Ministry of Education and Science of the Republic of Kazakhstan
Suleyman Demirel University

Aidana Shongariyeva, Bibizhan Orazaliyeva, Aizada Askar

Creating Adaptive and Secure Enterprise Network
Создание адаптивной и безопасной корпоративной сети
Бейімделген және қауіпсіз корпоративті желіні құру

A thesis submitted for the degree of
Bachelor in Information Systems
(degree code: 5B070300)

Kaskelen, 2020

Ministry of Education and Science of the Republic of Kazakhstan
Suleyman Demirel University
Faculty of Engineering and Natural Sciences

Creating Adaptive and Secure Enterprise Network
Создание адаптивной и безопасной корпоративной сети
Бейімделген және қауіпсіз корпоративті желіні құру

A thesis submitted for the degree of
Bachelor in Information Systems
(degree code: 5B070300)

Author: **Aidana Shongariyeva, Bibizhan Orazaliyeva, Aizada Askar**

Supervisor: **Diana Burissova, Darmen Kariboz**

Dean of the faculty:
Assist. Prof. Bogdanchikov Andrey

Kaskelen, 2020

Abstract

Over the last few decades, Network Enterprise is the most important aspect of our life. Particularly we can highlight "connection to the Internet". Every Enterprise to get information needs Network. So aim of the project is to create an adaptive, reliable and secure network. This article describes the development of a modeling enterprise network. To create a Network we use SDU's Network Information (Server Room) and to get information about devices and connection. To get a strong connection between devices we use configurations such as: Switch and Router configurations, VTP, VLAN, DHCP, IP Routing, ACL, NAT and etc.

Аңдатпа

Соңғы бірнеше онжылдықта корпоративті желі біздің өміріміздің маңызды бөлігі болды. Атап айтқанда, «Интернет байланысын» бөліп көрсетуге болады. Әрбір кәсіпорынға ақпарат алу үшін желі қажет. Сондықтан біздің мақсатымыз - бейімделетін, сенімді және қауіпсіз желіні құру. Бұл мақалада корпоративтік желіні модельдеудің дамуы сипатталған. Желіні құру үшін біз СДУ желісі (сервер бөлмесі) туралы ақпаратты қолдандық, сонымен қатар құрылғылар мен қосылыстар туралы жайында ақпаратты алдық. Құрылғылар арасында сенімді байланыс алу үшін біз осы конфигурацияларды қолдандық: коммутатор мен маршрутизатордың конфигурациясы, VTP, VLAN, DHCP, IP-бағыттау, ACL, NAT және т.б.

Аннотация

За последние несколько десятилетий корпоративная сеть является наиболее важным аспектом нашей жизни. В частности, мы можем выделить «подключение к Интернету». Каждое предприятие для получения информации нуждается в сети. Поэтому наша цель - создать адаптивную, надежную и безопасную сеть. В этой статье описывается развитие моделирующей корпоративной сети. Для создания сети мы используем информацию о сети СДУ (серверную комнату) и информацию об устройствах и подключении. Чтобы получить надежную связь между устройствами, были использованы: конфигурации коммутатора и маршрутизатора, VTP, VLAN, DHCP, IP-маршрутизацию, ACL, NAT и т. д. д.

Contents

Chapter 1

Introduction

1.1 Motivation

In the 21st century, the Internet serves us to be enabled to the information. Every organization, university, and school must have its own Network to be connected to the Internet. To successfully connect they have to adaptive, reliable and secure Networks. It sounds easy but if we go to the deep it's a science with complicated things. It is a crucial part of any organization. So we choose this topic to completely understand and to help the organizations for creating adaptive and secure Networks.

1.2 Aims and Objectives

Our aim is to understand the essential parts of the Network and their connection, and how they work. We start by creating a Network topology virtually with the virtual devices to reinforce our knowledge. Now we are aimed to use theoretical knowledge we gained from different disciplines and small lab works to create Network topology from the very beginning.

1.3 Current situation

The current network uses routers and switches that perform different standards depending on when they were purchased. Network configured with inefficient topology. Vlans are managed in a disorganized way. University portal works slow due to server performance.

1.4 Benefits

The main benefits of the project are improved network security and reliability, also increased network capacity and future scalable ability. Therefore points of

failure will be identified in order to increase network adaptivity and provide fault tolerance by implementing redundancy.

Chapter 2

Review

2.1 Network Design

In the information society, networking is a necessary trend in computer development. Especially with the rapid development of the Internet, the computer network has become the consent of the whole society. Among all of the essentials for human life, the necessity to interact with other people is the most important one.

Networks can be of different size, beginning with simple networks with two computers and ending up with system that connects millions of devices and users. Hence, the Internet which is the largest network have changed the manner that we distribute information, learn, communicate, and work.

Networks have to correspond the current requirements of organizations and support emerging technologies as advanced technologies are used. Now it is possible to build flexible, adaptive, and manageable network with current network design models and principles. Despite of network size and requirements, there are the well-structured engineering principles that should be followed in order to successfully implement any network design, as listed below:

Hierarchy

When considering design rules that should be integrated in a structured manner to organization, it's helpful to look at the issue from the side of whole hierarchical structure of the building considering functions and features that have to be executed at every layer of hierarchy. Also on the second hand key modules and building blocks should be considered by determining how they relate to one another and operate in general hierarchy. If we look at the fundamental concepts, the campus is typically consist of three-tier hierarchical model which are the core, distribution, and access layers. Every element in the hierarchy run a concrete number of functions or services offered by this element and has a particular role to carry out which is considered as the main principle of the hierarchical design.

Flexibility

Key factors of the effective performance of campus design are the ability to retrofit distribution of the network by adding new services and increasing capacity without heavy upgrade. By using the structural hierarchical design, a high degree of flexibility can be indeed achieved, so that it is possible to gradually vary every module in the network independently from the others.

Modularity

Building blocks that integrate into a large campus are called system modules. If some module fails then it can be separated from the others on the network, wherein a quick detection of problems can be ensured, as well as high overall system availability. Network modifications, updates and implementation of new features can be carried out in a controlled and phased manner, providing major flexibility in the functionality and maintenance of the enterprise network. If a particular module does not have adequate capacity anymore or is losing a some functions or service, it affords to be upgraded or substituted by different module which plays the same specific role in the whole hierarchical design.
[6]

2.2 Multi-Tiered Architecture

The apply of Multi-tiered Architecture, campus networking, security in the network, Network Protocols, IP addressing, ACL's are all key aspects for making up this project. The first of them is about hierarchical network design model as mentioned above which helps build topology in particular layers. Each layer operates specific functions, therefore the right systems and features have to be chosen for each layer. [7]

A traditional hierarchical topology as in Figure 2.1 consists of the following:

- A Core layer with high end routers and layer 3 switches that are optimized for accessibility and execution.
- A Distribution layer with routers and switches that integrate policies.
- An Access layer provides connection between users through lower access switches and wireless access points.

Every layer in the hierarchical design plays a concrete role. The first core layer allows efficient transport between objects. The distribution layer implements rules concerning security, routing and traffic loading and provides connection between network services with access layer, the last access layer gives access for computer user through switches and hubs.

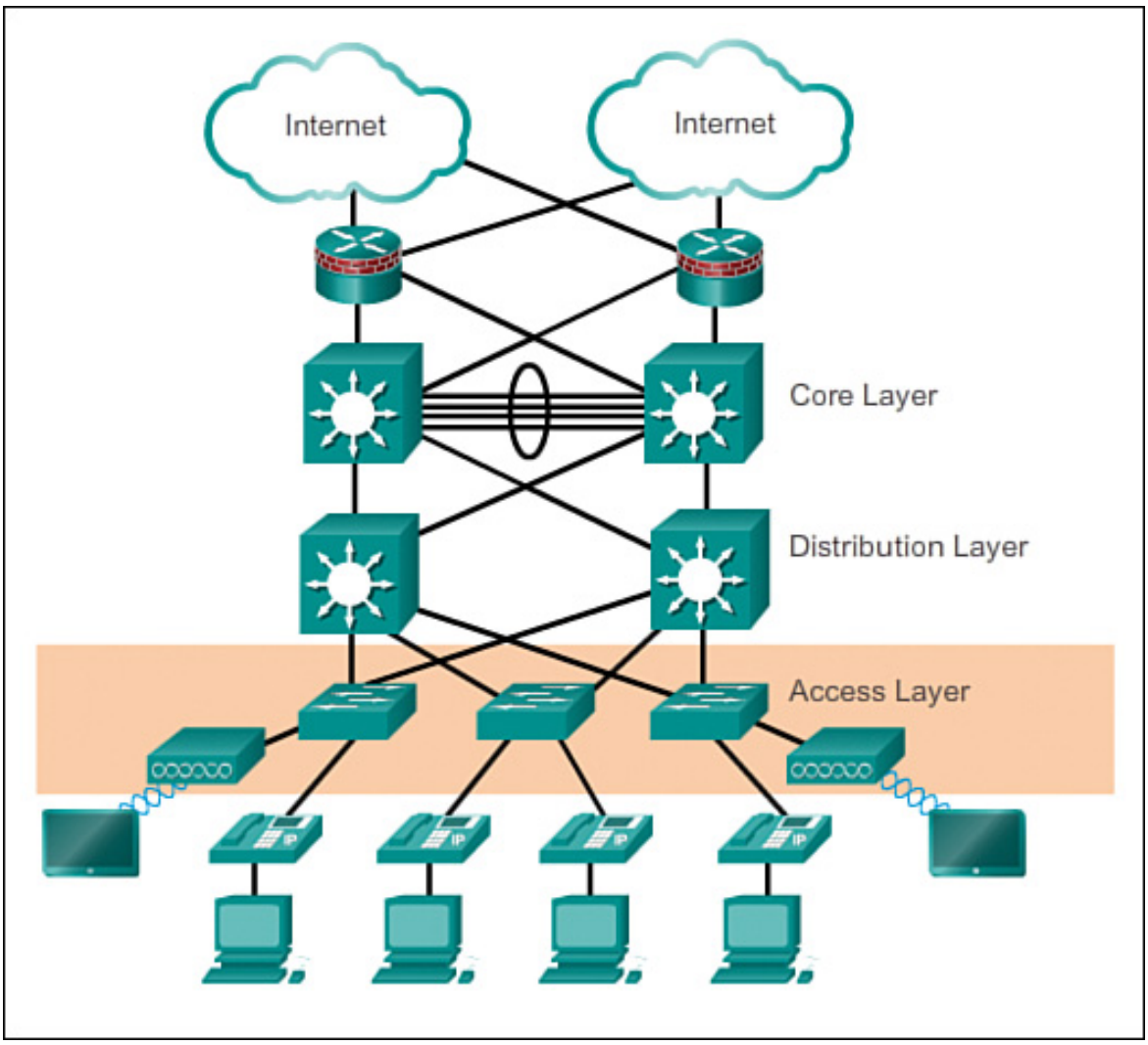


Figure 2.1: The Hierarchical Architecture of a Network

2.3 Enterprise Networks

We can imagine an enterprise network as a platform for connecting many different computing devices. Every system is potentially able to interact with all other systems while maintaining acceptable efficiency, security, and reliability in this platform.

Internet protocols and Web technologies have contributed in achieving this platform by providing better results with lower cost and negligible configuration problems. TCP/IP is a collected network protocol which allows organizations link offices and partition LANs into one network, and connect to the Internet. An enterprise network connects all the isolated branch offices into an intercompany network, by giving the opportunity for end users in an organization to access any computing data or resource. It can provide interaction among dissimilar and autonomous systems and also, have the ultimate goal of decreasing the number of applied network protocols. [1]

2.3.1 Requirements of an Enterprise Network

All of those system modules that mentioned above open up deep security implications. Each new connection can be a failure source or potential attack vector. Enterprise networks must be able to secure these new connections by recognizing potentially malicious behaviors or detecting anomalies. Consequently network security and adoptivity are main requirements of our university network.

Security in the network is controlled by particular operations which are destined to protect the integrity and usability of network and data. It can be implemented through hardware and also software technologies and stops any type of threats from accessing data or spreading on network. Network security includes several layers of defense at the edge and in the network because failures can happen at any layer, so every layer in network security implements certain policies and controls. There are many particularized techniques and types of network security in order to implement defense in depth .

- Firewalls act as a obstacle between the untrusted outside networks and our trusted inside network.
- Securing Cisco devices, including passwords on IOS devices and enabling SSH on routers.
- Antimalware and antivirus software protect a network from a malicious software, including worms, viruses and trojans.
- ACLs are like filter in network to permit or deny data flows into or out of network interfaces that are used by routers or switches.

2.4 Network Devices

Network physical devices are an integral part network used for communication of hardware on a computer network. There are a variety of end devices, hubs and access points, switches, routers servers and cables that connect all of them to each other. Network devices allow to build usable and scalable enterprise network

2.4.1 Firewall

A firewall as a security hardware device controls entering and exiting network traffic deciding whether to permit or block specific traffic based on a determined set of security rules. It has been a first line of protection in network security for more than 25 years. There are several types of firewalls: Proxy firewall, Unified threat management (UTM) firewall, Stateful inspection firewall, Next-generation firewall (NGFW). First one serves as the gateway from one network to another for a specific application and can provide additional features such as

content caching and security by protecting network from direct connections from outside the network. UTM firewall combines many security-related functions like intrusion detection and prevention system also includes cloud management. Next a stateful inspection firewall permits or denies traffic based on port, and protocol and monitors behavior of connections from their opening until they are closed. Last one blocks advanced malware and application-layer attacks which are example of modern threats.

2.4.2 Routers

A **router** is a hardware network device that is used to link several network sections into one logical network by grasping in what way to transmit traffic from a sender to eventually reach a receiver, thus protocols that are being used strongly influence on routing behavior. Routers run on the network layer of the OSI model so it demands comprehending how Network layer protocols behave. A router directs a packet to its network or to Internet destination applying routing protocols to transmit information and define routing decisions. Routing occurs in a core layer between routing devices and between a edge gateway router and a router on the ISP network. Every time when a packet needs to be redirected between interfaces consults with routing tables that are maintained by routers. It is possible to manually add routes to the routing table which is a very reliable but less-manageable method, relying on the size of the network or it can be updated automatically using the following routing protocols: [2]

1. Routing Information Protocol (RIP)/RIPv2.
2. Interior Gateway Routing Protocol (IGRP).
3. Enhanced Interior Gateway Routing Protocol (EIGRP).
4. Open Shortest Path First (OSPF) and etc.

Knowing how the routing protocols work is extremely important in avoiding trouble situations, such as:

1. A A hacker sending updates of route to network in order to poison an important route causing a DoS condition.
2. The occurrence of router overload due to a routing loop in result the network becomes very slow.

2.4.3 Switches

Switches, as in Figure 2.2, are an unusual type of hub that can offer an additional functionalities to physical-layer repeater hubs. They runs at the physical layer

and the data link layer of the OSI Model. A switch must read the MAC address of every frame that transmits through it. This data allows them to repeat entering data frames only to receivers to which a frame is addressed. This accelerates the network and decrease congestion. Switches perform at the physical layer and the data link layer of the OSI Model. [3]

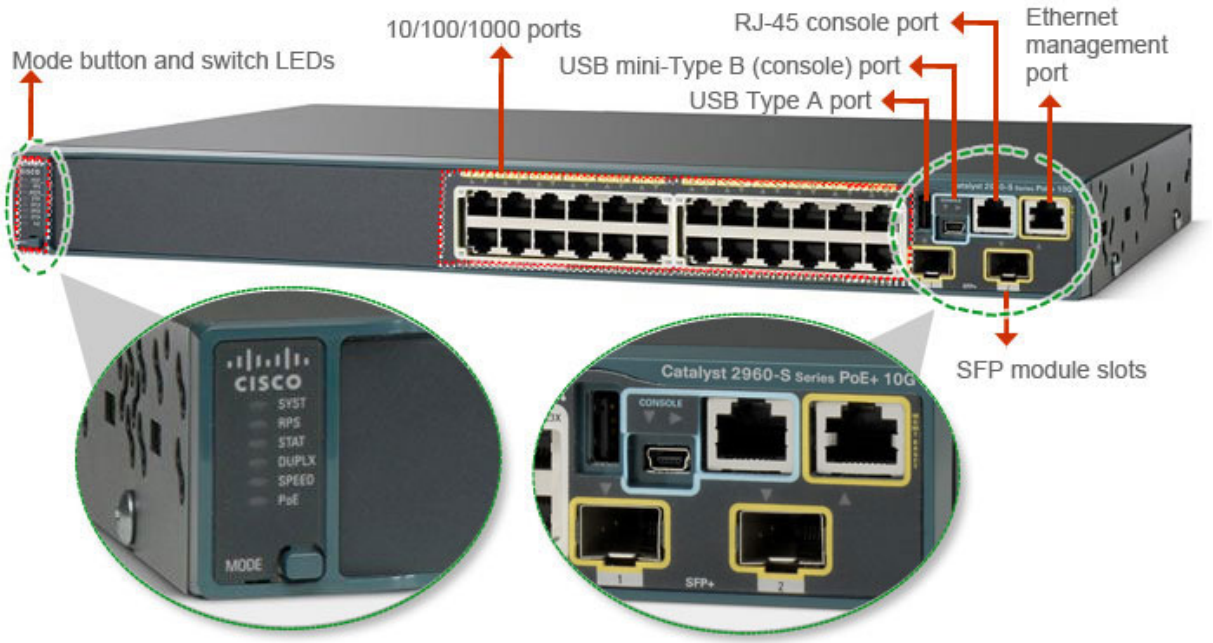


Figure 2.2: The Interface of a Switch with Ports

2.4.4 Multilayer Switch

A multilayer switch is a network physical device which runs at core layer and distribution layer of hierarchical design and operates at higher layers of the OSI reference model, unlike access switches. This switch performs the functions of both a switch and a router at incredibly fast speeds. Unlike a typical switch layer 3 switch examines deeper into the protocol description unit at segment level and to perform routing functions it uses ASIC hardware circuits while typical routers reside on a microprocessor and uses applications running on it.

Virtual LANS in Switches

A VLAN is a group of hosts, potentially located in different places, but can communicate as if they were connected to a broadcast domain due to same set of requirements configured on hosts. Once the VLANs are created, smaller broadcast domains can be created at the Layer 2 switched network, by assigning different interfaces on the switch to serve different subnets. A VLAN is considered to be its

own subnet, which means that frames broadcast to the network are only switched between interfaces that are logically organized within one VLAN. [4]

VLAN Trunking Protocol (VTP)

VLAN Trunk Protocol (VTP) decreases work for administration in a scaled network which is implemented by configuring switches as VTP server and VTP clients, for example during the configuration of a new VLAN on VTP server, this VLAN is shared through all other switches in the domain while without VTP the same VLAN was needed to be configured everywhere. The key point for correct realization is that VTP client must have the same domain name with the VTP server and for security aspects need to set password. Protocol is available on most products of the Cisco Catalyst series.

2.4.5 Wireless Access Point (WAP)

An access point typically defined as wireless network adapter card with transceiver, broadcasts and receives signals between surrounding computers passing back and forward between the wireless end devices and the cabled network. They act as wireless hubs by connecting several wireless devices into one subnet and they have at least one physical port to bridge to a typical wired Ethernet network.

2.4.6 Servers

A server network device controls network resources responding to requests made over a network. Servers perform only server tasks thus they are often devoted. HTTP, DHCP, FTP, DNS, SMTP protocols can be applied on servers to manage university network.

HTTP governs the way a web client and web server cooperate. It determines the content and the way of formatting the requests and responses that are transmitted between the client and server by specifying the message types used for that communication.

Dynamic Host Configuration Protocol (DHCP) server simplifies IP address assignment to end devices in local network. Centralized DHCP server facilitates for organizations administering assignments of all dynamic IP address from a single server. This is useful for network efficiency as it ensures consistency across the company, including branch offices. IP addresses are dynamically assigned from a DHCP pool of available addresses for some period of time, depending on configuration on the server, or until the client no more needs the address.

A DNS server resolves host names into IP addresses on a network. It accomplishes this by accepting DNS queries from clients and by performing DNS queries at DNS server, depending on how the server has been configured. A DNS

server stores a various domain names, records, Internet hosts and other related information in its database and it always connected to the network.

FTP transfers files between a server and client on a network where server is a computer which stores data and client is computer requesting data. Port 21 is usually used by FTP as its main means of communication. FTP clients can authenticate by passing the username and password explicitly, or connect anonymously if allowed on the server.

2.5 Network Address Translation (NAT)

NAT conserves public IPv4 addresses as its main function by allowing devices to use private IPv4 addresses in LAN and providing conversion to a public address when needed. Also, NAT includes an additional advantage of adding to a network a degree of privacy and security because it conceals internal IPv4 addresses from outside networks. Routers can be configured with one or multiple valid public IPv4 addresses depending on configured NAT types. NAT pool contains these public addresses and when LAN device sends request to external network, the router with enabled NAT translates the private address of the device to a public IPv4 address from the NAT pool.

Converting the address and port number of the PAT (also called NAT with overload) saves addresses in the internal pool of global addresses, allowing the router to use one internal global address for several internal local addresses. That is to say, a one public IPv4 address can maintain dozens or even hundreds of internal private IPv4 addresses.

2.6 Access Control Lists

Access Control List (ACL) are filtering mechanism that enables to monitor weather routing updates or packets are allowed or blocked into or from the network. Administrators use them to provide additional security for networks because ACLs gives a powerful method to manage entering and exiting network traffic. it is possible to determine who to hang certain politicians on like who will participate in certain processes, and who will not, for whom needs to limit in speed to 500mb, and who to 1gb. All routed network protocols can be configured with ACLs.

Providing network security with managing the network traffic is the main reason to enable ACLs on the other hand.

2.6.1 Why Use ACL

The following are some main causes of enabling ACL in a network:

- Network performance would rise due to restricting network traffic.

- It ensures controlling of traffic flow by limiting the transmission of updates in the routing.
- Security is a key factor when enabling ACL.
- Manages traffic of which type should be permitted or blocked by the router.
- Capability controlling areas which are available for client access.

2.6.2 Types of Access Control Lists

The types of ACLs used in networks are described in the following paragraphs:

Standard Access-List

Standard access lists build filters from source addresses to use for filtering as a server. Access lists based on address differentiate routes on a network uses a network address number (IP) to control. These address-based access lists include ranged addresses or listed addresses and also, a statement that represents whether access toward or forward from that address is allowed or blocked.

Extended Access Lists

The mostly used Extended access lists makes filters for packets that flow on the network using destination address, source address, port number and protocol in use.

2.7 Cisco Packet Tracer

Cisco Packet Tracer is a powerful platform for network simulation that gives opportunity to build strong virtual network by making experiments with network behavior. Packet Tracer is used to teach and learn complicated networking technology concepts with functionalities such as visualization, simulation, evaluation and cooperation with other users. Platform supports a lot of devices that encourages troubleshooting practice with limited physical equipments in the classrooms.

2.8 Graphical Network Simulator-3 (GNS3)

GNS3 (Graphical Network Simulator) is an open source program which provides simulation of complex networks by making it very similar to performing of real network. It is possible without using physical devices such as switches and routers. It is possible to experiment network configurations that can be integrated later on real devices.

Chapter 3

Methodology

3.1 Network Design

A number of technologies which were essential for the completion of the task were used in order to design the Network:

1. The Network Architecture
2. Network Connectivity
3. EtherChannel
4. VLAN
5. VLAN Trunking Protocol (VTP)
6. HTTP, FTP, DNS, SMTP
7. DHCP Configuration
8. Static Routing Configurations
9. Access Control Lists Configuration
10. Network Address Translation

By the help of given technologies the network works as an Enterprise Network.

3.1.1 Network Architecture

Physical Design

The physical design demonstrates network upgrade in physical topology of university including the devices their locations, and cable installation. As seen in Figure 3.1 below in the main floor of the building, the mainframe and the five servers are

in place. Router, firewall and one multilayer switch with two servers are placed in server room in main floor of university. Firewall is located inside the network because it adds stronger filtering opportunity, compared to the external firewall to protect servers and workstations from external attack. Managed Cisco Catalyst C2960 switches are used within the building. Overall there are six switchrooms each one contains four or six access switches, one of switchrooms located in dormitary, others are placed within 3 floors and also in ground floor. Access switches first connect to 3 distribution switches then these multilayer switches connect to core layer switches linked to router. The purpose of core layer switches is to manage Vlans and perform servers. This was done to avoid overload of router. The building is equipped with hubs and wireless access points in the offices, classrooms, labs, and so on that connect end devices with managed switches. There are 170 hubs and 31 access points at all.

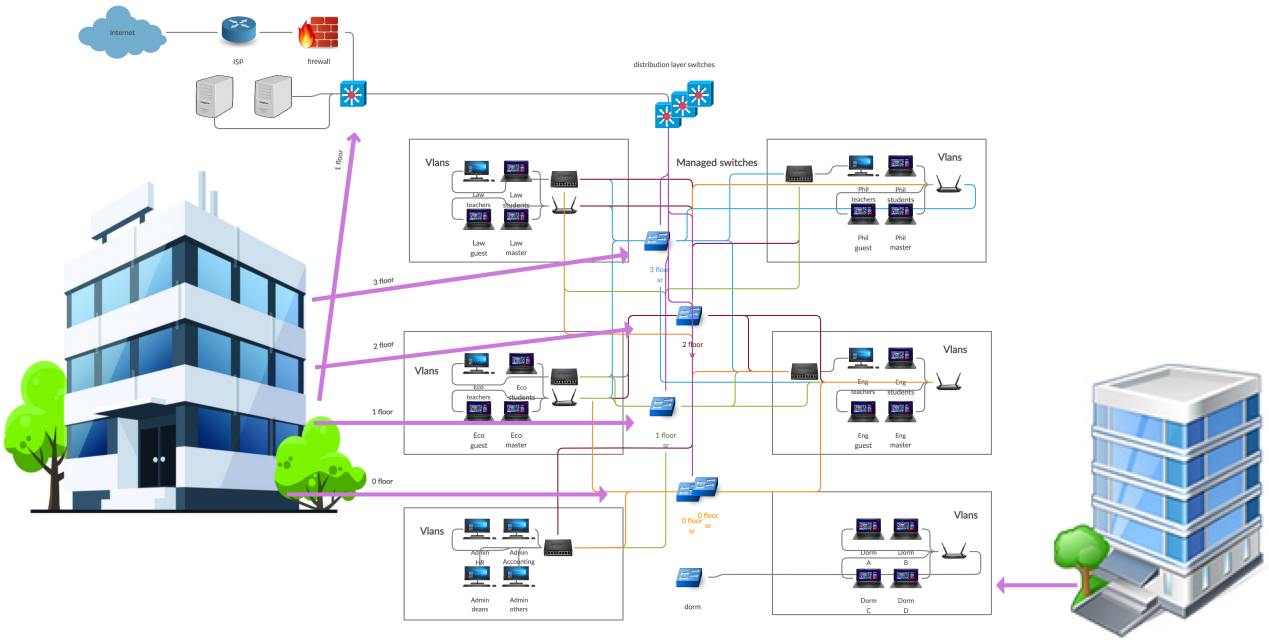


Figure 3.1: The Physical Design

Logical Design

Logical design demonstrates conceptual relationship of devices. The core layer had a router and 2 multilayer switches one of which had DHCP server and server. The distribution layer had 3 multilayer switches, 25 switches, and 6 main switches which were located in the Switch Rooms for: Administration, Law Faculty, Philology Faculty, Engineering Faculty, Economics Faculty, and for the Dormitory as in Figure 3.2. The access layer had hubs and access points where PC's could connect. Accordingly, the network was logically divided into 40 VLANs.

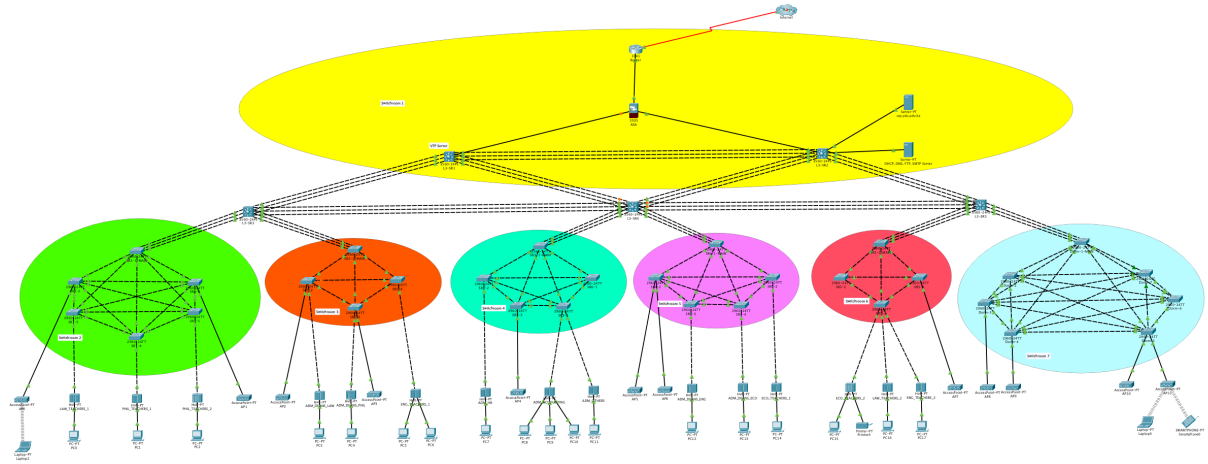


Figure 3.2: The Architectural View of the Network Design

3.1.2 Network Connectivity

In this topology, generic devices were used. At the core and distribution layer, a generic router was used as it had interfaces for straight-through connectivity for network with switches. Generic switches were also used at the access layer. Figure 3.3

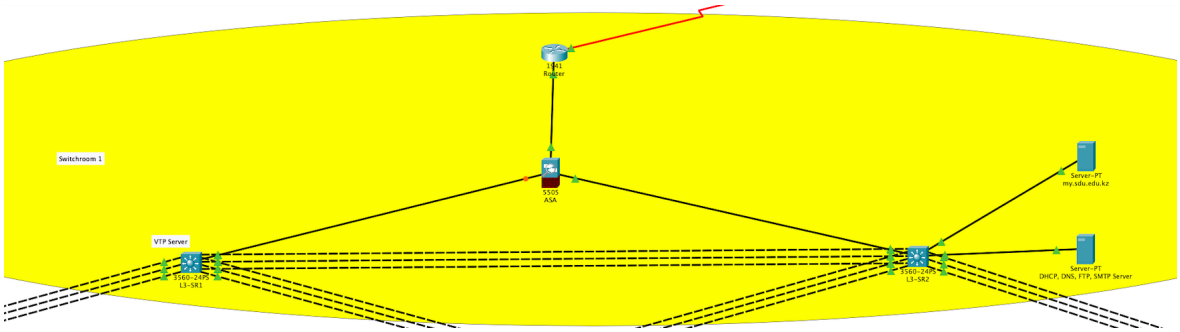


Figure 3.3: Part of the Straight-through Connectivity of the Network

3.1.3 EtherChannel

A logical link can be created utilizing several physical links between two devices, which is called link aggregation. Consequently, it allows load sharing between the physical devices.

```
L3-SR1(config) #interface range fa0/2 - 4
L3-SR1(config-if) #switchport trunk encapsulation dot1q
L3-SR1(config-if) #switchport mode trunk
L3-SR1(config-if) #channel-group 1 mode on
L3-SR1(config-if) #interface port-channel 1
```

3.1.4 Spanning Tree Protocol

We deployed STP as we need redundant links in networok in case of some failovers. Redundant links are important like backups because if primary links fail the backup links will be activated so users can keep on using the network. Hence STP prevents loops that happens due to failures by enabling on the bridges and switches. Specially we used Rapid PVST protocol as it runs an spanning-tree instance per VLAN.[5]

```
L3-SR1(config) #spanning-tree mode rapid-pvst
```

Also we add

```
L3-SR1(config) #spanning-tree portfast
L3-SR1(config) #spanning-tree enable
```

configurations in order to STP does not influence on access ports

3.1.5 VLAN

40 VLANs were divided in accordance with the Campus blocks, faculties, the year when students entered, and students' degrees (Table 3.1). The VLANs were first configured from the VLAN database by giving a number and a name to each VLAN. While distributing IP addresses, all the ports on a switch were assigned to the appropriate VLAN hence configuring it in global configuration mode as:

```
L3-SR1(config) #interface VLAN 2
L3-SR1(config-if) #IP add 10.8.0.2 255.255.192.0
```

The above configuration enabled packet transfer from and to switch interfaces.

Name	Network Address	VLANs
Administration	10.8.0.0/16	2-5
Law Faculty	10.12.0.0/16	5-13
Philology Faculty	10.16.0.0/16	14-21
Engineering Faculty	10.20.0.0/16	22-29
Economics	10.24.0.0/16	30-37
Dormitory	10.28.0.0/16	38-41

Table 3.1: VLANs table

3.1.6 VLAN Trunking Protocol (VTP)

In order to share VLAN information, we use the VTP server where VLANs already created. To get access to VLANs we configured intermediary devices as VTP Client. For instance, we chose the L3-SR1 multiplayer switch as a VTP Server and created all 40 VLANs. As a VTP Client, we took all the switches, then we get access to all VLANs.

Configuration for VTP Server:

```
L3-SR1(config) #vtp mode server
L3-SR1(config-if) #vtp domain SDU_NETWORK
L3-SR1(config-if) #vtp password cn_project2020
```

Configuration for VTP Client:

```
Dorm-2(config) #vtp mode server
Dorm-2(config-if) #vtp domain SDU_NETWORK
Dorm-2(config-if) #vtp password cn_project2020
```

3.1.7 DHCP

Server connected to an L3-SR2 multilayer switch was chosen as a DHCP server. Clients (end devices) could request the server to get the IP address dynamically. The DHCP configuration made in Figure 3.4 develops a pool with the specific name for all VLANs with the default gateway router and DNS server's IP address. In order for Layer 3 switches to receive DHCP request and forward them to a specified DHCP server the following configurations was made:

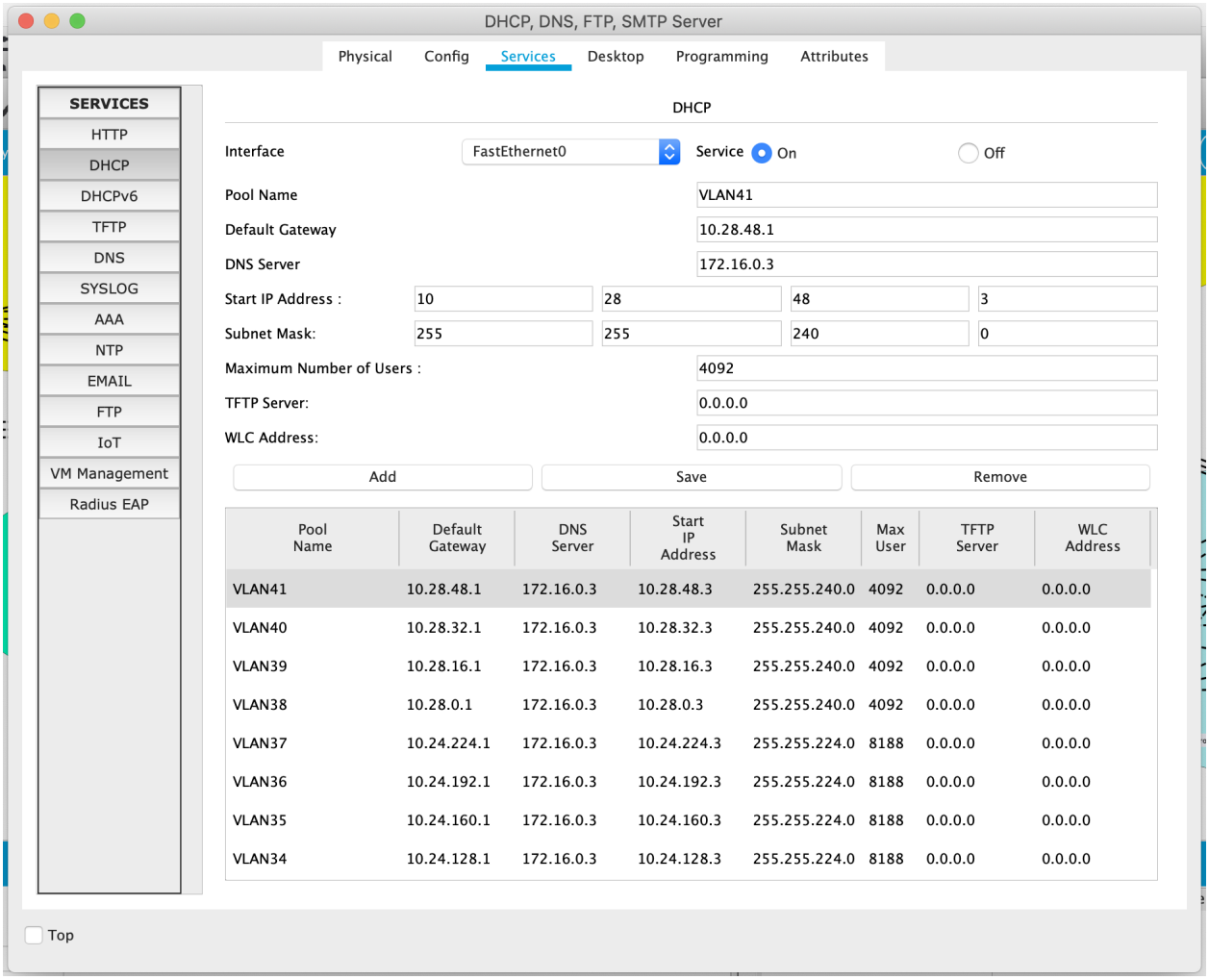
```
L3-SR1(config) #interface vlan 2
L3-SR1(config-if) #ip helper-address 172.16.0.3

L3-SR2(config) #interface vlan 2
L3-SR2(config-if) #ip helper-address 172.16.0.3
```

3.1.8 Static Routing Configuration

We configured static routing because it is the most secure method of routing. It decreases overhead from network resources by manually adding routes in routing table.

```
Router(config) #ip route 0.0.0.0 0.0.0.0 128.0.0.2
Router(config) #ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
VLAN41	10.28.48.1	172.16.0.3	10.28.48.3	255.255.240.0	4092	0.0.0.0	0.0.0.0
VLAN40	10.28.32.1	172.16.0.3	10.28.32.3	255.255.240.0	4092	0.0.0.0	0.0.0.0
VLAN39	10.28.16.1	172.16.0.3	10.28.16.3	255.255.240.0	4092	0.0.0.0	0.0.0.0
VLAN38	10.28.0.1	172.16.0.3	10.28.0.3	255.255.240.0	4092	0.0.0.0	0.0.0.0
VLAN37	10.24.224.1	172.16.0.3	10.24.224.3	255.255.224.0	8188	0.0.0.0	0.0.0.0
VLAN36	10.24.192.1	172.16.0.3	10.24.192.3	255.255.224.0	8188	0.0.0.0	0.0.0.0
VLAN35	10.24.160.1	172.16.0.3	10.24.160.3	255.255.224.0	8188	0.0.0.0	0.0.0.0
VLAN34	10.24.128.1	172.16.0.3	10.24.128.3	255.255.224.0	8188	0.0.0.0	0.0.0.0

Figure 3.4: DHCP server

3.1.9 Access Control Lists Configuration

We used Extended ACL configuration in order to deny access from students to connecting websites like the game, social media, and etc, but permit access to useful websites like google and for the administration of any websites. The configuration was used to the Router using the access-group number and inbound ACL which first of all do the ACL filtration, then routing.

```
Router(config) #access-list 111 deny icmp 10.12.0.0 0.0.31.255
host 176.9.168.239
Router(config) #access-list 111 deny icmp 10.12.0.0 0.0.31.255
host 87.240.190.67
Router(config) #access-list  111 permit ip any any
```

3.1.10 Network Address Translation

NAT overload(PAT), which translates private addresses to the public, was used in order to access the Internet with public IPv4 address. The source translation

was configured using the interface and overload keywords. To the interfaces, we used commands to identify which interface connected as outside or inside. The commands were used to the interfaces in order to define inside and outside interfaces.

```
Router(config) #ip nat inside source list 1
interface FastEthernet0/0 overload
Router(config) #interface g0/1
Router(config-if) #ip nat inside
```

3.1.11 Firewall configuration

We used firewall inside the network as security level of internal firewall is stronger. It filters traffic that goes to outside the network as well as filtering inside network traffic.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 172.16.0.5 255.255.255.240

interface Vlan2
 nameif outside
 security-level 0
 ip address 128.0.0.2 255.255.255.252

class-map inspection_default
 match default-inspection-traffic

policy-map global_policy
 class inspection_default
  inspect icmp
service-policy global_policy global
```

3.1.12 Securing network devices

Last thing that needs to be done is securing device access. For this issue we used basic security configurations such as: securing user and privileged EXEC modes with strong passwords, applying weak encryption to all the passwords in configuration file, allowing only encrypted type (SSH) of console connection. Only users that have already been created in the configuration file will be able to access devices.

```
Router(config) #username Admin privilege 15 password Adminpa123
Router(config) #enable secret passen123
Router(config) #line console 0
Router(config) #password passcon123
Router(config) #login local
Router(config) #exec-timeout 5
Router(config) #ip domain-name SDU_DOMAIN
Router(config) #crypto key generate rsa general-keys modulus 1024
Router(config) #ip ssh version 2
Router(config) #ip ssh authentication-retries 3
Router(config) #ip ssh time-out 120
Router(config) #line vty 0 4
Router(config) #login local
Router(config) #exec-timeout 5
Router(config) #transport input ssh
Router(config) #service password-encryption
Router(config) #login block-for 60 attempts 3 within 120
```

Chapter 4

Conclusion

Finally we simulated building upgraded secure and adaptive network using Suleyman Demirel University current network on packet tracer and gns3 platforms. To gain our objectives we deployed a lot of protocols and features to virtual network by considering critical vulnerable points of current network. The following items demonstrates results of configurations:

- Verify optimization techniques 4.1

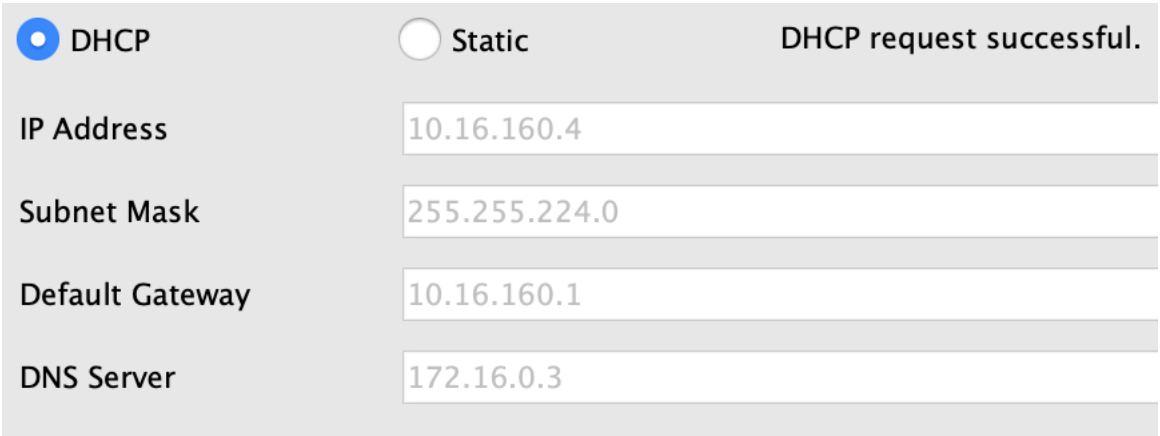


Figure 4.1: DHCP request

- Testing traffic flow from internal network
- Verify network connectivity 4.2
- Validation of LAN technologies on Router
- Verify access to the Internet through the GNS3 Figure4.3, Figure, 4.4

Network architecture and its security are significant for any organization. If we follow the hierarchical network design then network will be reliable, scalable and performance and security will be increased. In this work, we proposed effective secure campus network design based on the work environment and required scalability, security and other aspects.

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.24.160.16

Pinging 10.24.160.16 with 32 bytes of data:

Reply from 10.24.160.16: bytes=32 time=577ms TTL=128
Reply from 10.24.160.16: bytes=32 time=1ms TTL=128
Reply from 10.24.160.16: bytes=32 time=18ms TTL=128
Reply from 10.24.160.16: bytes=32 time<1ms TTL=128

Ping statistics for 10.24.160.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 577ms, Average = 149ms

C:\>
```

Figure 4.2: Internal network connection between Vlans

```
84 bytes from 64.233.161.138 icmp_seq=3 ttl=125 time=124.248 ms
*10.8.0.2 icmp_seq=4 ttl=255 time=61.583 ms (ICMP type:3, code:1, Destination ho
st unreachable)
84 bytes from 64.233.161.138 icmp_seq=5 ttl=125 time=122.610 ms

[Admin> ping stopgame.ru
stopgame.ru resolved to 176.9.168.239
84 bytes from 176.9.168.239 icmp_seq=1 ttl=125 time=186.896 ms
84 bytes from 176.9.168.239 icmp_seq=2 ttl=125 time=197.365 ms
84 bytes from 176.9.168.239 icmp_seq=3 ttl=125 time=204.971 ms
84 bytes from 176.9.168.239 icmp_seq=4 ttl=125 time=192.899 ms
84 bytes from 176.9.168.239 icmp_seq=5 ttl=125 time=213.411 ms

[Admin> ping google.com
google.com resolved to 64.233.161.113
84 bytes from 64.233.161.113 icmp_seq=1 ttl=125 time=141.647 ms
Redirect Network, gateway 10.8.0.3 -> 10.8.0.5
84 bytes from 64.233.161.113 icmp_seq=1 ttl=125 time=106.408 ms
84 bytes from 64.233.161.113 icmp_seq=2 ttl=125 time=108.365 ms
84 bytes from 64.233.161.113 icmp_seq=3 ttl=125 time=119.879 ms
84 bytes from 64.233.161.113 icmp_seq=4 ttl=125 time=134.903 ms
84 bytes from 64.233.161.113 icmp_seq=5 ttl=125 time=130.513 ms

Admin>
```

Figure 4.3: Verify access to the Internet from Admin

```
Trying 192.168.231.128...
Connected to 192.168.231.128.
Escape character is '^]'.

VPCS> ping google.com
google.com resolved to 64.233.161.101
84 bytes from 64.233.161.101 icmp_seq=1 ttl=125 time=163.962 ms
Redirect Network, gateway 10.12.0.3 -> 10.12.0.5
84 bytes from 64.233.161.101 icmp_seq=1 ttl=125 time=170.766 ms
84 bytes from 64.233.161.101 icmp_seq=2 ttl=125 time=161.250 ms
84 bytes from 64.233.161.101 icmp_seq=3 ttl=125 time=207.261 ms
84 bytes from 64.233.161.101 icmp_seq=4 ttl=125 time=236.671 ms
84 bytes from 64.233.161.101 icmp_seq=5 ttl=125 time=106.828 ms

VPCS> ping stopgame.ru
stopgame.ru resolved to 176.9.168.239
*10.8.0.5 icmp_seq=1 ttl=255 time=62.657 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.8.0.5 icmp_seq=2 ttl=255 time=32.176 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.8.0.5 icmp_seq=3 ttl=255 time=17.176 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.8.0.5 icmp_seq=4 ttl=255 time=14.020 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.8.0.5 icmp_seq=5 ttl=255 time=155.869 ms (ICMP type:3, code:13, Communication administratively prohibited)
```

Figure 4.4: Verify access to the Internet from Student

Appendix A

Appendix A

A.1 L3-SR1 multilayaer swtich configuration

```
!
interface Port-channel1
 description TO_L3-SR2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel2
 description TO_L3-SR3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 description TO_L3-SR4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode active
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 3 mode active
!
```

```
interface Vlan33
 mac-address 0001.634d.3e20
 ip address 10.24.96.1 255.255.224.0
 ip helper-address 172.16.0.3
!
interface Vlan34
 mac-address 0001.634d.3e21
 ip address 10.24.128.1 255.255.224.0
 ip helper-address 172.16.0.3
!
interface Vlan35
 mac-address 0001.634d.3e22
 ip address 10.24.160.1 255.255.224.0
 ip helper-address 172.16.0.3
!
interface Vlan36
 mac-address 0001.634d.3e23
 ip address 10.24.192.1 255.255.224.0
 ip helper-address 172.16.0.3
!
interface Vlan37
 mac-address 0001.634d.3e24
 ip address 10.24.224.1 255.255.224.0
 ip helper-address 172.16.0.3
!
interface Vlan38
 mac-address 0001.634d.3e25
 ip address 10.28.0.1 255.255.240.0
 ip helper-address 172.16.0.3
!
interface Vlan39
 mac-address 0001.634d.3e26
 ip address 10.28.16.1 255.255.240.0
 ip helper-address 172.16.0.3
!
interface Vlan40
 mac-address 0001.634d.3e27
 ip address 10.28.32.1 255.255.240.0
 ip helper-address 172.16.0.3
!
interface Vlan41
 mac-address 0001.634d.3e28
 ip address 10.28.48.1 255.255.240.0
 ip helper-address 172.16.0.3
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.0.5
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
!
```

Appendix B

Appendix B

B.1 Router configuration

```
!
!
interface GigabitEthernet0/0
 description TO_ASA
 ip address 128.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 209.100.165.1 255.255.255.252
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 128.0.0.2
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
!
!
!
!
!
!
line con 0
 exec-timeout 5 0
 password 7 08314D5D1A1A0A1943595F
 login local
!
line aux 0
!
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
line vty 5 15
 login
!
```

References

[1] Cisco Academy. “Introduction to Networks”. In: netacad.com. Chap. 11.1.

[2] Cisco Academy. “Routing and Switching Essentials”. In: netacad.com. Chap. 1.1.

[3] Cisco Academy. “Routing and Switching Essentials”. In: netacad.com. Chap. 4.2.

[4] Cisco Academy. “Scaling Networks”. In: netacad.com. Chap. 2.3.

[5] *Campus Network for High Availability Design Guide*. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html. (accessed: 10.04.2020).

[6] *Enterprise Campus 3.0 Architecture: Overview and Framework*. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html. (accessed: 03.04.2020).

[7] *Hierarchical Network Design-Layer of The Hierarchical Network Design Model*. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html. (accessed: 03.04.2020).