****

2021

Computing Department, Letterkenny Institute of Technology, Port Road, Letterkenny, Co. Donegal, Ireland.

**Report for Security SCI assignment -**

**- secure LAN and WAN connectivity**

**Author : Konrad Jeziorski (L00169649)**

**Course title : Secure Communication Infrastructure (2021/22)**

**Lecturer’s name : Saim Ghafoor**

**Packet Tracer Ver. : 7.3.1.0362**

**Date Submitted : December 12, 202****1**

Table of Contents

[1. Summary 3](#_Toc90245037)

[2. Introduction 3](#_Toc90245038)

[3. General network specification 3](#_Toc90245039)

[3.1. Components 3](#_Toc90245040)

[3.2. Features of the LAN network 3](#_Toc90245041)

[3.3. Hierarchical network model 4](#_Toc90245042)

[3.4. Structured Cabling 4](#_Toc90245043)

[3.5. Distribution Point 4](#_Toc90245044)

[4. Audit 5](#_Toc90245045)

[4.1. Purpose and design assumptions 5](#_Toc90245046)

[4.2. The floor plan of the building 6](#_Toc90245047)

[4.3. VLAN allocation 6](#_Toc90245048)

[4.4. Cabling and network sockets 7](#_Toc90245049)

[4.5. MDF and IDFs 8](#_Toc90245050)

[4.5.1. Characteristics and evaluation 8](#_Toc90245051)

[4.5.2. MDF topology 9](#_Toc90245052)

[4.5.3. Specification of network devices 10](#_Toc90245053)

[5. Building a LAN 15](#_Toc90245054)

[5.1. Subnetting and Addressing 15](#_Toc90245055)

[5.2. Topology 15](#_Toc90245056)

[5.3. End Devices layer 15](#_Toc90245057)

[5.4. Distribution and Core layers 17](#_Toc90245058)

[6. Over the LAN network – ASA and Outside and DMZ 19](#_Toc90245059)

[6.1. Routing 19](#_Toc90245060)

[6.2. Firewalls 19](#_Toc90245061)

[6.2.1. ASA1 19](#_Toc90245062)

[6.2.2. ASA2 23](#_Toc90245063)

[6.2.3. Outside 24](#_Toc90245064)

[6.2.3. DMZ 24](#_Toc90245065)

[7. Security implementation and configuration 25](#_Toc90245066)

[7.1. Secured LAN 25](#_Toc90245067)

[7.1.2. Native VLAN 25](#_Toc90245068)

[7.1.3. Guard Root 25](#_Toc90245069)

[7.1.4. Port Security 26](#_Toc90245070)

[7.1.5. VLANs and security 26](#_Toc90245071)

[7.1.5. Access Control Lists 26](#_Toc90245072)

[7.1.6. Passwords 27](#_Toc90245073)

[7.1.7 Failover 28](#_Toc90245074)

[7.2. ASAs 28](#_Toc90245075)

[8. Conclusion 32](#_Toc90245076)

[9. References 33](#_Toc90245077)

[10. Appendix – Connectivity tests 34](#_Toc90245078)

[10.1. Communication between VLANs 34](#_Toc90245079)

[10.2. Telnet Access 34](#_Toc90245080)

[10.3. FTP Access 35](#_Toc90245081)

[10.4. DNS, HTTP Access 35](#_Toc90245082)

[10.5. Connectivity (ICMP) between Inside, Outside, and DMZ 36](#_Toc90245083)

[10.6. Test - access to the server in the DMZ from Outside 36](#_Toc90245084)

# Summary

This report provides detailed descriptions, procedures, and configurations for designing a LAN for an office building as an extension of a corporate network located in another city. Particular emphasis is placed here on matters related to a secure WAN network. As a network administrator, I have tried to meet these expectations. in the first step I designed the LAN network, then I devoted a lot of attention to the secure connection of the corporate network, I used tools such as Firewall and DMZ to control the network traffic and the servers to be well secured in the WAN network.

# Introduction

The ordering party for the project is EXCEL FINANCE, operating in the financial investment industry, where customer and employee data is very important. Their headquarters are in Dublin, but they want to expand to County Donegal. They require an established network design with conference rooms, department offices, executive and administrative offices. Their office is located on the ground floor of the building. The building is 100 m east-west and 80 m north-south. The height of the storey is 4 meters. They expressed a concern for network security, so this is an important part when designing. Therefore, the goal of the network administrator is to plan the LAN design and strategy for secure network deployment.

# General network specification

## 3.1. Components

Components of a computer network can be divided into two groups: active and passive devices. Active network devices are those that either generate or modify the signal transmitted over the network. Passive, in turn, are network elements that carry the signal, but do not modify it.

Examples:

Active elements: Routers, Switches, Access Points, Servers.

Passive components: Transmission media (cables), Patch panel, Rack, Socket.

## 3.2. Features of the LAN network

A well-designed and constructed computer network should have certain features that determine its quality, the most important features include:

* scalability,
* redundancy,
* performance,
* security,
* ease of maintenance and management.

More on this subject, along with a description of individual network features, can be found here [>>>](https://students.mimuw.edu.pl/~zbyszek/sieci/CCNA4%20Sample.pdf) [[1]](#footnote-1)

## 3.3. Hierarchical network model

When designing a computer network, you can use the model proposed by experts. This model assumes the use of 3 layers: core layers, distribution layers, access layer.

* the access layer enables end devices such as computers to access the network. Switches to which end devices are connected are usually located close to end devices,
* the distribution layer mediates data exchange between the access layer and the core layer,
* the core layer takes on traffic from the entire network and delivers data to the local network and beyond.

## 3.4. Structured Cabling

As we already know, a computer network consists of active and passive elements. Passive network elements do not interfere with the signal but can only transport it. All the passive elements of the network make up a whole called structured cabling. Structured cabling consists of:

* horizontal cabling,
* vertical cabling,
* campus (inter-building) cabling,
* distribution points,
* network sockets.

In this project, I will focus on the use of horizontal cabling, so it is worth describing this type of cabling a bit. Horizontal cabling is the part of structured cabling that connects the network sockets located at the office stand with the distribution point on the same floor. Mains cables run from all sockets to the patch panel located in the distribution point. The horizontal cabling system includes, apart from the mains cable, sockets, and the patch panel, also connection cables and station cables. They are used to connect a switch with a patch panel, as well as a socket with a computer. These cables, called patch cords, are terminated with RJ45 terminals. Assuming that the horizontal cabling system is based on a twisted pair cable, you can come across shielded (F/UTP) and unshielded (U / UTP) patch cords. When using copper cables, i.e. twisted pair, we must remember about the maximum length of the cable. If we use the FastEthernet and GigabitEthernet standards in the network, the maximum distance between the switch and the computer cannot be longer than 100 meters.

## 3.5. Distribution Point

Distribution points are where the cabling from the network segment converges. Distribution cabinets (RACK), in which all network equipment are mounted, are installed in distribution points. This is where servers and routers are stored, Internet access is provided, and structured cabling converges here. According to the standards, the rooms for distribution points should not be smaller than: 3 meters in length, 2.6 meters in height, 2.2 meters in width.[[2]](#footnote-2)

For the designed network to be consistent with the previously described features, it is necessary to mark the sockets and ports to which the other end of the cable has been attached in the patch panel. This marking will make it easier to find individual wires in the future.

# Audit

## 4.1. Purpose and design assumptions

* The purpose of designing and implementing a local computer network for an office building is to provide reliable access to the hardware resources of the company's network and enabling access to the Internet for all employees of the company. In addition, the rights in it should be limited, in accordance with the provisions of the client. As already mentioned, the network MUST be secure. We already know the size of the floor on which the LAN is to operate.
* The number of computers assigned to IP addresses corresponds to the number of employees, but more employees are expected to be hired, therefore the number of network sockets in individual departments should be increased. For every 10m2 of office space, I have tried to put at least one socket (according to the standard).
* The company already has an internet connection provided by XXXX.
* The project does not involve the implementation of electrical installations. We assume that it has been modernized and meets all the requirements for this type of installation confirmed by a certificate.
* The cabling of the network will be based on the F/UTP, cat. 6 cable for network sockets, while the cabling for MDF and IDF will be based on the U/UTP, cat. 5e cable.
* The following will be installed in MDF: routers, switches, servers, patch panels, ASA. I also recommend adding a UPS.

## 4.2. The floor plan of the building

Diagram, engineering drawing

Description automatically generated

## 4.3. VLAN allocation

I decided to assign individual offices and departments to different VLANs. Here they are:

VLAN 10 - Employee: Employee Room 1, Employee Room 2

VLAN 20 - HR: HR Room

VLAN 30 - Finance: Finance Room

VLAN 40 - Management: Manager / Admin Room, Reception, Hallway (printers)

VLAN 50 - Consultation: Conference Room

Canteen, Toilets, Stairs will not be assigned to any VLANs, because there is no such need (they do not even have access to network sockets).

Addressing and connection specification of individual VLANs are available in the attached documentation: [Connection Addressing](C:\\Users\\Konrad\\SkyDrive\\Gotowe nie kasować!\\Connection Addressing.ods), [Subnetting for LAN](file:///C:\Users\Konrad\SkyDrive\Gotowe%20nie%20kasować!\Lan%20Design%20do%20CA.ods).

## 4.4. Cabling and network sockets

A picture containing text, wall, indoor, different

Description automatically generated

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Port designation | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 | B1 | B2 | B3 | B4 |
| Cable length | 10 | 10 | 20 | 20 | 20 | 20 | 30 | 30 | 40 | 40 | 10 | 10 | 15 | 15 |
| Port designation | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | E1 | E2 | F1 | F2 |
| Cable length | 10 | 10 | 10 | 10 | 20 | 20 | 25 | 25 | 30 | 30 | 15 | 15 | 60 | 60 |
| Port designation | G1 | G2 | G3 | G4 | G5 | G6 | G7 | G8 | G9 | G10 | H1 | H2 | H3 | H4 |
| Cable length | 20 | 20 | 30 | 30 | 40 | 40 | 50 | 50 | 70 | 70 | 10 | 10 | 15 | 15 |
| Port designation | H5 | H6 | H7 | H8 | H9 | H10 | I1 | I2 | I3 | I4 | I5 | I6 | I7 | I8 |
| Cable length | 15 | 15 | 25 | 25 | 35 | 35 | 60 | 60 | 60 | 60 | 70 | 70 | 90 | 90 |

A total of 1,991 meters for sockets - 1,810 meters plus 10% redundant cable.

MDF: 10 meters of F/ UTP, Cat. 6 cable, including 10% redundancy, 2 meters of U/UTP Cat. 5e cable,

IDF1-MDF: 166 meters of F/UTP, Cat. 6 cable, including 10% redundancy,

IDF2-MDF: 178 meters of F/UTP, Cat. 6 cable, including 10% redundancy. \*

**Total cable size for U/UTP Cat. 5e – 1,993 meters**

**Total cable size for F/UTP, Cat. 6 – 354 meters**

\* The required length for MDF and IDF is calculated from the diagram presented in the next section.

Category 6 (F UTP, Cat. 6) twisted-pair cabling will enable a transfer rate of 1 Gb/s. The use of a shielded cable will also eliminate any interference generated by devices operating in the building. Unshielded twisted pair, category 5e (U/UTP, Cat.5e) will be used as the wiring to the sockets.

## 4.5. MDF and IDFs

### 4.5.1. Characteristics and evaluation

The active network devices used guarantee the reliability and efficiency of the network. In the core layer, two 3650-24PS Multi-Layer Switches work in parallel, in the event of failure of one of them, its tasks will be taken over by the other (I used redundancy).

The following devices will be used in the network:

* 3 x CISCO2911/K9 routers - with two Gigabit Ethernet ports, as well as free slots for expansion modules,
* 3 x WS-C3650-24PS-S Multi-Layer Switches - is the ideal access layer switch for small businesses with LAN access or office environments, combining 10/100/1000 and PoE configurations for maximum productivity and investment protection.
* 4 x Cisco Catalyst 2960X-24PS-L– those series switches provide branch office services to conventional office workspaces. They can work in the GigabitEthernet standard.
* 2 x Dell PowerEdge T1100 Rack Server - with a 4-core processor, 16 GB of RAM and two disks, each with 2 TB
* The Liebert PSI 3000VA (3kVA) UPS
* Cable organizer
* 42U RACK cabinet, TiRAX model.

Active devices will be connected with each other with an excess number of wires, thanks to which the trouble-free operation of the network will be ensured. Two CISCO 2911 switches with patch panels will be placed in an Intermediate Distribution Frame (IDF) each. All but these two switches will be placed on the Main Distribution Frame (MDF).

Two IDFs will be connected to the MDF. MDF will also act as IDF for printers in the hallway, conference room and HR office.

IDF1 will include: Employee Room1 and Manager/Admin Room, and IDF1 will be connected to the sockets in Finance Room, Employee Room2 and the Reception.

The network was made in an extended star topology, it will be based on MDF, which will be located in a well-protected room at the end of the corridor. It has no windows and requires multi-factor authentication to access it. In order to maintain the correct operating temperature and air humidity in the Control Room, the Midea MUB-36HRN1-R/MOU-36HN1-Rair conditioner will be installed.

### 4.5.2. MDF topology

Diagram, schematic

Description automatically generated

### 4.5.3. Specification of network devices

* Cabinet, 19", 42U, 'TiRAX cool-roof', 2000x800x800 mm (height,width,depth), IP 54, w/air conditioning [[3]](#footnote-3)

Text

Description automatically generated with medium confidence

* Midea MUB-36HRN1-R / MOU-36HN1-R[[4]](#footnote-4)

Text

Description automatically generated

* Liebert PSI 3000VA Rackmount/Tower UPS[[5]](#footnote-5)

Table

Description automatically generated

* WS-C3650-24PS-S[[6]](#footnote-6)

Table

Description automatically generated

* Cisco Catalyst 2960X-24PS-L[[7]](#footnote-7)

Text

Description automatically generated

* CISCO2911/K9

Text

Description automatically generated with medium confidence

* Dell PowerEdge T1100 Rack Server [[8]](#footnote-8)

Table

Description automatically generated

# Building a LAN

To take a closer look at the process of building a LAN, let me walk you through the Cisco Packet Tracer simulator. I will show the configuration of the devices selected above, network functionality and, of course, applications related to its security.

## 5.1. Subnetting and Addressing

All IP addresses, subnetting, VLANs, etc. can be found in the sheets attached to the project: [Connection Addressing](file:///C:\Users\Konrad\SkyDrive\Gotowe%20nie%20kasować!\Connection%20Addressing.ods), [Subnetting for LAN](file:///C:\Users\Konrad\SkyDrive\Gotowe%20nie%20kasować!\Lan%20Design%20do%20CA.ods).

## 5.2. Topology

Diagram

Description automatically generated

## 5.3. End Devices layer

I started by allocating individual departments to VLANs, according to their purpose. I combined some rooms or parts of devices from different locations of the building into a shared VLAN. I believe that dividing them into smaller VLANs would not be too necessary here.

Switch1 is in IDF1, Switch two is in MDF, and Switch 3 is located in IDF2.

The diagram below shows the individual VLANS and the access devices.

Chart, radar chart

Description automatically generated

An example of the configuration (command lines for creating VLANs with addressing) on the Switch is given below.

config terminal

vlan 10

name Employee

vlan 20

name HR

vlan 30

name Finance

vlan 40

name Management

vlan 50

name consultastion

int range fa0/1-10

switchport mode access

switchport access vlan 10

int range fa0/11-14

switchport mode access

switchport access vlan 40

int vlan 10

ip address 192.168.0.1 255.255.255.224

int vlan 20

ip address 192.168.0.33 255.255.255.240

int vlan 30

ip address 192.168.0.49 255.255.255.240

int vlan 40

ip address 192.168.0.65 255.255.255.240

int vlan 50

ip address 192.168.0.81 255.255.255.240

## 5.4. Distribution and Core layers

After assigning each department to a VLAN, I configure the distribution layer along with the core layer.

Diagram

Description automatically generated

I designate the traffic network here. I connect all 3 Switches 2960 with each Multilayer Switch, and I also connect these with each other. Thus, we have redundant connections. From now on, in case of failure of one of the cables connecting the lower switches with the multilayer switch, the transmission will go through another. MultiSwitch2 works as Primary Root here, which means that traffic from all lower switches goes to it first. I used Router On The Stick here, it is a method of routing between VLANs. It has a single physical or logical connection to the network, in other words, the router is connected to the switch with a single cable. This diverts traffic between locally attached hosts in separate logical routing domains. The discussed configuration on Multi-Switch and Router is listed below.

**MultiSwitch2**

config terminal

vlan 10

name Employee

vlan 20

name HR

vlan 30

name Finance

vlan 40

name Management

vlan 50

name Consultation

spanning-tree vlan 1-4094 root primary

int range g1/0/1-24

spanning-tree guard root

int range g1/1/1-4

spanning-tree guard root

**Router1**

int g0/0.10

encapsulation dot1Q 10

ip address 192.168.0.30 255.255.255.224

exit

int g0/0.20

encapsulation dot1Q 20

ip address 192.168.0.46 255.255.255.240

exit

int g0/0.30

encapsulation dot1Q 30

ip address 192.168.0.62 255.255.255.240

exit

int g0/0.40

encapsulation dot1Q 40

ip address 192.168.0.78 255.255.255.240

exit

int g0/0.50

encapsulation dot1Q 50

ip address 192.168.0.94 255.255.255.240

exit

int g0/0

no shut

int gi0/1

ip address 10.0.0.1 255.255.255.248

no shut

# Over the LAN network – ASA and Outside and DMZ

Before we discuss the firewall application in detail, let's create a connection with the company's headquarters and DMZ, also known as a separate server zone (server farm).

## 6.1. Routing

First of all, we need to create routing on all servers and ASAs. I used RIP on local networks, and I used BGP for WAN connection. Border Gateway Protocol (BGP) refers to a gateway protocol that allows the Internet to exchange routing information between autonomous systems (AS). BGP enables peering. Special BGP attributes allow for greater flexibility and to make complex decisions about choosing the best routes. RIP is a distance vector routing protocol but has a slow convergence time.

Examples of routing commands below.

**Router1 (RIP)**

Router rip

Network 192.168.0.0

Network 192.168.0.32

Network 192.168.0.48

Network 192.168.0.64

Network 192.168.0.80

Network 209.165.200.224

**Router2 (BGP)**

Router bgp 65000

bgp log-neighbor-changes

no synchronization

neighbor 21.0.0.2 remote-as 65001

network 20.0.0.0 mask 255.255.255.248

## 6.2. Firewalls

CISCO ASA, next to routers and switches, is another network device whose main task is to protect our network against intruders and unauthorized access. This protection works by blocking illegal network traffic. The ASA device in the network controlled by us acts as a firewall.

### 6.2.1. ASA1

This firewall is to protect our network against access from outside and from the DMZ. I have defined a set of rules protecting the local network against unauthorized access from the DMZ zone and the Outside zone, ensuring simultaneous access to them.

**ASA1 configuration**

hostname ASA

int gi1/1

no ip address

no nameif

no security-level

exit

int gi1/2

no nameif

no security-level

no ip address dhcp

exit

int gi1/3

no nameif

no security-level

no ip address dhcp

exit

int gi1/1

ip address 10.0.0.2 255.255.255.248

nameif Inside

security-level 100

no shut

exit

int gi1/2

ip address 20.0.0.2 255.255.255.248

nameif Outside

security-level 0

no shut

exit

int gi1/3

ip address 11.0.0.2 255.255.255.248

nameif DMZ

security-level 70

no shut

exit

Router rip

Network 10.0.0.0

Network 11.0.0.0

Network 20.0.0.0

object network INSIDE-NET

subnet 192.168.0.0 255.255.255.224

subnet 192.168.0.32 255.255.255.240

subnet 192.168.0.48 255.255.255.240

subnet 192.168.0.64 255.255.255.240

subnet 192.168.0.80 255.255.255.240

subnet 10.0.0.0 255.0.0.0

nat (inside,outside) dynamic interface

exit

conf t

class-map inspection\_default

match default-inspection-traffic

exit

policy-map global\_policy

class inspection\_default

inspect icmp

exit

service-policy global\_policy global

policy-map global\_policy

class inspection\_default

inspect http

exit

policy-map global\_policy

class inspection\_default

inspect dns

exit

policy-map global\_policy

class inspection\_default

inspect ftp

exit

conf t

object network INSIDE-DMZ

subnet 192.168.0.0 255.255.255.224

subnet 192.168.0.32 255.255.255.240

subnet 192.168.0.48 255.255.255.240

subnet 192.168.0.64 255.255.255.240

subnet 192.168.0.80 255.255.255.240

subnet 10.0.0.0 255.0.0.0

nat (inside,dmz) dynamic interface

exit

conf t

class-map inspection\_inside\_dmz

match default-inspection-traffic

exit

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect icmp

exit

conf t

service-policy inside\_dmz\_policy interface inside

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect http

exit

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect dns

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect ftp

exit

object network DMZ-OUTSIDE

subnet 11.0.0.0 255.255.255.248

subnet 192.168.80.0 255.255.255.0

nat (dmz,outside) dynamic interface

exit

conf t

class-map inspection\_dmz\_outside

match default-inspection-traffic

exit

policy-map dmz\_outside\_policy

class inspection\_dmz\_outside

inspect icmp

exit

service-policy dmz\_outside\_policy interface dmz

policy-map dmz\_outside\_policy

class inspection\_dmz\_outside

inspect http

inspect dns

inspect ftp

exit

### 6.2.2. ASA2

The second firewall is on the Dublin side. I assumed they had agreed to set the ASA Security Level to 0 during testing so that I could check our communication with their network.

### 6.2.3. Outside

On this side I put one computer and a server. The connection of devices is similar to our side, the Switch connected to the Multi-Layer Switch and the Routers going towards the WAN.

Diagram

Description automatically generated

### 6.2.3. DMZ

Here is a server farm and internet access. It is important that this part of the network is well secured. There are two servers here, one of which has only FTP service. The second one has active DHCP (used only on the DMZ side), DNS, HTTP, SYSLOG, NTP.

Access to this zone is possible only from the Inside zone (from our LAN network). Later, I will assign the access control list to the ASA for the outside computer so that it can also access one of the server's services.

Diagram

Description automatically generated

# Security implementation and configuration

Once we have the entire network created with proper routing, we should focus on its security. I will break this chapter down into sections. First, I will discuss the designed LAN network, I will determine the appropriately selected permissions for individual VLANs.

## 7.1. Secured LAN

Let's focus on the correct security and configuration of our switches, starting from the end point. After that we will go up to the router and then to the firewall.

### 7.1.2. Native VLAN

The default native VLAN on CISCO switches is VLAN 1, the one to which all switch ports belong before virtual networks are implemented. Good network security practice is to move the native VLAN to a different network than the default one, preferably one that is separated from other VLANs, of course only when the native VLAN does not carry some actual traffic that is desired in the network. Trunks, known as 802.1Q buses, can handle traffic from different VLANs, tagged traffic, but also traffic outside of the VLAN.

The commands must be executed on each Switch that has a VLANs assigned to it, each connected port.

**Configuration example on Switch1**

interface GigabitEthernet0/1

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,30,40,50,99

switchport mode trunk

interface GigabitEthernet0/2

switchport trunk native vlan 99

switchport trunk allowed vlan 10,20,30,40,50,99

switchport mode trunk

### 7.1.3. Guard Root

Root Guard is an STP feature that is enabled for each port. Prevents the configured port from becoming the root port. Root Guard prevents a switch (often misconfigured or bogus) from becoming a root bridge in a topology.

**guard root configuration on Multi-Layer Switch 2**

int range g1/0/1-24

spanning-tree guard root

int range g1/1/1-4

spanning-tree guard root

### 7.1.4. Port Security

Port Security is a type of security that allows you to transmit frames only to trusted devices, not everyone connected to the switch. Thanks to the appropriate configuration of this functionality, we will secure the network in such a way that only one computer can use a given port. The switch saves the MAC addresses of individual computers as trusted. I decided to assign a security port for the Management Department on Switch1 (Manager/Admin Office), because the most important data flows through these ports, incl. only here and only from one host is it possible to access telnet.

**Security port commands used on Switch1**

int range fa0/11-14

switchport mode access

switchport port-security

switchport port-security maximum 1

switchport port-security mac-address sticky

switchport port-security violation shutdown

### 7.1.5. VLANs and security

By creating VLANs, we divide our network into many smaller logical parts. In addition, we reduce the number of devices participating in the broadcast, and thus maintain the efficiency of our network at a high level. We can assign appropriate permissions for each VLAN allowing access to special resources and in the case of using security solutions.

### 7.1.5. Access Control Lists

I used all the following access control lists commands on the main LAN router (Router1)

* **No communication between VLANs 10 and 30.** In accordance with the ordering party's instructions, I limited unnecessary communication between the Employee and Finance Departments.

ip access-list extended Block\_Emp-Fin

deny ip 192.168.0.0 0.0.0.31 any

permit ip any any

exit

int g0/0.30

ip access-group Block\_Emp-Fin OUT

* **No access to FTP Server for VLANs 10 and 50**. Some departments should be blocked from accessing important corporate files on the FTP server.

ip access-list extended ftp10

deny tcp 192.168.0.0 0.0.0.31 host 192.168.80.2 eq ftp

permit ip any any

exit

int g0/0.10

ip access-group ftp10 IN

exit

ip access-list extended ftp50

deny tcp 192.168.0.80 0.0.0.15 host 192.168.80.2 eq ftp

permit ip any any

exit

int g0/0.50

ip access-group ftp50 IN

exit

* **Telnet access.** Telnet is an internet protocol that allows you to connect to another computer on your local network or the Internet. Take measures to protect your computer from unauthorized remote access. It is important that it is available only to an authenticated user, and that the password to it is encrypted.

line vty 0 4

password MyTelnet

login

exit

ip access-list extended AdminTelnet

10 permit tcp host 192.168.0.68 any eq telnet

line vty 0 4

access-class AdminTelnet in

exit

7.1.6. Passwords

It is good practice to use passwords to access all network devices.

Below I provide passwords for routers, switches, as well as server services in our LAN network.

All Routers in LAN: excel

All Switches: excel

FTP Server: user: excel, password: excel

Telnet: MyTelnet

line con 0

password excel

logging synchronous

login

history size 10 #*sets the number of previous commands stored in the session history*

exec-timeout 6 50 #*after 410 seconds of inactivity, the session will be disconnected, and the user will need to supply the console password to log back in*

exit

### 7.1.7 Failover

I mentioned earlier about using additional connections to ensure network reliability. I could increase the reliability of the LAN by adding another cable that would connect Multilayer Switch1 with Router1, then I would have to add a cross-over cable length of 1 meter. I leave the decision for analysis; it would also require adding the configuration on the GigabithEthernet0/2 port of the Router.

## 7.2. ASAs

Cisco ASA is a security platform that implements, among others firewall functions. I have configured traffic on ASA ports. Anyone who tries to access our network from outside and from the DMZ is blocked, but at the same time has access to them. It is a good practice to protect the network against unauthorized intrusion, thanks to which the network is very well secured. This is how ASA firewalls work.

Below I present the ASA1 configuration.

hostname ASA

int gi1/1

no ip address

no nameif

no security-level

exit

int gi1/2

no nameif

no security-level

no ip address dhcp

exit

int gi1/3

no nameif

no security-level

no ip address dhcp

exit

int gi1/1

ip address 10.0.0.2 255.255.255.248

nameif Inside

security-level 100

no shut

exit

int gi1/2

ip address 20.0.0.2 255.255.255.248

nameif Outside

security-level 0

no shut

exit

int gi1/3

ip address 11.0.0.2 255.255.255.248

nameif DMZ

security-level 70

no shut

exit

Router rip

Network 10.0.0.0

Network 11.0.0.0

Network 20.0.0.0

object network INSIDE-NET

subnet 192.168.0.0 255.255.255.224

subnet 192.168.0.32 255.255.255.240

subnet 192.168.0.48 255.255.255.240

subnet 192.168.0.64 255.255.255.240

subnet 192.168.0.80 255.255.255.240

subnet 10.0.0.0 255.255.255.248

nat (inside,outside) dynamic interface

exit

conf t

class-map inspection\_default

match default-inspection-traffic

exit

policy-map global\_policy

class inspection\_default

inspect icmp

exit

service-policy global\_policy global

policy-map global\_policy

class inspection\_default

inspect http

exit

policy-map global\_policy

class inspection\_default

inspect dns

exit

policy-map global\_policy

class inspection\_default

inspect ftp

exit

conf t

object network INSIDE-DMZ

subnet 192.168.0.0 255.255.255.224

subnet 192.168.0.32 255.255.255.240

subnet 192.168.0.48 255.255.255.240

subnet 192.168.0.64 255.255.255.240

subnet 192.168.0.80 255.255.255.240

subnet 10.0.0.0 255.255.255.248

nat (inside,dmz) dynamic interface

exit

conf t

class-map inspection\_inside\_dmz

match default-inspection-traffic

exit

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect icmp

exit

conf t

service-policy inside\_dmz\_policy interface inside

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect http

exit

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect dns

policy-map inside\_dmz\_policy

class inspection\_inside\_dmz

inspect ftp

exit

object network DMZ-OUTSIDE

subnet 11.0.0.0 255.255.255.248

subnet 192.168.80.0 255.255.255.0

nat (dmz,outside) dynamic interface

exit

conf t

class-map inspection\_dmz\_outside

match default-inspection-traffic

exit

policy-map dmz\_outside\_policy

class inspection\_dmz\_outside

inspect icmp

exit

service-policy dmz\_outside\_policy interface dmz

policy-map dmz\_outside\_policy

class inspection\_dmz\_outside

inspect http

inspect dns

inspect ftp

exit

It is also a good practice to secure ASA by adding a password on it. This is done with the command: *enable password*

# Conclusion

Reliable, efficient, functional, and secure network infrastructure is the basis of every company today. All network services critical to maintaining business continuity are based on a well-designed and implemented computer network. Properly designed infrastructure should meet business expectations and ensure business continuity. The proper functioning of the network is influenced by many interdependent factors that should be considered already at the LAN design stage.

However, it should be remembered that the implementation of appropriate devices along with the correct configuration of their functionality is not everything. Current analysis and planning, appropriate policies, and procedures and, above all, competent IT staff also count.

The corporate network is a dynamic environment that evolves with the development of each enterprise. The bandwidth requirements of LAN / WAN connections are increasing regularly. It may be necessary from time to time to implement new systems that will improve and optimize work. Such infrastructure requires further analysis and interference with the existing architecture.

Excel Finance should take these facts into account.

The project includes this report, a simulation performed in Cisco Packet Tracer version 7.3.1, worksheets that can help you locate ports, understand addressing and routing.

# References

Students.mimuw.edu.pl, *Introducing Network Design Concepts*, Available at: <https://students.mimuw.edu.pl/~zbyszek/sieci/CCNA4%20Sample.pdf>

DukeIOT, FEB 2016, *Communication Facilities Construction Design Standards*, Available at: <https://oit.duke.edu/sites/default/files/atoms/files/Design_2016.pdf>

Atel-electronics.eu, *Server Cabinet, rack 19", 42U, 'TiRAX cool-roof', 2000x800x800 mm (height,width,depth), IP 54, w/air conditioning,* Available at:<https://www.atelelectronics.eu/produkt.php?hash=06215>

Specsan.com, *Midea MUB-36HRN1-R / MOU-36HN1-R Air conditioning specs, reviews and features*, Available at: <http://specsan.com/air-conditioners-midea/midea-mub-36hrn1-r-mou-36hn1-r/>

Ecopowersupplies.com, *Emerson Liebert PSI 3000VA Rackmount/Tower UPS UPS Systems | PS3000RT3-230*, Available at: <https://www.ecopowersupplies.com/emerson-network-power/liebert-psi-3000va-rackmount-tower-ups>

Issuu, *Cisco catalyst 3650 24ps s datasheet*, Available at: <https://issuu.com/routerswitch5/docs/cisco_catalyst_3650-24ps-s_datashee>

www.elara.ie/, *Buy Online - WS-C2960X-24PS-L - CISCO Cisco Catalyst 2960X-24PS - Elara Online Ireland*, Available at: <https://www.elara.ie/productdetail.aspx?manufacturer=CISCO&mancode=WS-C2960X-24PS-L>

Slideshare.net, *Dell poweredge t110 spec sheet*, Available at: <https://www.slideshare.net/PascalJanot/dell-poweredge-t110-spec-sheet>

Saim Ghafoor, *COMM\_IT801 - LY\_ICYBR\_B: Secure Communication Infrastructure (2021/22),* Available at: <https://lyitbb.blackboard.com/ultra/courses/_52520_1/cl/outline>

# 10. Appendix – Connectivity tests

## 10.1. Communication between VLANs

Graphical user interface, application

Description automatically generated

Successful! VLAN10 can’t ping VLAN30 (as we wanted), the rest of the VLANs are pinging with each other.

## 10.2. Telnet Access

Graphical user interface, text

Description automatically generated

Successful! Only host Manager/Admin can telnet.

## 10.3. FTP Access

Graphical user interface, application

Description automatically generated

Successful! VLAN20, 30, 40 can reach FTP (as we wanted)

## 10.4. DNS, HTTP Access

Graphical user interface, application, Word

Description automatically generated

Successful! Computers on our network can use DNS and HTTP services of the DMZ server as well as on the Dublin side. The DMZ computer can use DNS and HTTP services from the Dublin server.

## 10.5. Connectivity (ICMP) between Inside, Outside, and DMZ

A screenshot of a computer

Description automatically generated with medium confidence

Successful!

Inside can ping Outside and DMZ,

Outside can't ping Inside and Outside,

DMZ can't ping Inside but can ping Outside.

## 10.6. Test - access to the server in the DMZ from Outside

By introducing the appropriate access control lists (ACL) on ASA1, we can ensure that computers from Outside have access to our resources (DMZ). This is just a test showing the possibilities of using ACL on ASA (as I mentioned earlier, I also assumed that during the connectivity tests, the headquarters in Dublin set their Firewall to level 0 to outside and inside.

I would also like to emphasize that the ASA configuration is not stable, the settings are not saved and after restarting, ASA must be added from scratch (copy / paste of the previously written commands save the situation). In this case ASA also becomes unstable after a while, so I assume it's a bug. Either way, it works in the early stages.

I will use the following commands on ASA1:

access-list test\_access extended permit icmp host 192.168.70.4 any

access-group test\_access in interface outside

access-list dns\_access extended permit tcp host 192.168.70.4 any

access-group dns\_access in interface outside

Graphical user interface

Description automatically generated

ICMP works!

Graphical user interface, application

Description automatically generated

TCP works!

1. https://students.mimuw.edu.pl/~zbyszek/sieci/CCNA4%20Sample.pdf [↑](#footnote-ref-1)
2. https://oit.duke.edu/sites/default/files/atoms/files/Design\_2016.pdf [↑](#footnote-ref-2)
3. https://www.atel-electronics.eu/produkt.php?hash=06215 [↑](#footnote-ref-3)
4. http://specsan.com/air-conditioners-midea/midea-mub-36hrn1-r-mou-36hn1-r/ [↑](#footnote-ref-4)
5. https://www.ecopowersupplies.com/emerson-network-power/liebert-psi-3000va-rackmount-tower-ups [↑](#footnote-ref-5)
6. https://issuu.com/routerswitch5/docs/cisco\_catalyst\_3650-24ps-s\_datashee [↑](#footnote-ref-6)
7. https://www.elara.ie/productdetail.aspx?manufacturer=CISCO&mancode=WS-C2960X-24PS-L [↑](#footnote-ref-7)
8. https://www.slideshare.net/PascalJanot/dell-poweredge-t110-spec-sheet [↑](#footnote-ref-8)