 address can be saved and internal IP plan of this network can be hidden from the outside world.

#### **EIGRP**

**Enhanced Interior Gateway Routing Protocol** **(EIGRP)** is an advanced distance vector routing protocol based on the principles of the Interior Gateway Routing Protocol (IGRP). It has a unique characteristic that improves the operational ability and fast converging rate. It can determine the shortest path distance vector, and it works on the principle of Interior Gateway Routing Protocol, a classless routing protocol. It uses metrics like bandwidth, load and delays to calculate the shortest optimal network route. It is a technologically, more advanced distance vector-based routing protocol.

EIGRP is config mainly in 2 Core switches and on 2 routers (Active and Backup) of

headquarters. This protocol takes the responsibility of guide the 2 Core switches to go on right path. In this network, when everything works normally, both Core switches will go through the router Active to connect to public networks. However, when the router active failed, these 2 switches would automatically change their road to the router Backup to keep everything on track.

#### **OSPF**

**Open Shortest Path First** **(OSPF)** helps finding the best routing between two routers in the same network by using SPF algorithm. In this scenario, we use OSPF for four main routers to connect four different networks.

#### **GRE Tunnel**

**GRE (Generic Routing Encapsulation), GRE Tunnel** is the mechanism that encapsulate one protocol in another protocol and provides connection between the nodes. This is done basically IP over IP. A Service Provider Network or [**Internet**](https://ipcisco.com/lesson/basic-terms-for-internet/) is used for **GRE (Generic Routing Encapsulation)**. **GRE** provides this communication over a Tunnel. This is called **GRE Tunnel**. This Tunnel means that there is a transport protocol and a passenger protocol. Tunnel End Points know this passenger protocol but between the end points, the transportation is done with transport protocol.

In this network, GRE Tunnel is used to set the communication between each branch to the headquarter. There are 6 tunnels on the headquarter which means each router (Active or Backup) has 3 tunnels. Each of those 3 tunnels are connected to 3 branch one by one. On the other hand, from the router in branch, there only 2 tunnels to the router Active and router Backup. Also, EIGRP is used to route these tunnels but in Cisco although we config it correctly but no matter what protocols we try to use, it still ends up being recursive routing.

### Transport layer

The transport layer uses data transferred during sessions in session layer, divides it into “segments” for transmitting purpose, reassembles those “segments” on the receiving end and sending to session layer. The transport layer maintains flow of communication by controlling the size of packets sent, ensuring rate of data sending matches connection speed of receiving device, error controlling and requesting data, if error occurs. Protocols using in this layer include TCP (maintains a reliable connection and protects data transmission) and UDP (provides quick transmission, transmit data in real-time without delays).

### Session layer

This layer creates sessions or communication channels. While keeping these sessions remain opened, the session layer also keeps sessions functional for data to be transferred. If any interruption occurs during the data transfer, session layer can resume data transfer once the connection is restored by setting checkpoints. At the end of the session, session layer is responsible for closing the channel. Each session allows only one transport connection. Protocols using in this layer include Zone Information Protocol (ZIP) and Session Control Protocol (SCP).

### Presentation layer

Data using in application layer is prepared in presentation layer. Also, this layer negotiates on how data should be encoded, encrypted, and compressed between two communicating systems. Presentation layer can be considered as the medium: taking what the layers below (session layer and below) deliver and translates it to what the layer above (application layer). As a result, protocols using in this layer are translation protocols (encryption/decryption, ASCII, EBCDIC, etc.)

### Application layer

Application layer is used by end-devices’ software to communicate over the network (for example, email and web browsers). For that specific purpose, protocols provided by this layer supports software to send/receive data and present such data to users. For our network architecture, we use the following protocols that include in application:

* DNS - Domain Name System
* FTP - File Transfer Protocol
* DHCP - Dynamic Host Configuration Protocol

#### DNS

Instead of using IP address to access, DNS server helps assign readable name for users' accessibility and convenience. In our network, we have built one website for marketing and promoting purpose, named as esports.com and assigned the IP address: 192.168.50.253.

#### FTP

FTP allows computers to access files. Every device in the network can access this server but only people in the headquarters can login in and use it. We created two accounts for the directors, which have full access to the files, and the staff in other departments, which has less control over the files.

#### DHCP Configuration

Every PCs in our network architecture use DCHP to automatically get their own IP addresses, default gateway and DNS server. In Hanoi – Headquarters, we config DHCP in the Server-PT DHCP. Each VLAN, which accounts for different departments in the company, has its own DHCP configuration in the server. However, they all share the same network ID of 192.168 (class C) with the subnet mask of 255.255.255.0 and DNS server of 8.8.8.8. Furthermore, the maximum IP addresses the DHCP server can provide in each VLAN is 200, which means that each department can fit up to 200 users. In addition, in the other three sub venues, we config DHCP in the router of each site, through the CLI. All three sites have the same network ID of 172.16 while the third octet of Ha Dong, Ba Dinh, Cau Giay is 1, 2, 3, respectively. Like the headquarters, its venues have the DNS server of 8.8.8.8.

# References

Kugathasan, Janarthanan. (2017). Network Design Report.

Pedamkar, P. (2021) *What is EIGRP? Fundamentals & Benfits of EIGRP routing protocol*, *EDUCBA*. Available at: <https://www.educba.com/what-is-eigrp/> .

Sharma, S. (2021) *Hot Standby Router protocol (HSRP)*, *GeeksforGeeks*. Available at: <https://www.geeksforgeeks.org/hot-standby-router-protocol-hsrp/>.

Sheldon, R. (2021) *What is Spanning Tree Protocol?*, *Networking*. TechTarget. Available at: <https://www.techtarget.com/searchnetworking/definition/spanning-tree-protocol#:~:text=Spanning%20Tree%20Protocol%20(STP)%20is,LAN)%20that%20contains%20redundant%20paths>..

Upravnik (2021) *What is VTP?*, *Study CCNA*. Available at: <https://study-ccna.com/what-is-vtp/> .