Mariia Miroshnichenko

DESIGN AND CONFIGURATION OF A FACTORY NETWORK

Bachelor's thesis
Information Technology

2018

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Mariia Miroshnichenko	Bachelor of Engineering	May 2018

Thesis title

Design and configuration of a factory network

60 pages

Commissioned by

AstraZeneca Russia

Supervisor

Matti Juutilainen (supervising lecturer)
Danila Belous (company representative)

Abstract

This work was aimed at preparing and testing the enterprise network for a factory which must support 500 users. The main idea of the work was to investigate design principles, understand in which way a good network should be designed and to summarize required information in a proposed design solution that would meet the company's need. The second aspect of this thesis was to highlight important technologies and protocols needed to run a network, gather theoretical information on them as a background study and to prepare configuration samples applied in the proposed design.

The information was gathered from different sources, such as books, articles and guidelines and the practical part included trying to apply the obtained knowledge using the PacketTracer software and Virtual Laboratory's environment at Kotka campus of South-Eastern Finland University of Applied Sciences.

As a result of this thesis a configured and tested network design was created.

Keywords

network design, hierarchical model, routing, switching, configuration

CONTENTS

1 INTRODUCTION

Planning and implementing a production network from scratch is a complex, time-consuming process in which many divisions of the organization are involved, including not only IT professionals. Everything should be taken into account - from the geographical location of the planned construction to the analysis of specific websites that a potential employee can visit during the working day.

The AstraZeneca pharmaceutical company where I work plans to expand its business on the territory of the Russian Federation and considers the possible construction of a new plant in the Ivanovo region, Kineshma Industrial Park. I was instructed to prepare a network topology plan that would meet the original requirements of the enterprise and to prepare configuration files for network devices.

To complete this task, I have studied the principles of building networks, possible topologies and the construction of a three-level hierarchical network design model. Also, information about the necessary equipment for the full functionality of the network and technologies to be implemented was studied and collected together.

The work consists of five chapters. The second chapter describes the principles of building networks. Chapter 3 includes a background description of the devices that are used to build modern networks and also the most important technologies and protocols for the initial full-fledged work of the enterprise infrastructure. Chapter 4 describes the practical application and configuration of these protocols and gives the hardware specifications of the devices that are planned for installation. Chapter 5 is the final one and includes conclusions on the accomplished work.

2 DESIGN PRINCIPLES

It is essential to understand from which point and following which guidelines the network design should be started. As networks continue to grow year after year, devices with new capabilities are implemented and technologies are updated, the obvious model to follow when creating a network design is the hierarchical model. It provides modularity, scalability, resiliency and other vital characteristics of the network (White & Donohue 2014). In this chapter I summarize information about the hierarchical network design model: what it consists of, why it is important and which advantages it provides.

2.1 Hierarchical network model

According to Lewis (2012), in order for the network to fully meet the needs of the enterprise, it needs to be designed in accordance with the three-level hierarchical model of network design. Such a network is easy to manage and can be scalable if necessary, and also provides the ability to quickly detect problems and problems. (Lewis 2012.)

Hierarchical network model bases on the division of the network into separate levels, each of which performs specific functions for this level. The division into levels is usually called modularity, and modularity provides scalability and network performance. The modern hierarchical model includes three layers: the core, distribution and access layers. (Lewis 2012.) A visual example of a three-layer network model is shown in Figure 1.

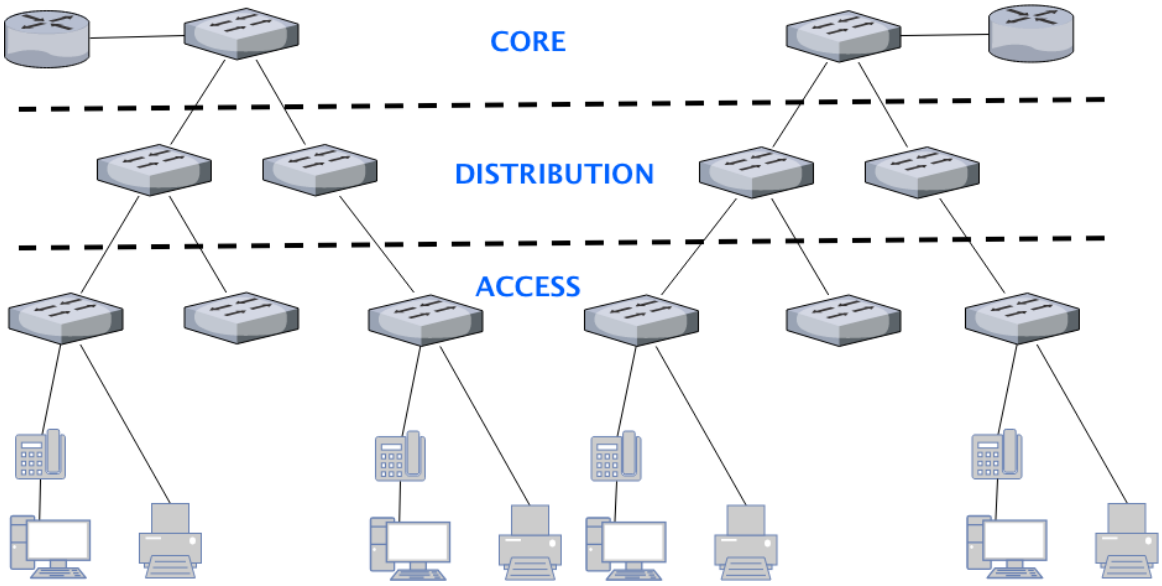

Figure 1. The hierarchial design model

The access level connects end users and devices (such as telephones, printers) to the rest of the network. At this level switches, bridges, hubs, wireless access points and even routers can operate. The main task of the access layer is to provide access to the network for end devices and to control which devices are granted with the access. (Lewis 2012.)

The distribution layer takes over the aggregation of data streams received from the access layer switches, performs traffic control based on policies, routes traffic between virtual local networks, and also limits broadcast domains. Distribution level switches are typically high-performance devices with high availability and redundancy, which provides the necessary reliability. (Lewis 2012.)

The most important level of the model, which aggregates all traffic coming from the distribution layer, is the core layer. An example of a core is shown in Figure 2.

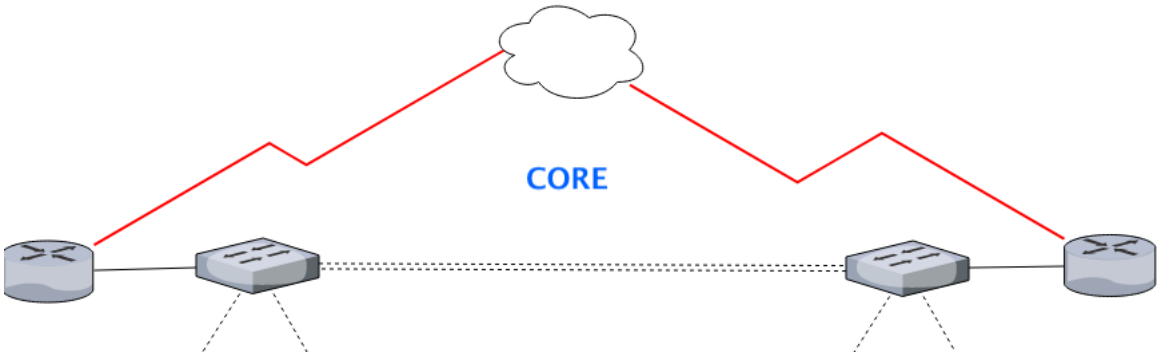

Figure 2. Core layer deployment example

Core devices must be able to pass large data streams and do it quickly. An important principle of core layer planning is redundancy and channel reservation. Not big enterprises adopt models with collapsed core - this means that core and distribution layers are united. (Lewis 2012.)

2.2 Advantages of hierarchical networks

Among the many advantages of hierarchical networks Lewis (2012) introduces the following:

Scalability means that the network can be added with nodes and the length of connections between them can be increased, while the performance stays at the same level. To ensure scalability of the network, it is necessary to use additional communication equipment and to structure the network in a special way. A network that has a hierarchical structure is well scalable. Such a network can include several thousand computers and at the same time provide each user of the network with the required quality of service.

Security. A high level of security in the hierarchical networks is ensured by the fact that security settings are performed at each layer. For example, at the access layer, the connected end devices are monitored, by parameters such as the MAC address. Security rules are assigned to specific ports of the access layer devices. At the distribution level, rules for individual traffic types can be defined and security policies can be configured.

Manageability and serviceability of the hierarchical network is quite simple, since each level performs its own functions. Due to this, the settings of the switches of the same level are similar to each other, which allows copying to be changed from one device to another if necessary and in case devices need service it is also easier to provide with the hierarchical design approach.

2.3 Design principles of hierarchical networks

The presence of a hierarchical structure does not yet mean that the network is designed correctly. The principles that must be taken into account when designing efficient and reliable networks built on a hierarchical model are defined below. These principles characterize the first practical steps in bringing a single-level network topology to a hierarchical architecture. (Lewis 2012.)

2.3.1 Diameter of the network

The first characteristic that Lewis (2012) mentions, which should be taken into account when building a hierarchical network, is the diameter of the network. Usually diameter is a measure of distance, but in the context of telecommunications networks, this term is used to measure the number of devices. The network diameter is the number of devices through which the packet must pass before it reaches its destination. Maintaining a small network diameter guarantees low and predictable delays in the transfer of information between devices.

In Figure 3 the communication scenario between the devices PC1 and PC3 is shown. Between these devices there are up to six connected switches. In this case, the network diameter is 6. Each switch in the path of the packets represents a certain amount of delay. The delay on a network device is the time that the device spends on processing a packet or frame. Each switch determines the MAC address of the destination node, compares it with its MAC address table, and routes the frame to the appropriate port. Despite the fact that such an operation is performed in a fraction of a second, the total time increases when passing from one device to another.

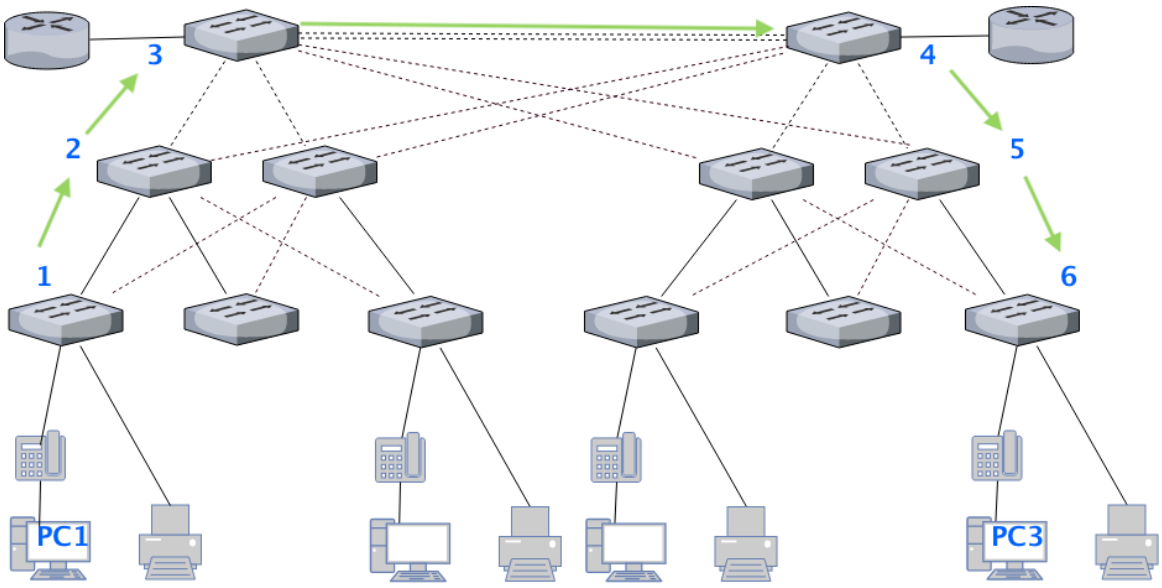

Figure 3. The example scenario of communication between PCs

Lewis (2012) explains, that in a hierarchical network, the network diameter is always a predictable number of hops between the source and the destination node.

2.3.2 Bandwidth aggregation

It is possible to increase the network bandwidth at any layer of the hierarchy by implementing aggregation. Bandwidth aggregation is the combination of several physical interfaces between switches into one logical link. (Lewis 2012.)

Link aggregation allows multiple channels of switches to be combined at the port level to achieve greater throughput between switches (Lewis 2012). For example, Cisco owns its own link aggregation technology, called EtherChannel, and allows the consolidation of multiple Ethernet channels. It is one of the first technologies for link aggregation. Figure 4 shows an example of aggregation of channels in the network.

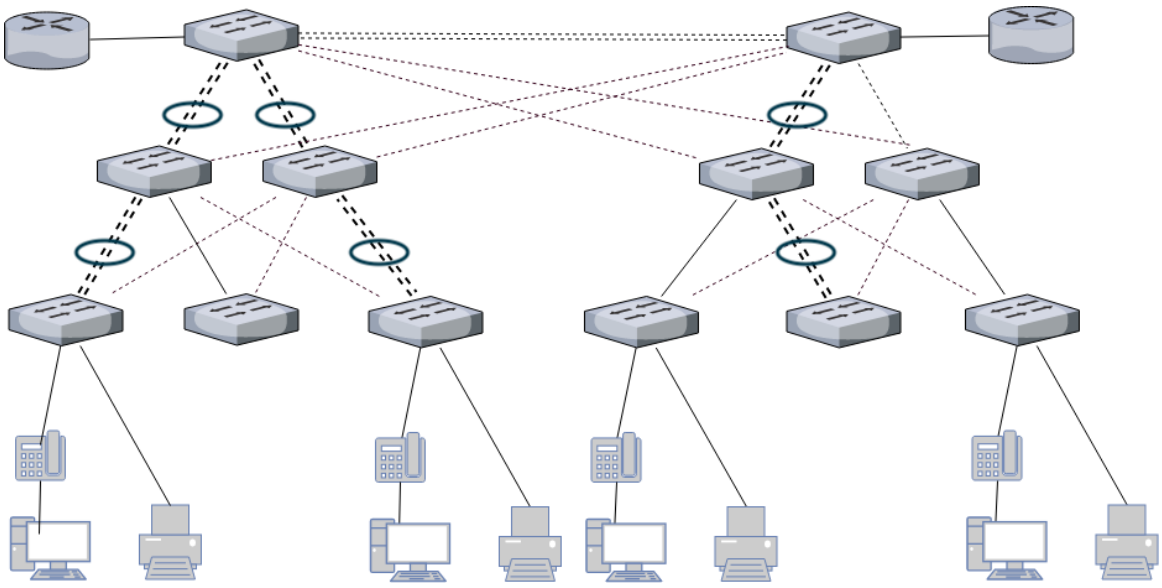

Figure 4. Link aggregation schema

Thus, the throughput of several network segments is increased by combining several physical connections into one logical.

2.3.3 Redundancy

Lewis (2012) continues to explain that reservation is one way to create a network with a high degree of availability. Redundancy can be provided in several ways. For example, the number of physical connections between devices can be doubled, or the number of devices themselves.

Building backup links can be an expensive task. One can imagine a situation where each switch at a certain hierarchy level has a connection with each switch at the next level. Implementing redundancy at the access level seems unlikely to be necessary due to its cost and the limited capabilities of endpoints, but redundancy at the distribution level and at the core level is a task that is solved when building effective hierarchical networks.

In Figure 5 the backup connections at two levels–distribution and core–are shown. At the distribution level, there are two switches–the minimum that is sufficient to provide redundancy at this level. The access level switches are

cross-connected to the distribution level switches. This ensures that the network is protected from the cases when one of the distribution level switches fails.

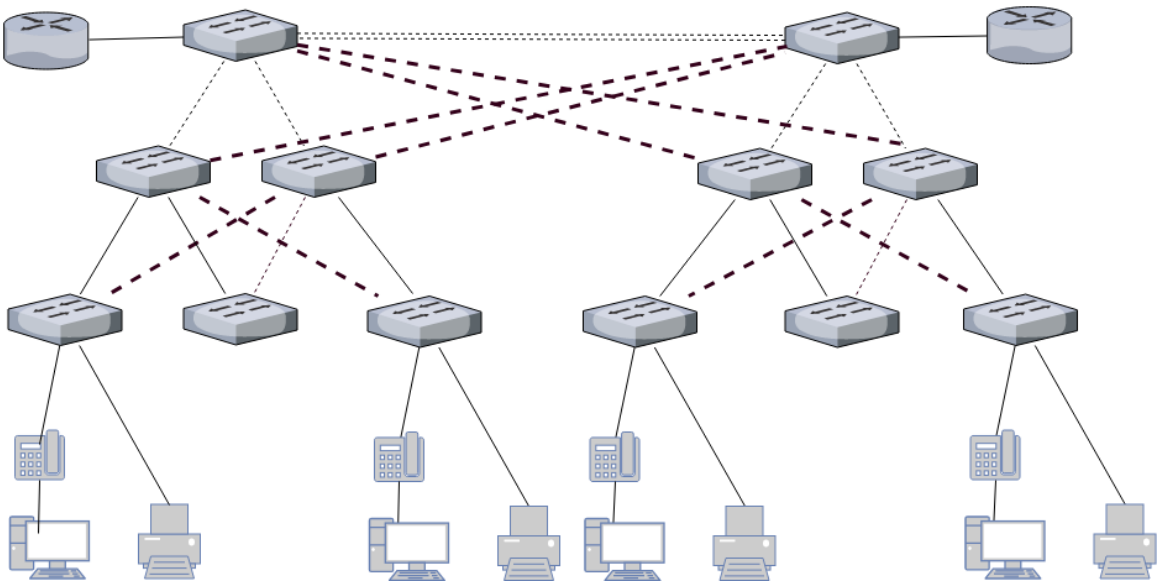

Figure 5. Redundant connections between core and distribution layers

There are such scenarios of network errors that can not be prevented, for example, when the entire city is out of electricity, or when the whole building is destroyed due to an earthquake. Links or devices' redundancy does not provide protection against such incidents and disasters.

2.3.4 Access layer is a starting point

When a network project needs to be developed, architecture requirements, such as the level of performance or the availability of reservations, are determined by the organization's business objectives. Once these requirements are documented, the designer can begin to choose the equipment and infrastructure for the project.

When hardware is selected for the access layer, it must be ensured that all network devices that require network access are covered. After all end devices are taken into account, the solution for the problem of determining the number of access level switches becomes more clear.

The number of access layer switches and the estimated amount of traffic that each will generate will help determine the number of switches required at the distribution level to ensure the required performance and redundancy.

With a known number of switches at the distribution level, the number of core switches required to maintain network performance can be determined. (Lewis 2012.)

3 DEVICES AND TECHNOLOGIES

This section gives an overview on the devices that are used to build modern networks. At this moment the most popular are switches, routers and firewalls. Also, this section covers the description and some basic information about network technologies and protocols that are needed to have a working network in which devices can communicate, have access to the Internet, etc.

3.1 Devices

The term *network devices* applies to devices that are connected to a network segment and are able to receive and / or transmit any data. There are several main devices that are implemented in the modern networks and serve in some cases similar and in some cases different purposes.

Switch

Switch is a device intended to connect several nodes of a computer network within one or more network segments. The switch works on the Layer 2 of the OSI model. Switch transmits data only directly to the recipient, the exception is broadcast traffic to all nodes of the network and traffic for devices that do not know the outgoing port of the switch. This improves the performance and security of the network, eliminating the remaining segments of the network from the need to process data that they did not intend. (Hucaby 2015.)

There are three switching methods that Hucaby (2015) mentions. Each of them is a combination of parameters such as waiting time and reliability of transmission.

Store and forward is the method when the switch reads all the information in the frame, checks it for errors, selects the commutation port, and then sends a frame to it.

The **cut-through** switch reads only the destination address in the frame and then commutes. This mode reduces transmission delays, but there is no error detection method in it.

Fragment-free or **hybrid** mode is a modification of the cut-through mode. Transmission is performed after filtering collision fragments: the first 64 bytes of the frame are analysed for the presence of an error and in its absence the frame is processed in a cut-through mode.

Due to the smallest amount of delay, cut-through switching is more suitable for complex applications performing high-performance computing (HPC), for which the delay between processes should be 10 microseconds or less. (Hucaby 2015.)

While traditional Layer 2 switches operate using the MAC addresses of the source and destination, in case when there are several subnets in the Local Area Network, routing needs to be implemented. It is accomplished by using devices that can operate on Layer 3 of the OSI Model. Nowadays there are Layer 3 switches, that can perform routing using routing mechanisms such as OSPF, RIP, EIGRP, etc. Layer 3 switches perform really fast routing, because packet-switching processes take place at the hardware level and software support remains for procedures that are not directly related to traffic processing: calculation of routing tables, access lists, etc. On the other hand, Layer 3 switches can not substitute traditional routers, because even though they can handle routing really fast, they are not supposed to fully operate as routers do. (Hucaby 2015.)

Router

Routers are devices on the interconnected networks that forward packets between networks based on Layer 3 addresses. Routers are able to choose the best path in the network for the data transmission. Operating at the Layer 3 of the OSI model, the router can make decisions based on network addresses instead of using individual second-layer MAC addresses. Routers are also able to interconnect networks with various second-layer technologies, such as Ethernet, Token Ring and Fiber Distributed Data Interface (FDDI). Typically, routers also connect networks that use asynchronous transfer mode (ATM) and serial connections. Due to its ability to forward packets based on information of the third layer, routers have become the main backbone of the global Internet and use the IP protocol. (Cisco Networking Academy 2014.)

Firewall

The firewall as a term originates from a fireproof wall made of stone or metal that stoped the fire flames to spread across the area. Later, the term was adopted to represent a metal sheet between vehicle's engine compartment and the passenger compartment. Eventually, the term firewall became widely used in the computer network's terminology: like a wall, it prevents harmful and undesirable traffic to pass into the secured network. (Santos & Stuppi 2011.)

A firewall is a single or a group of systems that enforces an access control policy between networks (Moraes 2011). Firewalls can be as a standalone hardware, embedded in the network devices or be a software on the host computers. Even though they can differ much, according to Santos & Stuppi (2011), there are similarities that are common to all firewalls:

- They are attack resistant.
- They represent the only transit point between networks, all traffic passes through firewalls.
- They enforce the policies of access control.

The first packet filtering firewall was created in 1988. These early firewall inspected packets according to a set of rules: depending on the whether the packet matches the criteria of a rule it was forwarded or dropped. This method of filtering is known as stateless. Each packet is inspected based on certain parameters in the header of the packet (Cisco Network Academy 2012).

The first stateful firewall was developed by At&T Bell Laboratories in 1989. Stateful firewalls are able to understand when the packet belongs to an existing flow of data. The static rules are substituted by dynamic rules which are created upon inspecting an active flow. Stateful firewalls are helpful to mitigate denial of service attacks. (Moraes 2011.)

Originally, firewalls were not standalone but rather an enhanced software on routers or dedicated servers. When firewalls became standalone devices that allowed to significantly reduce the intensive packet filtering activity on memory and processor. Nowadays, however, routers of integrated services known as ISRs are fully capable of performing firewall features and a dedicated firewall can be pruned from the network (Moraes 2011).

There are some other security systems such as intrusion prevention and intrusion detection. While firewall analyses header of a packet, IPS and IDS inspect the whole packet, with payload. Intrusion detection system is looking for known events and if such is found the log message is sent. Intrusion prevention system not only inspects the packet, but when anomaly (new event) occurs it rejects the packet (Frahim et al. 2014). Modern firewalls support hardware or software modules that perform IDS/IPS inspection.

3.2 VLAN

Virtual Local Area Network or VLAN is a standard used to group devices that can physically be located in different places into common logical segment of the network. This technology introduces flexibility to network design (Farell 2009).

VLANs also border broadcast domains on the Layer 2 of the OSI Model. The broadcast domain is a group of devices that receive broadcast frames when those are created by a device within the group. Normally, broadcast domains extend to the router, because router does not pass broadcast frames. It is necessary to distinguish different types of ports and therefor modes in which a port can operate when dealing with virtual local area networks. An access port operates in access mode and is designated to connect and operate traffic from an end device that is assigned to a specified VLAN. Any data received at this port is assumed to belong to a VLAN that is configured on the interface. The device itself is unaware about to which VLAN it belongs; it assumes it is a part of some broadcast domain. (Cisco Network Academy 2014.)

In order to forward traffic, the trunking protocols are used. There are two most popular trunking protocols:

• IEEE 802.1Q: An open standard that is supported on switches from many vendors and most NICs.
• Cisco ISL (Inter-Switch Link): An old Cisco proprietary protocol that is only supported on some Cisco switches.

The 802.1Q standard is Tagging the Ethernet frame with *VLAN identifier*. The frame example can be observed in Figure 6.

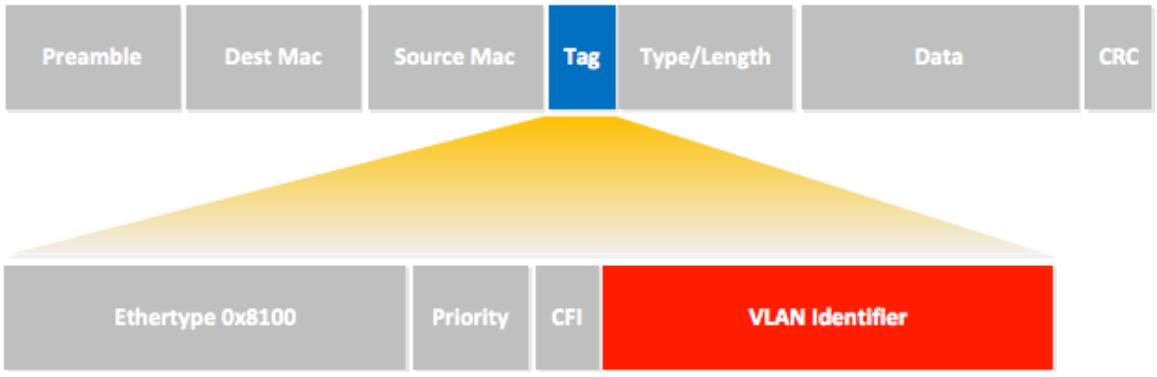

Figure 6. A 802.1Q Ethernet frame

Even though it is used to think that an access port can be assigned only to a single VLAN, nowadays switches were upgraded with a possibility to carry the voice traffic in a separate voice VLAN which lays on top of data VLAN.
The feature is extremely useful in todays networks - it provides possibility to attach a phone and a personal computer to a single switch port. The trunk link is a point-to-point connection between two devices, be it switch-switch, switch-router, etc. and it can carry multiple VLANs' traffic. (Allied Telesis 2015.)

3.3 STP

The spanning tree protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network (Hucaby 2015).
A loop in the network is caused by multiple active paths. These paths allow duplicate messages to exist causing switches to see stations appear on both sides of the switch. This confuses the switches forwarding algorithm and duplicate frames are forwarded. Without spanning tree protocol, a local area network with redundant links would cause Ethernet frames to loop for an indefinite period of time.

STP defines a topological tree which spans all switches in the network and forces certain unused data paths into block mode. Should one network segment in the topology go down or topological cost change, spanning tree algorithm will adjust the topology by enabling blocked links.

Without the implementation of STP, the three major problem are faced.
Broadcast storm occurs when a frame is repeatedly forwarded on the same links and consumes significant part of links' capacity. MAC address table instability occurs with the continual updating of the switch's MAC address table with incorrect entries. This results in frames being sent to the wrong locations. Lastly, multiple frame transmission is a side-effect of looping frames, in which multiple copies of one frame are delivered to the intended host, confusing the host. (Molenaar 2011.)

3.3.1 Key elements in the environment.

Switches participating in spanning tree send messages called bridge protocol data units (BPDU) out all ports to share information about their view of the local area network with other switches. The message that does the most work is known as STP Hello BPDU. This message contains the sending switch's root bridge ID, which is the switch, that descender believes to be the root bridge. It contains a sender's bridge ID, which is the bridge ID of a switch sending the Hello BPDU, the cost to reach root which is the STP cost between the sending switch and current root and lastly timer values on the root switch which includes the hello max age and forward delay timers. (Hucaby 2015.)

Figure 7 illustrates the visual example of spanning tree operations. STP elects the root bridge which is the logical centre of the STP topology based on the bridge IDs contained in the BPDUs. The switch with the lowest value for the bridge ID is the root switch. All ports on the root switch are placed into forwarding state. After this each switch must choose the root port. This is the interface with the lowest STP cost to reach the root switch. The last step is choosing a designated port on each LAN segment. This is the switch with the lowest cost to reach the root out of all switches on that segment. All designated ports are placed into a forwarding state. (Hucaby 2015.)

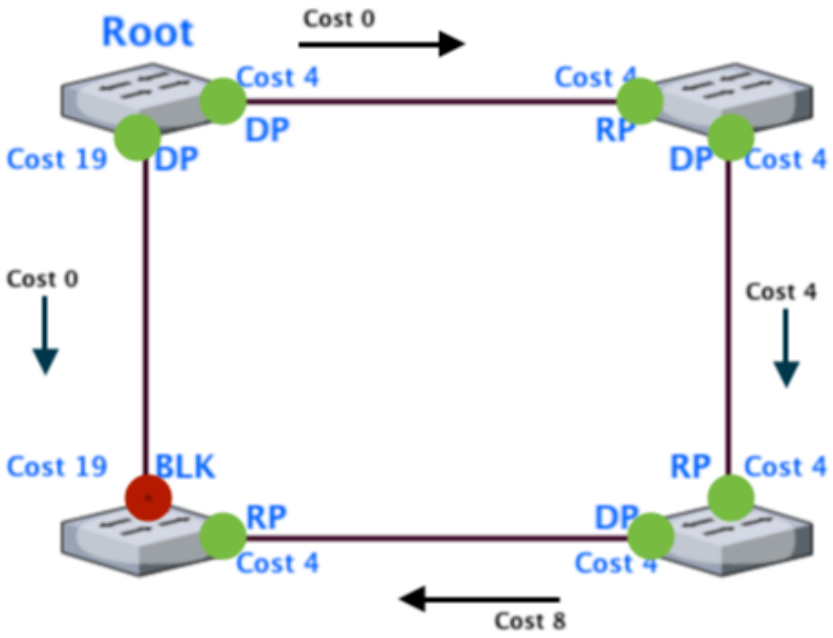

Figure 7. Example topology with spanning tree protocol

By default, the root switch sends a hello BPDU every 2 seconds. The Hello is then forwarded by non-root switches on all designated ports after making two changes. The cost is updated to show the switches cost to reach the root as well as the sender's bridge ID. This process of forwarding the modified Hellos to all designated ports causes all switches to receive Hello BPDUs every 2 seconds.

If the switch stops receiving Hellos, a failure has occurred which results in the switches initiating the process of changing the spanning tree topology. This process requires the use of three timers that are dictated by the root switch. The Hello timer is the period between Hellos created by the host. The Max Age timer is how long any given switch should wait after not hearing from Hellos before trying to change the topology. The Forward Delay is the delay affecting the process that occurs when the interface changes from blocking to forwarding state. A port stays in a temporary listening state and later a temporary learning state based on the time in seconds declared in the Forward Delay timer.
If the switch does in fact stop receiving Hello packets within the given Max Age timer it will begin to re-evaluate which switch should be the root switch, which

port should be the root port and which ports should be designated ports. When spanning tree converges, a switch chooses transition interfaces from on state to another. If switch changes immediately from blocking to forwarding, temporary frames may loop. To prevent this from happening the transitioning of the interface through two immediate interface states must occur: listening state is similar to the blocking state in that that it it does not forward frames. While in the listening state, old incorrect MAC table entries are timed out. If they were not removed during this process, there would be the sole cause of temporary looping. Following the listening state, a switch transitions into the learning state. Frames are still not forwarded but the switch is now able to learn MAC addresses of the frames received on the interface. (Molenaar 2011.)

3.3.2 STP options

Molenaar (2011) explains the difference between different versions of Spanning Tree Protocol:

Per-VLAN spanning tree protocol (PVST) is Cisco proprietary protocol. It uses ISL protocol to organize trunks. The spanning tree is built separately for each VLAN. This allows to balance traffic at the Layer 2. For PVST, port extensions, such as BackboneFast, UplinkFast and PortFast, have been developed.

Per-VLAN spanning tree protocol plus (PVST +) is Cisco proprietary protocol and is designed to support the IEEE 802.1Q trunking protocol. It supports all extensions of PVST and introduced additions–BPDU guard and Root guard.

Rapid per-VLAN spanning tree protocol (rapid PVST +) is Cisco proprietary protocol. Based on the IEEE802.1w standard and has a shorter convergence time than STP. It supports all PVST and PVST + extensions.

Rapid spanning tree protocol (RSTP) is public protocol. It includes BackboneFast, UplinkFast and PortFast extensions. It has shorter convergence time than traditional STP.

Multiple STP (MSTP) is also a public protocol. It allows building spanning trees for multiple VLANs. This allows reducing the number of trees on the switch. It provides several ways for traffic redirection and possibility to balance the load.

Nowadays, Cisco switches use only proprietary STP versions (PVST and Rapid PVST) and MSTP. STP and RSTP are not used on Cisco devices.

3.4 Link aggregation between switches

Link aggregation is a technology that allows combining several physical links into a single logical link (Molenaar 2011). Such a combination allows increasing the bandwidth and reliability of the channel. Aggregation can be configured between two switches, a switch and a router, between the switch and the host.

Aggregation of channels allows solving two tasks:

- increasing bandwidth
- providing a reserve in case of failure in one of the channels

Most aggregation technologies allow combining only parallel channels. That is, the ones that start on the same device and end on the other (Figure 8).

Figure 8. Aggregated link

If redundant connections between switches are considered, without the use of special technologies for aggregating channels data will be transmitted only through one interface that is not blocked by STP (Figure 9). This option allows channels' redundancy, but does not allow increasing the bandwidth.

Figure 9. Ports blocked by STP

Link aggregation technologies allow the use of all interfaces simultaneously. At the same time, devices control the propagation of broadcast frames (as well as multicast and unknown unicast) so that they do not get stuck. To do this, the switch, when receiving a broadcast frame via a normal interface, sends it to the aggregated channel only through one interface. And when a broadcast frame is received from an aggregated channel, it does not send it back. (Hucaby 2014.)

Although link aggregation allows increasing the bandwidth of a channel, an ideal load balancing between interfaces in an aggregated channel should not be expected. Technologies for load balancing in aggregated channels usually focus on balancing by such criteria as MAC addresses, IP addresses, ports of the sender or recipient. (Hucaby 2014.)

Link aggregation in Cisco

To aggregate channels in Cisco, either one of the three options listed below can be used:

- LACP (Link Aggregation Control Protocol) standard protocol IEEE
- PAgP (Port Aggregation Protocol) proprietary Cisco protocol
- Static persistence without the use of protocols

Since LACP and PAgP carry out the same tasks with slight differences in capabilities, it is better to use a standard protocol. An average comparison of negation protocols and static persistence is described below.

The main benefit of static aggregation is that it does not introduce additional delay when raising an aggregated channel or changing its settings. But on the other hand, there is no negotiation of the settings with the remote party. Errors in configuration can lead to loops (Molenaar 2011).

When performing aggregation using LACP or PAgP, the reconciliation of the settings with the remote side allows avoiding errors and loops in the network. The protocols also support standby-interfaces allowing to aggregate up to 16 ports, 8 of which will be active, and the rest in standby mode. On the contrary, LACP and PAgP provide additional delay when raising an aggregated link up or changing its settings.

Terminology

When configuring link aggregation on Cisco equipment, several terms are used:

- EtherChannel – link aggregation technology.
- port-channel is a logical interface that combines physical interfaces.
- channel-group – command that indicates which logical interface the physical interface belongs to and which mode is used for aggregation

Figure 10 demonstrates explained terms.

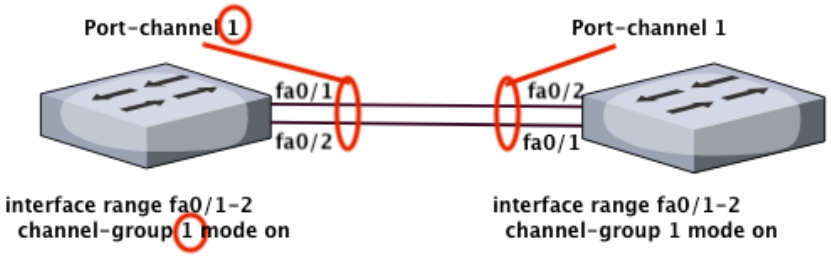

Figure 10. Terminology in Link Aggregation

The number after the channel-group command specifies which number will be at the Port-channel logical interface. The numbers of the logical interfaces on both sides of the aggregated link do not have to coincide. Numbers are used to distinguish different groups of ports within a single switch.

General EtherChannel configuration rules

For proper configuration of Link Aggregation, interfaces on both sides and those that are going to be grouped, need to have the following characteristics the same:

- speed
- duplex mode
- native VLAN
- range of allowed VLANs
- trunking status
- type of interface

After EtherChannel is configured, the changes that apply to the port-channel interface are applied to all physical ports that are assigned to this port-channel interface. Also, changes that apply to a physical port affect only the port on which the changes were made. (Molenaar 2011.)

3.5 IP Addressing

In this chapter I give a brief explanation of IP addressing, their types and what an IP address consists of. In the thesis work, IP of version 4 are used. The definition and explanation of version 6 is later in this chapter.

The numeric value that is assigned to a host and defines it among other hosts at the 3 Layer of the OSI model is know as an IP address. An IP address consists of 4 octets of 32 bits in total (Javvin Technologies Inc. 2005).

There are two types of Ipv4 addresses: public and private. Private IP addresses are described in the RFC 1918 standard. They are intended to be used on the private networks to define the hosts but these addresses are not possible to be routed on the Internet. The IP addressing space is not unlimited and therefore, private IP addresses are well-needed. They allow companies to assign computers and other network devices from the private range and purchase single public IP address to connect to the WAN, to the Internet. In order to translate

private addresses to public one, the Network Address Translation technology is used. It is described in the 3.7 section of this thesis paper. (Kocharians & Palúch 2015.)

Different types of IP addresses exist. **Loopback** addresses, also know as localhost, are used to test that the device itself is active. The range for loopback addresses is from 127.0 .0 .1 through 127.255.255.254.

Another type is the **broadcast** addresses. Packets destined to a broadcast address are send to every host on the network segment.
Unicast addresses, on the contrary, specify the single interface. The packets send to the unicast address are received by a single destination host.

When a packet is sent to a **multicast** address, the fourth type, it is meant that it was transmitted by a single source to multiple destinations. (Bonaventure, 2011.) IP addresses are used by Layer 3 routing capable devices to pass packets to a different network.

IP version 6 protocol was introduced in 1996 and is know to be *next generation* protocol for defining addresses of devices on the Internet. The protocol was created because IP version addresses seemed to be not enough in the nearest future. Ipv6 address consists of 128-bits written in hexadecimal form and with column separation. The protocol eliminates the need of using Network Address Translation, prevents collisions between private device addressing, simplifies routing and easies administration as DHCP is not needed. (Molenaar 2011.)

Still, the popularity of IPv6 is not that wide as of IPv4. For simplicity, and because guidelines and references are mostly written for IPv4 networks, in this thesis I configure IPv4 addresses, and IPv6 protocol is left behind.

3.6 IP Routing

The process of passing a packet from a device on one network to a device on the other network is know as routing (Bonaventure 2011). The following factors must be known to a router in order to deliver the packet correctly: destination address, neighbouring routes that will teach the router about remote networks, possible routes to all remote networks, the best path to reach a remote network, knowledge on how to maintain and verify routing information.

There are two ways how a router finds out about remote networks: either from neighbour routers or from the network administrator. Based on this information, router creates a routing table which includes all the routes to the networks that router is aware of. Router automatically know about directly connected networks. But to get to know remote networks a one of two solutions must be used: static route declaration or dynamic routing protocol implementation.

The **static routing** methods assumes that an administrator manually defines all remote networks that a router must know. This way brings its advantages and disadvantages. The main advantages are: there is no additional CPU usage and that allows to choose cheaper router than would be needed when using dynamic routing; the router-router communication does not require bandwidth; it adds security as the administrator can decide which networks have access to which ones. But there are some disadvantages as well: administrator of the network should be well-aware about all networks under his control; the manual configuration of new routes into routing tables is needed whenever there is a new network attached.

One well-know example of the static route is the **default route**. It is to forward packets to it whenever there is no entry found in the routing table that provides information on how to reach the destination network (Molenaar 2011).

Dynamic routing protocols introduce the automatic update of a routing table on a router, protocols do this job. A dynamic routing protocol defines the way the

routing information will be passed between router. There are two types of routing protocols: distance-vector protocols and link-state protocols.

Distance-vector protocols define the best path to a remote network based on the distance to it. For RIP protocol, each time a packet goes through a router is defined as a hop, and the best path to the destination network is defined by the least number of hops that separates source and destination. After some period, the RIP protocol sends updates of the whole routing table of the router to its neighbors. EIGRP is an advanced distance-vector dynamic routing protocol developed by Cisco (Molenaar 2011).

Another type of dynamic protocols is **link-state** protocols. They are also known as shortest-path-first protocols. Routers that are configured with a dynamic link-state protocol have three separate tables. One is to keep all directly attached neighbors, the second determines the entire topology and the third is used as a routing table. The most know example of a link-state protocol is Open Shortest Path First protocol (OSPF). Link-state protocols send updates about the state of its own connections of the router to its directly connected neighbors. (Cisco Network Academy 2014.)

3.7 NAT

Address translation using the NAT method can be performed by almost any routing device -the router, the access server, the firewall (Cisco Systems Inc. 2004). The most popular is the SNAT, the essence of the mechanism is to replace the source address when passing a packet in one direction and reverse the replacement of the destination address in the response packet. In addition to the source / destination addresses, the source and destination port numbers can also be replaced.

When taking the packet from the local computer, the router looks at the destination IP address. If this is a local address, the packet is forwarded to

another local computer. If not, then the packet must be sent out to the Internet. But after all, the return address in the packet is the local address of the computer that will not be accessible from the Internet. Therefore, the router translates (reverses) the IP address of the packet to its external (visible from the Internet) IP address and changes the port number to distinguish between response packets addressed to different local computers. The router retains the combination needed for the reverse substitution in the temporary table. Some time after the client and the server have finished exchanging packets, the router will erase the entry about the port after the limitation period in its table.

In addition to source NAT (which allows users of a local network with internal Internet access addresses), NAT is often used when external requests are broadcast by a firewall to the user's computer on the local network, which has an internal address and therefore is not accessible from outside the network directly (without NAT) (Cisco Systems Inc. 2004).

There are 3 basic concepts of address translation: static (Static Network Address Translation), dynamic (Dynamic Address Translation), IP masquerading (NAPT, NAT Overload, PAT).

Static NAT - Displays an unregistered IP address to a registered IP address on one-to-one basis. It is especially useful when the device must be accessible from outside the network. An example of static NAT operation shown in Figure 11.

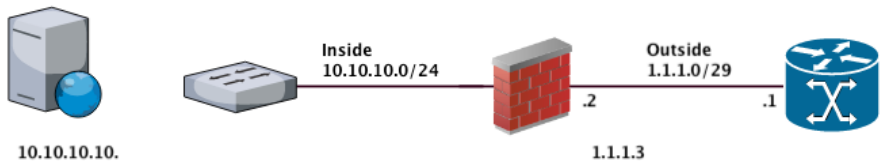

Figure 11. Static NAT example

Dynamic NAT - Displays an unregistered IP address to a registered address from a group of registered IP addresses. Dynamic NAT also establishes a direct mapping between unregistered and registered addresses, but the mapping may

vary depending on the registered address available in the address pool during communication. It is visually presented in the Figure 12.

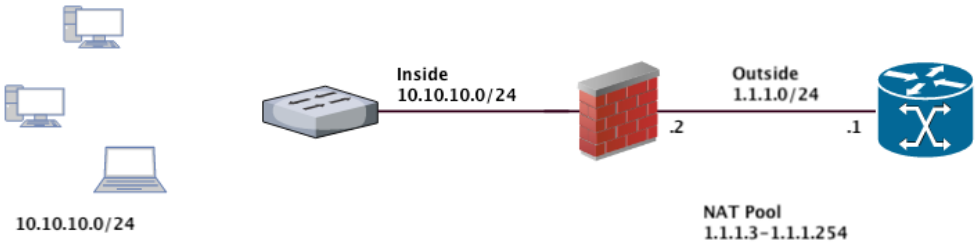

Figure 12. Dynamic NAT example

Overloaded NAT (NAPT, NAT Overload, PAT, IP masquerading) is a form of dynamic NAT that displays several unregistered addresses in a single registered IP address using different ports. It is also known as PAT (Port Address Translation). When NAT overload is used each computer on a private network broadcast to the same address, but with a different port number as shown in Figure 13.

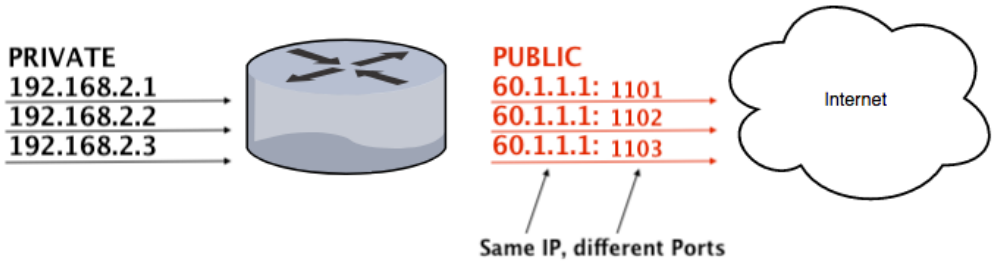

Figure 13. PAT

The NAT mechanism is defined in RFC 1631, RFC 3022.

3.8 ACL

Access control lists (ACLs) selectively restrict or allow traffic flows, filter routing protocols and redirect traffic according to rules (policy-based routing).

ACL is a list of rules and processed from the top to down until the first match. If one of the conditions is met, the list is not processed further. Following this, more

specific rules– for a specific host or port–are written above, while the more general ones– for the whole network –are below. It also makes sense to place the most frequently run rules closer to the top of the list. If there are no matches in the list, then the traffic will be blocked by the deny all rule. (Santos & Stuppi 2011.)

As stated in the same source, access lists must be assigned either: one per protocol, one per port or one per direction. Each protocol uses its own ACL such as IP, IPX, Apple Talk, etc. One list can be assigned for incoming traffic or for outgoing traffic. Access lists can be standard and extended**. Standard** lists can inspect only the source addresses. **Extended** lists can check the source addresses, as well as the address of the recipients, in the case of IP, the protocol type and TCP / UDP ports. Access lists are indicated either by numbers or by names. **Numbered** access lists are designated as follows:
Standard: 1 to 99
Extended: 100 to 199
Named ACLs are also divided into standard and extended ones. Extended ones can check much more than standard ones, but they also work more slowly, as they will have to look inside the packet, unlike standard ones where only the source address field is revised. (Santos & Stuppi 2011.)

4 IMPLEMENTATION STAGE

In this chapter I apply gathered knowledge into the configurations and commands that are needed to be conducted on the devices in the network.

4.1 Requirements

The network should cover the area of a built-in-nearest future production plant which will include a main office, a warehouse, a security office(central entrance) and two workshops. It should support around 500 users and IP telephony.
The main office is a three floor building with a server room located in the basement. There are several departments in the company: sales department, logistics department, call center, technical support and accounting department.

All of the departments will share the same Office VLAN. The server part is not covered in this thesis work, but for network planning it is assumed that Active Directory Domain Controller, DHCP, NTP, applications and databases servers, as well as web-server for the company's Intranet will be running on the network.

The warehouse is a separate building to store produced goods before its transportation. This part of the network relates to main office and needs to be places in the same VLAN. Warehouse Wi-Fi is needed for the use of barcode scanners and their connectivity with warehouse employees' portable devices. Even though Wi-Fi technologies and its configuration is not covered in this work, Wi-Fi VLANs are mentioned and created.

Workshops must be protected from any intrusions, traffic needs to be isolated inside each of the workshops. For this purpose, firewalls will be placed to border workshops' parts of the network.

After considering the approach to design the campus network discussed in the second chapter I developed a plan of the network that will fit the company's needs. The design was clearly separated into core, distribution and access layers. The functionality of the implemented devices will be separated so the main features are distinguishable and met. As defined with the company's engineers there must be:

1. the network device that will connect the LAN to the Internet (WAN) should be a Layers 3 device to be able to perform routing. At this point (end point between our LAN and WAN) the security must be implemented.
2. a switch stack that will be capable of connecting users in the main office, server room and be connected to the rest of the network.
3. Distribution and access switches for connecting workshops, warehouse and the security office.

Based on the requirements the network plan, shown in Figure 14, is designed and accepted by the company's engineers.

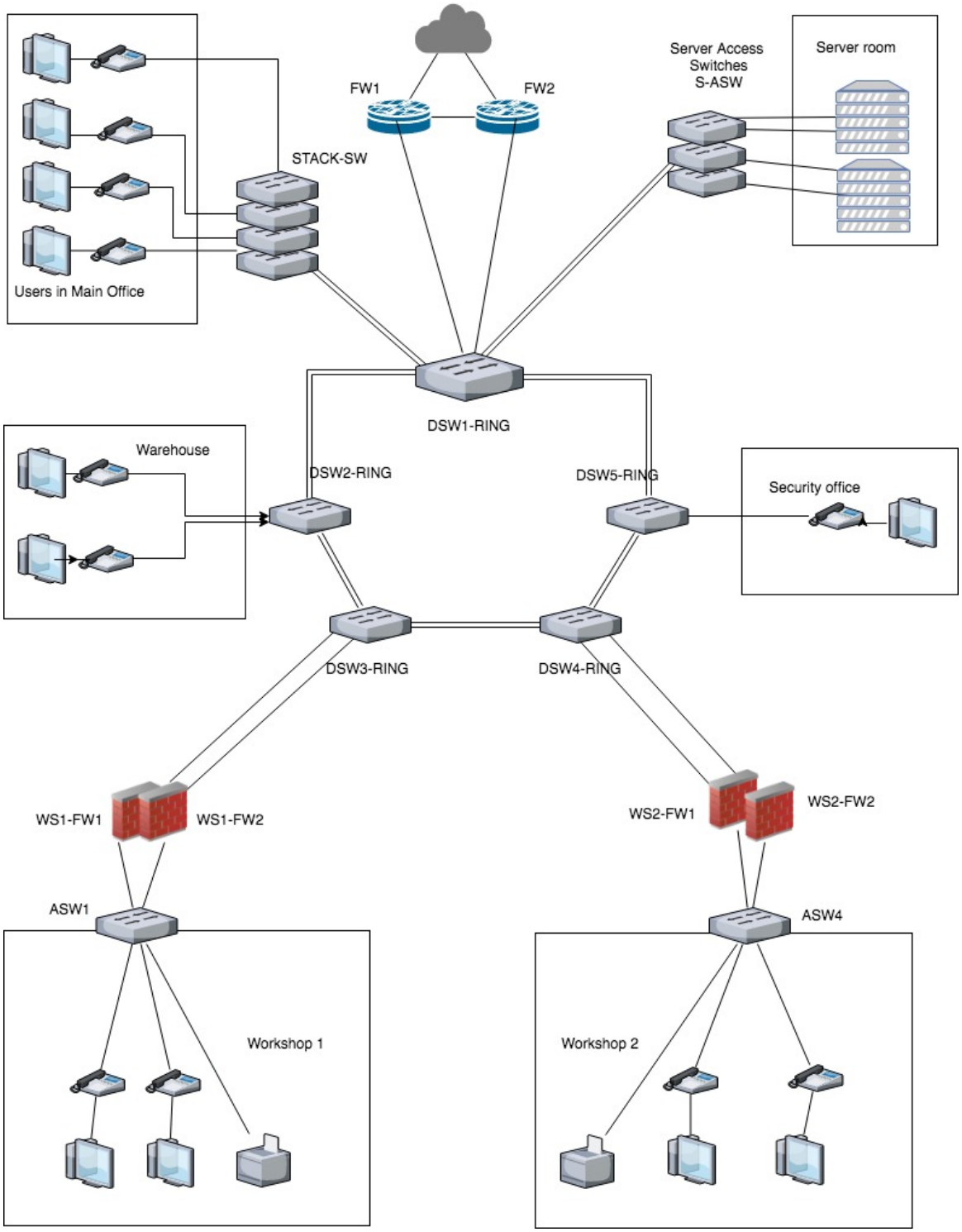

Figure 14. The network design created according the the company's needs and approval

4.2 IP addressing

Table 1 provides the IP addressing plan for VLANs and devices.

Table 1. IP-addressing plan for the network

Network, ip address	VLAN name	VLAN number	Interface on the device
172.16.2.0	**MNGT**	**2**	
172.16.2.1	FW1, FW 2		int g0/1.2
172.16.2.2	STACK		vlan 2
172.16.2.3	S-ASW		vlan 2
172.16.2.4	DSW1-ring		vlan 2
172.16.2.5	DSW2-ring		vlan 2
172.16.2.6	DSW3-ring		vlan 2
172.16.2.7	DSW4-ring		vlan 2
172.16.2.8	DSW5-ring		vlan 2
172.16.2.9	WS1-FW1, WS1-FW2		int g0/0.2
172.16.2.10	WS2-FW1, WS2-FW2		int g0/0.2
172.16.2.13	ASW1		vlan 2
172.16.2.14	ASW2		vlan 2
172.16.2.15	Administrator's PC		NIC
172.16.3.0/24	**SERVERS**	**3**	
172.16.3.1	FW1, FW 2		g0/1.3
172.16.3.2-254	Servers' pool		
172.16.100.0	**OFFICE**	**100**	
172.16.100.1	FW1, FW 2		int g0/1.100
172.16.100.2	WS1-FW1, WS1-FW2		int g0/0.100
172.16.100.3	WS2-FW1, WS2-FW2		int g0/0.100
172.16.100.4-254	Users' pool		
172.16.108.0	**WIFI**	**108**	
172.16.108.1	FW1, FW 2		int g0/1.108
172.16.108.2	WS1-FW1, WS1-FW2		int g0/0.108
172.16.108.3	WS2-FW1, WS2-FW2		int g0/0.108
172.16.108.4-254	Users' pool		
172.16.109.0	**WAREHOUSEWIFI**	**109**	
172.16.109.1	FW1, FW 2		int g0/1.109
172.16.109.2	WS1-FW1, WS1-FW2		int g0/0.109
172.16.109.3	WS2-FW1, WS2-FW2		int g0/0.109
172.16.109.4-254	Users' pool		

172.16.110.0	**VOICE**	**110**	
172.16.110.1	FW1, FW 2		int g0/1.110
172.16.110.2	WS1-FW1, WS1-FW2		int g0/0.110
172.16.110.3	WS2-FW1, WS2-FW2		int g0/0.110
172.16.110.4-254	Users' pool		
172.16.111.0	**PRINTERS**	**111**	
172.16.111.1	FW1, FW 2		int g0/1.111
172.16.111.2	WS1-FW1, WS1-FW2		int g0/0.111
172.16.111.3	WS2-FW1, WS2-FW2		int g0/0.111
172.16.111.4-254	Users' pool		
172.16.112.0	**WS1**	**112**	
172.16.112.1	WS1-FW1, WS1-FW2		int g0/1.112
172.16.112.2-254	Users' pool		
172.16.113.0	**WS1WIFI**	**113**	
172.16.113.1	WS1-FW1, WS1-FW2		int g0/1.113
172.16.113.2-254	Users' pool		
172.16.114.0	**WS1PRINTERS**	**114**	
172.16.114.1	WS1-FW1, WS1-FW2		int g0/1.114
172.16.114.2-254	Users' pool		
172.16.115.0	**WS2**	**115**	
172.16.115.1	WS1-FW1, WS1-FW2		int g0/1.115
172.16.115.2-254	Users' pool		
172.16.116.0	**WS2WIFI**	**116**	
172.16.116.1	WS1-FW1, WS1-FW2		int g0/1.116
172.16.116.2-254	Users' pool		
172.16.117.0	**WS2PRINTERS**	**117**	
172.16.117.1	WS1-FW1, WS1-FW2		int g0/1.117
172.16.117.2-254	Users' pool		

For the network of the factory, the following VLANs listed in Table 2 are going to be implemented.

Table 2. VLANs of the factory.

Number	Name	Purpose
1	default	Not used

2	MNGT	Device management
3	SERVERS	For servers
100	OFFICE	For the rest of office employees
108	WIFI	For guests and personnel, only Internet access
109	WAREHOUSEWIFI	Warehouse Wi-Fi for barcode scanners and portable devices
110	VOICE	IP-telephony
111	PRINTERS	Printers
112	WS1	Workshop 1
113	WS1WIFI	Workshop 1 Wi-Fi
114	WS1PRINTERS	Workshop 1 printers
115	WS2	Workshop 2
116	WS2WIFI	Workshop 2 Wi-Fi
117	WS2PRINTERS	Workshop 2 printers

4.3 Equipment selection

For the purposes of this thesis work, the choice of exact devices was defined by the company. My investigation in the devices was limited to summarising the specifications and features of the chosen equipment and to prepare configuration guidance for future installation.

Switch

Switches of the Cisco 2960-S Series are stackable Layer 2 switches that are available with the support of 24 and 48 Gigabit Ethernet ports. The Cisco Catalyst 2960S-48FPS-L model with 48 Gigabit ports with full (740W) power over Ethernet capacity, LAN Base Cisco IOS software and FlexStack modules was chosen as an access switch for connecting main office (in a stack), warehouse and also as stack members in the workshops (behind firewalls).

The 2960S-24PS-L (370W for Power over Ethernet) model with 24 ports and same capabilities and features was chosen as a distribution switch in the ring, that connects main office, server room, warehouse and security office to Cisco ASA cluster, it is named DSW-RING1. Also 24-ports models connect workshops to the ring. The switch has 88Gbps for forwarding bandwidth and 176 Gbps for

switching bandwidth in full-duplex capacity. It supports up to 255 active virtual local area networks with 4000 available VLAN IDs. (Cisco Systems Inc. 2014.)

Cisco ASA

The Cisco ASA5520 firewall is a mid-size security appliance. With four Gigabit Ethernet interfaces and support for up to 150 virtual subnets (VLANs), the Cisco ASA5520 allows division of the entire enterprise network into different zones. Cisco ASA5520 equipment can be integrated into a cluster of 10 firewalls, which will simultaneously support up to 7500 VPN clients and perform load balancing. Cisco ASA5520 supports active / active and standby services, thanks to which it is possible to use up to twenty Cisco ASA 5520 firewalls with a separate control of security policies. The Cisco ASA5520 firewall comes with the DES encryption algorithm license. (Cisco Systems Inc. 2018.)

4.4 Configuring switches

The approximate configuration on the example of the stack switch that connects users of main office is as follows:

Set up password for privileged EXEC mode on the switch:

```
Switch> enable
Switch# configure terminal
Switch(config)# enable password 1234
```

Turn on password encryption so that the passwords are not shown in clear text in the configuration:

```
Switch(config)# service password-encryption
```

Set up the unique device name:

```
Switch(config)# hostname STACK-SW
```

Configure an IP address for the device. Address is needed for management purposes. IP address can be found in Table 1 in the Chapter 2. For the stack switch it is 172.16.2.2 and it is in the VLAN 2.

```
STACK-SW(config)# interface vlan 2
STACK-SW(config-if)# ip address 172.16.2.2 255.255.255.0
STACK-SW(config-if)# exit
```

Disable the domain lookup feature so that the device does not start searching for a match whenever a typing mistake occurs:

```
STACK-SW(config)# no ip domain-lookup
```

Define the domain name:

```
STACK-SW(config)# ip domain-name my-domain.ru
```

Set up the current time by defining the NTP server. NTP server resides in the server farm.

```
STACK-SW(config)# ntp server 172.16.3.6 version 2 source
vlan 2
STACK-SW(config)# ntp clock-period 36029056
STACK-SW(config)# ntp max-associations 1
```

Disable web-interface:

```
STACK-SW(config)# no ip http server
```

Set up default gateway:

```
STACK-SW(config)# ip default-gateway 172.16.2.1
```

Configure SSH connection to the device. RSA key needs to be generated, user has to be created, assigned with AAA model and SSH needs to be enabled on virtual terminal lines:

```
STACK-SW(config)# crypto key generate rsa
STACK-SW(config)# username user privilege 15 password 7 1234
STACK-SW(config)# aaa new-model
STACK-SW(config)# line vty 0 15
STACK-SW(config)# transport input ssh
STACK-SW(config)# logging synchronous
```

Define access-list to access the switch only from specific IP-addresses:

```
STACK-SW(config)# ip access-list standard SSH
STACK-SW(config-std-nacl)# permit 172.16.2.15
STACK-SW(config-std-nacl)# exit
```

Apply the access-list:

```
STACK-SW(config)# line vty 0 15
STACK-SW(config-line)# access-class SSH in
```

Set up timeout of inactivity in the SSH session. When the time is exceeded and no actions were taken, the telnet session will be closed.

```
STACK-SW(config-line)# exec-timeout 5 0
STACK-SW(config-line)# exit
```

Save the configurations:

```
STACK-SW# copy running-config startup-config
```

Or

```
STACK-SW# write
```

Similar configurations are applied for all the devices.

4.4.1 VLAN

VLANs and their description need to be configures on every switch.
For easy management, the VTP (VLAN Trunking Protocol) can be configured.
DSW-RING1 will be defined as a VTP server, while other switches are defined as clients.
All the VLANs need to be created on the VTP server as follows:

```
DSW-RING1# configure terminal
DSW-RING1(config)# vlan 2
DSW-RING1(config-vlan)# name MNGT
DSW-RING1(config-vlan)# vlan 3
DSW-RING1(config-vlan)# name SERVERS
DSW-RING1(config-vlan)# vlan 100
DSW-RING1(config-vlan)# name OFFICE
DSW-RING1(config-vlan)# vlan 108
DSW-RING1(config-vlan)# name WIFI
DSW-RING1(config-vlan)# vlan 110
DSW-RING1(config-vlan)# name VOICE
DSW-RING1(config-vlan)# vlan 111
DSW-RING1(config-vlan)# name PRINTERS
DSW-RING1(config-vlan)#vlan 109
DSW-RING1(config-vlan)#name WAREHOUSEWIFI
DSW-RING1(config-vlan)#vlan 112
DSW-RING1(config-vlan)#name WS1
DSW-RING1(config-vlan)#vlan 113
DSW-RING1(config-vlan)#name WS1WIFI
DSW-RING1(config-vlan)#vlan 114
DSW-RING1(config-vlan)#name WS1PRINTERS
DSW-RING1(config-vlan)#vlan 115
DSW-RING1(config-vlan)#name WS2
DSW-RING1(config-vlan)#vlan 116
```

```
DSW-RING1(config-vlan)#name WS2WIFI
DSW-RING1(config-vlan)#vlan 117
DSW-RING1(config-vlan)#name WS2PRINTERS
```

The next thing, is to actually define DSW-RING1 as a VTP server with the following commands:

```
DSW-RING1(config)# vtp domain MY
DSW-RING1(config)# vtp password MY
DSW-RING1(config)# vtp mode server
```

and to configure other switches as clients:

```
DSW-RING2(config)# vtp domain MY
DSW-RING2(config)# vtp password MY
DSW-RING2(config)# vtp mode client
```

4.4.2 Configuring interfaces

As soon as all VLANs are created, the interfaces can be configured to either be in access mode and to belong to a specific VLAN or to operate in trunk mode and pass tagged traffic.

Access ports

Interfaces, that connect PCs and phones to switches will be configured in access mode. The VLAN to which a PC relates as well as Voice VLAN must be specified on the interface. It was decided to implement the Layer 2 security. The number of possible MAC addresses on the interface is restricted to two and in case of violating this rule the port must become disabled.

An example configuration of an access port that needs to applied on the main office access switch STACK-SW is the following:

```
STACK-SW(config)# switchport access vlan 100
STACK-SW(config)# switchport mode access
STACK-SW(config)# switchport voice vlan 110
STACK-SW(config)# switchport port-security maximum 2
STACK-SW(config)# switchport port-security
STACK-SW(config)# switchport port-security violation
shutdown
```

Similar commands are needed to be applied on other ports and o other devices.

Trunk ports

In order to pass traffic from different VLANs, trunking protocol needs to be configured on the interfaces that are pointing to neighbor switches. Configuration for DSW-RING1 on the interface GigbitEthernet 0/0–the one that points to FW1– is the following:

```
DSW-RING1(config)# interface GigabitEthernet 0/0
DSW-RING1(config-if)# switchport trunk encapsulation dot1q
DSW-RING1(config-if)# switchport trunk native vlan 2
DSW-RING1(config-if)# switchport mode trunk
DSW-RING1(config-if)# switchport nonegotiate
```

Similar configurations are needed for connections between DSW-RING3 and DSW-RING4 and firewalls clusters.

To configure trunking between switches in the ring, e.g. between DSW-RING1 and DSW-RING2 and DSW-RING1 and DSW-RING3, the configuration is applied on the port channel interfaces. The configuration of port channels is described later in this section. Actually, it does not differ much from the one applied to a single port:

```
DSW-RING1(config)# interface port-channel 1
```

```
DSW-RING1(config-if)# switchport trunk encapsulation dot1q
DSW-RING1(config-if)# switchport trunk native vlan 2
DSW-RING1(config-if)# switchport mode trunk
DSW-RING1(config-if)# switchport nonegotiate
```

Following the same manner, trunking is needed to be configured on the links between all the switches in the ring and between DSW-RING1 and STACK-SW and S-ASW.

4.4.3 Stacking

Stacking possibility with Cisco FlexStack modules allow unifying up to four devices with the 20 Gbps stack throughput. If a new switch is added to the stack, its software will be automatically upgraded and the switch will become a member of the stack transparently.

Switches, that are part of a stack, behave as a single device which reduces maintenance costs and eases its management. Cross-stack features, such as EtherChannel, can be highlighted as an advantage of creating a stack.

Each member of the stack is identified with a stack member number. If the number a switch was assigned is already taken, it will select the lowest available in the stack number. After changing the member number, the member must be reset.

The higher the priority number of a stack member, the higher the chance this switch will be chosen as a stack master. Stack master operates the stack and all configurations applied to a stack master are later replicated to stack members. The MAC address of the stack determined is the same as the master switch has. The stack MAC persistency can be configured. It ensures that, if a master switch fails, the MAC address will still be the same during the persistency timer and, if the same switch becomes the master again, it will not change. If another switch

become master, the MAC address will be inherited from it. (Cisco Systems Inc. 2016.)

Global configuration commands are the following:

```
STACK-SW(config)# switch 1 renumber 1
STACK-SW(config)# switch 1 priority 10
STACK-SW(config)# stack-mac persistent timer 0
```

For verifying the configurations of the switch the *show switch* command is issued.

4.4.4 Spanning tree and its features

By default, the switches have PVST+ spanning tree protocol enabled. Automatically, the root switch is selected based on its bridge identifier which is summed from switch priority and the MAC address.

DSW-RING1 switch is chosen to be the root switch in the network and in order to accomplish it, its priority will be manually lowered with the command:

```
DSW-RING1(config)# spanning-tree vlan 1-4096 root primary
```

In order to protect the root switch, the root guard will be enabled on its interfaces that are pointing to other switches in the topology:

```
DSW-RING1(config-if)# spanning-tree guard root
```

For all access interfaces that point to end clients/devices the portfast and bpduguard features are enabled:

```
DSW-RING1(config-if)# spanning-tree portfast
DSW-RING1(config-if)# spanning-tree bpduguard enable
```

For the port-channels, the following command will enable additional protection in

case of misconfiguration:

```
DSW-RING1(config)# spanning-tree etherchannel guard
misconfig
```

4.4.5 EtherChannel

Link aggregation allows increasing bandwidth and also adds redundancy, if port goes down, cable is harmed or unplugged, etc. The configuration of the aggregation is simple, but in order to aggregate several ports they have to have identical characteristics such as:

- the same speed;
- same duplex settings;
- same VLAN settings.

For the network I am working on, the links between switches in a ring are aggregated (GigabitEthernet interfaces g0/0-1 to one neighbour switch and g0/2-3 to another) using the LACP protocol. The following introduces an example configuration on a DSW-RING2:

```
DSW-RING1(config)# interface range GigabitEthernet 0/0-1
DSW-RING1(config-if)# description * to DSW-RING1*
DSW-RING1(config-if)# channel-group 1 mode active

DSW-RING1(config)# interface range GigabitEthernet 0/2-3
DSW-RING1(config-if)# description * to DSW-RING3*
DSW-RING1(config-if)# channel-group 2 mode active
```

4.5 Configuring edge device

The edge devices in this thesis means the ones that separate production LAN from the Internet – FW1&FW2 and also failover clusters of WS1FW1-WS1FW2 and WS2FW1-WS2FW2 firewalls that separate Workshops from LAN. In this section configuration examples for interfaces, routing, network address translation and access control lists are presented.

4.5.1 Failover clustering

For each firewall presence, the Active/Standby failover needs to be configured.

Configuring primary unit:

```
WS1FW1(config)# failover lan unit primary
```

This command assigns an interface that points to a standby device:

```
WS1FW1(config)# failover lan interface FAILOVER
GigabitEthernet0/3
```

This command assigns an IP address to a failover interface:

```
WS1FW1(config)# failover interface ip FAILOVER 10.10.10.1
255.255.255.0 standby 10.10.10.2
```

Enable the interface:

```
WS1FW1(config)# no shutdown
```

Assign the same interfface to be a stateful failover link. There is no need to specify IP address, because it was already configured:

```
WS1FW1(config)# failover link statelink GigabitEthernet0/3
```

enable the failover:

```
WS1FW1(config)# failover
```

Configuring the secondary unit takes place as follows:

```
WS1FW2(config)#failover lan unit secondary
WS1FW2(config)#failover lan interface FAILOVER
gigabitEthernet0/3
WS1FW2(config)#failover interface ip FAILOVER 10.10.10.1
255.255.255.0 standby 10.10.10.2
WS1FW2(config)#failover link statelink GigabitEthernet0/3
WS1FW2(config)#failover
```

Following the same manner the failover clusters for FW1-FW2 and WS2FW1-WS2FW2 are configured.

4.5.2 Interfaces, subinterfaces

On Cisco ASA firewalls the interface that points to the ISP will be configured as OUTSIDE interface with the IP address defined by the Internet provider. The security-level of outside interface by default is 0. So, until it is necessary, there is no need to change it.

```
FW1(config)#interface GigabitEthernet 0/0
FW1(config-if)#nameif outside
FW1(config-if)#security-level 0
```

The interface that points to DSW-RING1(and connects the whole Local area network) will be INSIDE interface, but to perform inter-vlan routing, the configurations are not applied on the physical interface itself. Sub interfaces are created and assigned with IP addresses which are default gateways for specific VLANs.

```
FW1(config-if)#interface GigabitEthernet 0/1
FW1(config-if)#no name
FW1(config-if)#no ip address

FW1(config-if)#interface GigabitEthernet 0/1.3
FW1(config-if)#nameif SERVERS
FW1(config-if)#ip address 172.16.3.1 255.255.255.0
FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.2
FW1(config-if)#nameif MNGT
FW1(config-if)#ip address 172.16.2.1 255.255.255.0
FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.100
FW1(config-if)#nameif OFFICE
FW1(config-if)#ip address 172.16.100.1 255.255.255.0
FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.108
FW1(config-if)#nameif WIFI
FW1(config-if)#ip address 172.16.108.1 255.255.255.0
FW1(config-if)#security-level 100

FW1(config)#interface GigabitEthernet 0/1.109
FW1(config-if)#nameif WAREHOUSWIFI
FW1(config-if)#ip address 172.16.109.1 255.255.255.0
FW1(config-if)#security-level 100

FW1(config-if)#interface GigabitEthernet 0/1.110
FW1(config-if)#nameif VOICE
FW1(config-if)#ip address 172.16.110.1 255.255.255.0
FW1(config-if)#security-level 100
```

```
FW1(config-if)#interface GigabitEthernet 0/1.111
FW1(config-if)#nameif PRINTERS
FW1(config-if)#ip address 172.16.111.1 255.255.255.0
FW1(config-if)# security-level 100
```

Similar configurations are applied on the second member of the failover cluster.

4.5.3 Configuring workshops

The configuration of the workshop border firewalls is similar, but considering that WS1-FW1 and WS1-FW2 are implemented to protect production areas not only from outside intruders, but also from the possible harm or data leakage in the local network, the interfaces on this firewalls are as follows: the inside interface points to workshop network and the outside interface connects the factory LAN. Based on this, the outside interface is configured and divided into subinterface for each VLAN in the network, and the inside interface is configured for VLANs used inside workshop area. The configuration is as follows:

```
WS1-FW1(config)# interface GigabitEthernet 0/0
WS1-FW1(config-if)# no name
WS1-FW1(config-if)# no ip address

WS1-FW1(config-if)# interface GigabitEthernet 0/0.3
WS1-FW1(config-if)# nameif SERVERS
WS1-FW1(config-if)# ip address 172.16.3.2 255.255.255.0
WS1-FW1(config-if)#

WS1-FW1(config-if)# interface GigabitEthernet g0/0.2
WS1-FW1(config-if)# nameif MNGT
WS1-FW1(config-if)# ip address 172.16.2.2 255.255.255.0
WS1-FW1(config-if)# security-level 80

WS1-FW1(config-if)# interface GigabitEthernet g0/0.100
WS1-FW1(config-if)# nameif OFFICE
```

```
WS1-FW1(config-if)# ip address 172.16.100.2 255.255.255.0
WS1-FW1(config-if)# security-level 80

WS1-FW1(config-if)# interface GigabitEthernet 0/0.108
WS1-FW1(config-if)# nameif WIFI
WS1-FW1(config-if)# ip address 172.16.108.2 255.255.255.0
WS1-FW1(config-if)# security-level 80

WS1-FW1(config-if)# interface GigabitEthernet g0/0.109
WS1-FW1(config-if)# nameif WAREHOUSEWIFI
WS1-FW1(config-if)# ip address 172.16.109.2 255.255.255.0
WS1-FW1(config-if)# security-level 80

WS1-FW1(config-if)# interface GigabitEthernet 0/0.110
WS1-FW1(config-if)# nameif VOICE
WS1-FW1(config-if)# ip address 172.16.110.2 255.255.255.0
WS1-FW1(config-if)# security-level 80

WS1-FW1(config-if)# interface GigabitEthernet 0/0.111
WS1-FW1(config-if)# nameif PRINTERS
WS1-FW1(config-if)# ip address 172.16.111.2 255.255.255.0
WS1-FW1(config-if)# security-level 80
```

The interface that point to Workshop LAN are configured using the following conmmands:

```
WS1-FW1(config)# interface GigabitEthernet 0/1
WS1-FW1(config-if)# no name
WS1-FW1(config-if)# no ip address

WS1-FW1(config-if)# interface GigabitEthernet 0/1.112
WS1-FW1(config-if)# nameif WS1
WS1-FW1(config-if)# ip address 172.16.112.1 255.255.255.0
WS1-FW1(config-if)# security level 100
```

```
WS1-FW1(config-if)# interface GigabitEthernet 0/1.113
WS1-FW1(config-if)# nameif WS1WIFI
WS1-FW1(config-if)# ip address 172.16.113.1 255.255.255.0
WS1-FW1(config-if)# security level 100

WS1-FW1(config-if)# interface GigabitEthernet 0/1.114
WS1-FW1(config-if)# nameif WS1PRINTERS
WS1-FW1(config-if)# ip address 172.16.114.1 255.255.255.0
WS1-FW1(config-if)# security level 100
```

Almost the same configurations are applied for WS-FW2 firewall cluster, but there the device addresses on the subinterfaces pointing to factory LAN end with three as in the example:

```
WS2-FW1(config)# interface GigabitEthernet 0/0.3
WS2-FW1(config-if)# nameif SERVERS
WS2-FW1(config-if)# ip address 172.16.3.3 255.255.255.0
WS2-FW1(config-if)# security-level 80
```

The subinterfaces that point inside Workshop 2 LAN are configured for its VLANs: WS2, WS2Wifi and WS2Printers.

4.5.4 Routing

For inter-vlan routing, so that the traffic can pass between different VLANs configured on the subinterfaces on a single physical port, the following commands are issued:

```
WS1-FW1(config-if)# same-security-traffic permit inter-
interface
WS1-FW1(config-if)# same-security-traffic permit intra-
interface
```

For the FW1-FW2 cluster, the default route to the Internet is configured. Also, routes towards Workshop 1 and Workshop 2 LANs are statically defined.

The default route on FW1-FW2 cluster towards the Internet is:

```
FW1(config-if)# route OUTSIDE 0.0.0.0 0.0.0.0 229.10.105.1
```

where 229.10.105.1 is the address on the ISP device that faces this network.

Static routes to declare how to reach WS1 and WS2, their Wi-Fi and printers networks are the following:

```
WS1-FW1(config)# route OFFICE 172.16.112.0 255.255.255.0
172.16.100.2
WS1-FW1(config)# route OFFICE 172.16.113.0 255.255.255.0
172.16.100.2
WS1-FW1(config)# route OFFICE 172.16.114.0 255.255.255.0
172.16.100.2

WS1-FW1(config)# route OFFICE 172.16.115.0 255.255.255.0
172.16.100.3
WS1-FW1(config)# route OFFICE 172.16.116.0 255.255.255.0
172.16.100.3
WS1-FW1(config)# route OFFICE 172.16.117.0 255.255.255.0
172.16.100.3
```

Default routes are configured for WS1 and WS2 firewalls as follows:

```
WS1-FW1(config)# route OFFICE 0.0.0.0 0.0.0.0 172.16.100.1
```

Similar configurations are needed to be applied on all other firewalls of the network.

4.5.5 ACL

For testing and planning environment, a rule that allows a host in the main office with IP address 172.16.100.48 to have RDP access to a server(172.16.112.22) in the workshop 1 was configured on the WS1-FW1 in the following way:

```
WS1-FW1(config)# access_list RDP_IN extended permit tcp host
172.16.100.48 host 172.16.112.22 eq 3389
```

The access list is applied on the Office interface as follows:

```
WS1-FW1(config)# access-group RDP_IN in interface OFFICE
```

Following the same manner, access lists are needed to be configured for WS1-FW2.

4.5.6 NAT

Nat rules are applied only on FW1-FW2 in order to provide Internet access. For each subnet a network object needs to be created. As an example configuration for Office and Wi-Fi subnets is the following:

```
WS1-FW1(config)#object network OFFICE
WS1-FW1(config-object-network)# subnet 172.16.100.0
255.255.255.0
WS1-FW1(config-object-network)#nat (OFFICE,OUTSIDE) dynamic
interface

WS1-FW1(config)#object network WIFI
WS1-FW1(config-object-network)#subnet 172.16.108.0
255.255.255.0
WS1-FW1(config-object-network)#nat (WIFI,OUTSIDE) dynamic
interface
```

Similar configurations are needed to be performed for other subnets.

4.6 Summing up accomplished steps

In this section I intend to summarize accomplished work and clarify all steps that have been done and on which devices.

Switch stack and firewall failover clusters were configured. All configurations were executed on the master switch in stack and on the primary unit in failover cluster.

Every device was configured with a hostname and IP address for management purposes. For remote management SSH connection was enabled. NTP server was defined to have time synchronization inside network. Devices were added to the company's domain.

After that, all VLANs were created on the VTP server which is DSW-RING1 switch. Other switches on the network were configured as VTP clients and received changes from the server.

Interfaces that face end devices were configured as access ports and added to VLANs to which they relate. Port-security set up for two MAC-addresses. Portfast and Bpduguard spanning tree features were enabled on access ports.

Redundant links between switches in the ring (DSW1-RING, DSW2-RING, DSW3-RING, DSW4-RING, DSW5-RING) and between DSW1-RING and STACK-SW and S-ASW were aggregated into portchannels. EtherChannel guard was enabled on switches to protect network from misconfiguration of aggregated channels.

Connections between switches and between switches and firewalls were configured as trunks. Trunks carry tagged traffic from different VLANs.

To ensure the placement of the root switch for spanning tree, the DSW-RING1 was manually configured with lower priority value. The switch was also protected with root guard feature for confidence that in any circumstances it stays the root switch.

Cluster of FW1-FW2 firewalls was configured with the outside interface that points to Internet Service Provider and the inside interface that was divided into subinterfaces. Each subinterface belongs to a VLAN and configured with an IP address that is the default gateway for this VLAN. Inter-vlan routing takes place there. Default route to the Internet was configured for the outside interface. Static routes to reach workshops' networks were defined. NAT overload also known as PAT was configured to translate private inside addresses to an outside address.

Workshops' 1 and 2 firewall clusters were configured so that the outside interfaces point to the factory's LAN and the inside interfaces face the workshop's LAN. Both inside and outside interfaces were divided into subinterfaces. Outside interfaces divided into subinterfaces for each VLAN on the factory's network and have IP addresses from the subnet of the VLAN they belong to. Inside subinterfaces belong to VLANs that operate in the Workshops. Inside subinterfaces each have IP address which is the default gateway for workshops' VLAN. Default routes towards FW1-FW2 cluster were defined. An example access list was created and applied to an interface. That access list permits the RDP connection from a host in the OFFICE VLAN to a server in the WS1 VLAN.

5 CONCLUSION

In this thesis work the study on hierarchical network design approach was carried out. Hierarchical design allows separating levels and provides better management and scalability opportunities. The final design plan of the factory's new plant network was built following the three-layer hierarchical design model.

The necessary technologies and protocols were investigated and sample configurations that are needed to be performed were listed. Some of them were

tested using the equipment in Virtual Laboratory, some of them were tested using Cisco PacketTracer.

The design and configuration of a big enterprise network is a time-demanding, careful process and every little detail was hard to cover in this work. I prepared sample configurations, but it is obvious that in a scale of such a big network there are a lot of things to consider and more technologies must be implemented. I think that there are important issues that need to be reconsidered before implementing the network in the real life. Following prepared configurations, the network can be set up and running, but to be reliable in a production, future developments and improvements are needed. The most important thing to re-consider is that DSW-RING1 switch is a single point of failure for the entire network. I recommend adding redundancy at this point. There is also a need to establish security policy and configure devices and implement stronger security at every layer of the network according to it.

By the end of this work, I gained important experience and structured information, that I had in mind as separate theoretical pieces, together and practiced it in the test environment. For me, it was challenging task, because I needed to see the whole picture and understand from which end to start.

REFERENCES

A practical look at Network Address Translation. 2003. PDF document. Available at: http://www.csd.uoc.gr/~hy435/material/whitepaper_technicalnetworkaddresstranslation.pdf [Accessed 17 March 2018].

Allied Telesis. 2015. Virtual LANs. PDF document. Available at: https://www.alliedtelesis.com/sites/default/files/vlan_feature_config_guide_revb.pdf [Accessed 15 March 2018].

Bonaventure, O. 2011. Computer Networking. PDF document. Available at: https://www.saylor.org/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf [Accessed 25 March 2018].

Cisco ASA 5500 Series Adaptive Security Appliances Data Sheet. 2018. Cisco Systems, Inc. WWW document. Available at: https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-345385.html [Accessed 2 April 2018].

Cisco Network Academy. 2012. Network Security First-Step: Firewalls. WWW document. Available at: http://www.ciscopress.com/articles/article.asp?p=1823359 [Accessed 16 March 2018].

Cisco Network Academy. 2014. Cisco Networking Academy's Introduction to Routing Concepts. WWW document. Available at: http://www.ciscopress.com/articles/article.asp?p=2180208&seqNum=4 [Accessed 21 March 2018].

Cisco Network Academy. 2014. Cisco Networking Academy's Introduction to VLANs. WWW document. Available at:

http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=4 [Accessed 18 March 2018].

Cisco Systems Inc. 2014. Cisco Catalyst 2960-S Series Switches. PDF document. Available at: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.pdf [Accessed 2 April 2018].

Cisco Systems, Inc. 2004. Cisco IOS Network Address Translation. PDF document. Available at: https://www.cisco.com/c/en/us/products/collateral/security/ios-network-address-translation-nat/product_data_sheet0900aecd8064c999.pdf [Accessed 28 March 2018].

Farell, M. 2009. Virtual Local Area Networks. PDF document. Available at: http://systems.digital.nhs.uk/infogov/security/infrasec/gpg/vlan.pdf [Accessed 27 March 2018].

Frahim, J., Santos, O. & Ossipov, A. 2014. Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services. 3d Edition. Indianapolis: Cisco Press.

Hierarchical Network Design Principles. 2008. Cisco Exploration Blog. WWW document. Updated 24 November 2008. Available at: https://waveiceku.wordpress.com/2008/11/24/hierarchical-network-design-principles [Accessed 26 March 2018].

Hucaby, D. 2015. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Indianapolis: Cisco Press.

Javvin Technologies Inc. 2005. Network Protocols Handbook. 2nd Edition. Saratoga: Javvin Technologies.

Kocharians, N. & Palúch, P. 2015. CCIE Routing and Switching v5.0 Official Cert Guide. 5th Edition. Indianapolis: Cisco Press.

Lewis, W. 2012. LAN Switching and Wireless: CCNA Exploration Companion Guide. Indianapolis: Cisco Press.

Managing Switch Stacks. 2016. Cisco Systems, Inc. PDF document. Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swstack.pdf [Accessed 3 April 2018].

Molenaar, R. 2011. How to master CCNP route. CreateSpace Independent Publishing Platform.

Molenaar, R. 2011. How to master CCNP switch. CreateSpace Independent Publishing Platform.

Moraes, A. 2011. Cisco Firewalls. Indianapolis: Cisco Press.

Morgan, B. & Ball, J. 2016. CCNA Collaboration CIVND 210-065 Official Cert Guide. Indianapolis: Cisco Press.

Santos, O. & Stuppi, J. 2011. CCNA Security Official Cert Guide. Indianapolis: Cisco Press.

White, R. & Donohue, D. 2014. The art of network architecture: business-driven design. Indianapolis: Cisco Press.

Woland, A. & Redmond, K. 2015. CCNP Security SISAS 300-208 Official Cert Guide. Indianapolis: Cisco Press.