

Denis Kalvan

DESIGNING AND PLANNING A NETWORK FOR A RESTAURANT FRANCHISE

Bachelor's thesis

Bachelor of Engineering

Information Technologies

2022



South-Eastern Finland
University of Applied Sciences

Degree title	Bachelor of Engineering
Author(s)	Denis Kalvan
Thesis title	Designing and planning a network for a restaurant franchise
Commissioned by	-
Year	2022
Pages	38 pages
Supervisor(s)	Matti Juutilainen

ABSTRACT

With the constant growth of the amount of data being transferred across devices, the demand for modern network topologies and technologies will never decrease. The aims of the study were to gain knowledge on the basic aspects of building LANs and design a network topology for a restaurant franchise.

This thesis presents the theory of the processes running in LAN, routing protocols, WLANs and security solutions. Furthermore, it introduces described configuration of networking devices for a topology with a secured remote connection between facilities, using WinBox for configuring the equipment and GNS3 for testing in a virtual environment. Lastly, there is a list of hardware and budgets.

Finally, this project can be used as a solution for opening a new franchise with minor changes to some aspects.

Keywords: LAN, restaurant franchise network, basic network configuration

CONTENTS

1	INTRODUCTION	1
2	THEORY	2
2.1	Local Area Network	2
2.1.1	Internet Protocol	3
2.1.2	Dynamic Host Configuration Protocol	4
2.1.3	Routing	5
2.1.4	Network Address Translation	5
2.1.5	Wireless Local Area Network	6
2.1.6	Wi-Fi MESH	8
2.1.7	Power over Ethernet	8
2.1.8	Virtual Local Area Network	8
2.1.9	Firewall	10
2.2	Virtual Private Networks	10
2.2.1	VPN topologies	11
2.2.2	Generic Routing Encapsulation	12
2.2.3	GRE over IPsec	12
2.2.4	OpenVPN	13
3	PRACTICAL PART	13
3.1	Background of the restaurants	13
3.1.1	The data flow in the restaurant	14
3.1.2	Data flow in the office	14
3.2	Overall topology	15
3.3	Configuring the office	17
3.3.1	Topology description	17
3.3.2	Router configuration	18
3.3.3	Switch configuration	27

3.4	Configuring the restaurant	27
3.4.1	Overall topology of the restaurant.....	27
3.4.2	Network configuration	28
3.5	List of hardware and budgets	29
4	CONCLUSION.....	35
	REFERENCES	37

1 INTRODUCTION

It is well known that computers are integrated into everyday human life so deep that it would be almost impossible to do ordinary things without machines. Each hour more and more devices are produced and being used. In order for them to work with each other, the internet was invented. As the number of devices is growing with crazy speed, more data is being transferred between them. The demands on reliability, security and speed are increasing.

The internet is built by connecting an enormous amount of Local Area Networks (LAN). Each LAN might be a home router with Wi-Fi or a huge enterprise network with thousands of end-point devices. Each company requires a unique configuration for its network as it depends on various aspects such as the number of employees what services are provided, if there are any IoT devices, how many offices there are, and what is their location.

If the enterprise has several facilities, a Wide Area Network is built, which is a name for several LANs connected. It is essential to configure such networks secure as the data is transferred across foreign networks, while it also must be fast and reliable as in some cases it may save someone's life, for example, banks must send billing information across the globe, or a hospital needs the blood type but the data is stored in a data center in another facility.

In this thesis, I will build a Wide Area Network for a restaurant franchise based on my experience of working in such a company during my practical training. I will introduce basic knowledge of building LANs and connecting them securely across the Global Network. I will design the topology that could be used to open new facilities and easily integrate them into the network.

The aim of the study is to understand commonly used techniques in building secured and reliable WAN and LAN, to overcome general problems the restaurants might have based on my working experience in the sphere, and to create a modern solution for a company that wants to start the restaurant business. I will provide the necessary theory of local and wide area networks

firstly, therefore, common demands of a restaurant from a networking perspective will be described. Afterwards, I will present the process of designing the network for a restaurant and the office, which will also include the list of devices and average budget. Lastly, I will have the conclusion.

2 THEORY

This chapter will define the concepts of networking technologies that I will use in designing and building local and metropolitan area networks for the restaurant franchise.

2.1 Local Area Network

The internet is a conjunction of smaller networks. These networks can be divided into different groups by their scale on a geographical map starting with the biggest: wide area network (WAN), metropolitan area network (MAN), local area network (LAN), personal area network. Figure 1 represents the scaling of networks.

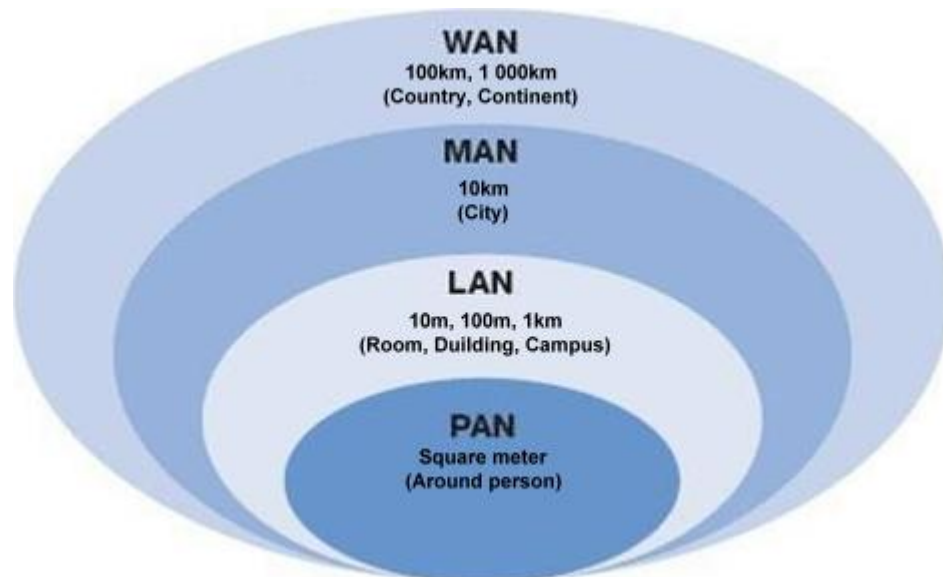


Figure 1. Networks by scale (Eldis Mujarić, n. d.)

A local area network is a group of electronic devices connected by a cable or wirelessly in some specific area, for example, an office, apartment, or room. It may be different sizes, ranging from a small network at home with a few users to

a company network with hundreds of users. When several LANs are connected, they unite into metropolitan area networks. MANs are united into wide area networks. (Cisco.) There is not much difference between wide and metropolitan networks as they are provided by an internet service provider, therefore further in this article WAN will be used.

To establish a stable, secured and fast connection, special network devices are used, such as a router, switch, access point, firewall and others. Depending on the needs of the network, their use varies. The upcoming design will use only basic devices to reduce the costs of building the network and simplify maintenance.

2.1.1 Internet Protocol

To receive data across a network, a device needs some identification. For that purpose, an internet protocol (IP) address was invented. There are two versions of IP addresses used in the world: IPv4 and IPv6. The initial version, which is addressed as Version 4, was first deployed in 1983 and is still in use widely. It is a 32-bit binary number that can be translated to a more human-readable form as four digit numbers separated with a dot in a range between 0 and 255, for example 172.16.10.243.

There are two types of IP addresses: public and private. A private IP address is assigned to any device that connects to the local network, for example, a smartphone, laptop or TV. Internet Assigned Numbers Authority reserved three IP ranges for private networks to increase practicality. Any address from these pools cannot be seen in a public network.

- Class A: 10.0.0.0-10.255.25.255
- Class B: 172.16.0.0-172.31.255.255
- Class C: 192.168.0.0-192.168.255.255.

Therefore, the public IP address is used to communicate across WAN, it is assigned by the internet service provider to the gateway device which is placed on the edge of the local network. (Kaspersky.)

Another item that is required for establishing a connection is the subnet mask. It allows the device to detect whether the required address is on the local or remote network. The number of available addresses in a subnet is configured by specifying the subnet mask. For example, the most common network and mask are 192.168.1.0 255.255.255.0, which provides 256 IP addresses, where 192.168.1.0 is the network address and 192.168.1.255 is used for broadcasting. The rest can be assigned to any device.

2.1.2 Dynamic Host Configuration Protocol

To simplify the process of connecting a new device to the network, especially for an average user that is not familiar with the technical aspects, the dynamic host configuration protocol (DHCP) was invented in 1993. Whenever a new device is connected to a network, if the DHCP client is turned on, it sends the DHCP discovery message. After, the server replies with the DHCP offer, with which it proposes a free IP address from the DHCP pool. Figure 2 shows the dialogue between a new host and a server.

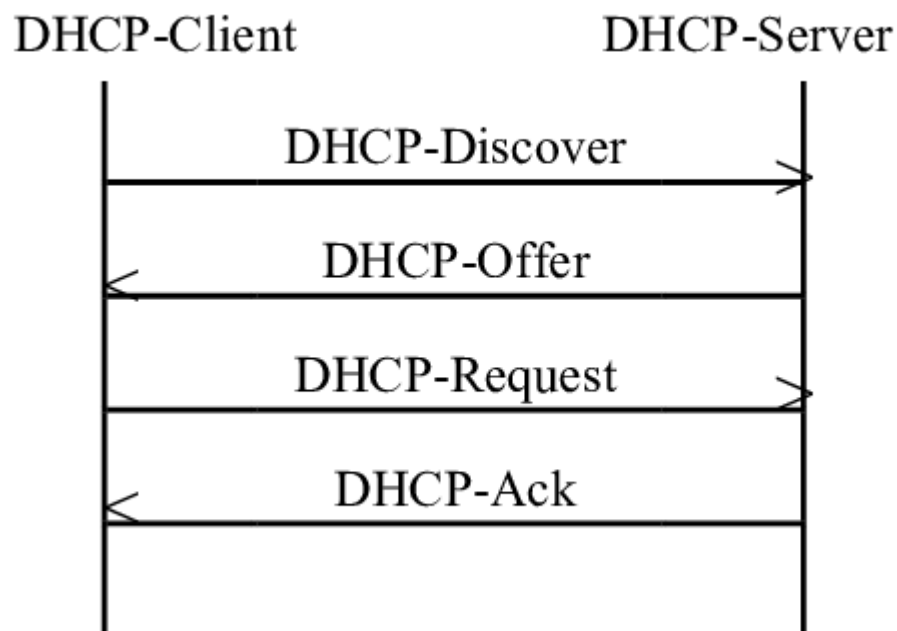


Figure 2. Typical DHCP sequence (A System to Save the Internet from the Malicious Internet of Things at Home - Scientific Figure on ResearchGate)

In large networks, there may be several DHCP servers, which is why the client must respond with the DHCP request to the offering. Lastly, the server sends DHCP acknowledgement, after which the client is allowed to use a new IP configuration. (Bluecat).

2.1.3 Routing

After a device tries to communicate with an unknown host, all the data is sent to the default gateway address which is assigned to a router. The router has a route table on it, configured manually, or automatically by various routing protocols. It is used to determine the path for the data to reach its destination. The routing table consists of a destination address, a gateway or in other words next hop, an interface that will be used to access the path and metric, a cost of using the route.

2.1.4 Network Address Translation

Whenever a host from a private network requires a connection to the public, the network address translation (NAT) is in charge of establishing the communication. Before leaving the router, the source address of traffic is replaced with the IP address of the output interface. The process is reversed when the reply comes back. (CompTIA).

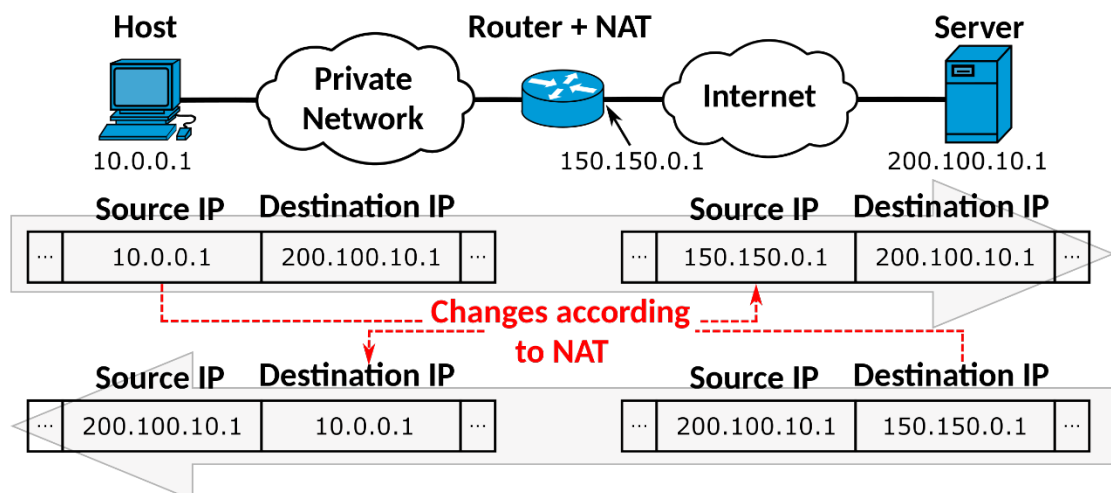


Figure 3. NAT IP Address swapping (Michel Bakni, n.d.)

The example of address translation is presented in Figure 3. It contains both outbound and inbound traffic.

2.1.5 Wireless Local Area Network

While some devices are connected with cables, most endpoint devices, such as laptops or smartphones are connected wirelessly for the usability of the user. IEEE 802.11 which is known as Wi-Fi, is the most widely used protocol for wireless connectivity. It specifies the use of networking technologies and radio waves for implementing wireless local area networks (WLAN). It was created in 1997 and has been improving ever since. Access Points are devices used to connect wireless devices to a wired network. Most home routers also support Wi-Fi. (Techopedia).

IEEE 802.11 uses different radio frequencies to establish the connection, the most common are 2.4 GHz, 5 GHz and 6 GHz. There are also different standards for the Wi-Fi protocol that were invented through the progression of wireless networks. Table 1 shows the difference between them.

Table 1. IEEE 802.11 standards

Standard	Frequency (GHz)	Maximum speed (Mbit/s)
802.11	2.4 GHz	2
802.11a	5 GHz	54
802.11b	2.4 GHz	11
802.11g	2.4 GHz	54
802.11n (Wi-Fi 4)	2.4 GHz, 5 GHz	600
802.11ac (Wi-Fi 5)	5 GHz	3466
802.11ax (Wi-Fi 6)	2.4 GHz, 5 GHz, 6 GHz	9608

Nowadays, most access points use 802.11n, as many devices still do not support 5 GHz.

One important detail to know to properly set up WLAN is a channel width. Wi-Fi needs at least 20 MHz channel width to work. The 2.4 GHz band operates in a range of 2.400 to 2.483 MHz, with a 5 MHz for a channel, it is divided to 11 usable channels, they are presented in Figure 4. To avoid the interference, it is wise to use the less overlapping channels which are 1, 6 and 11. The 5 GHz have a wider range

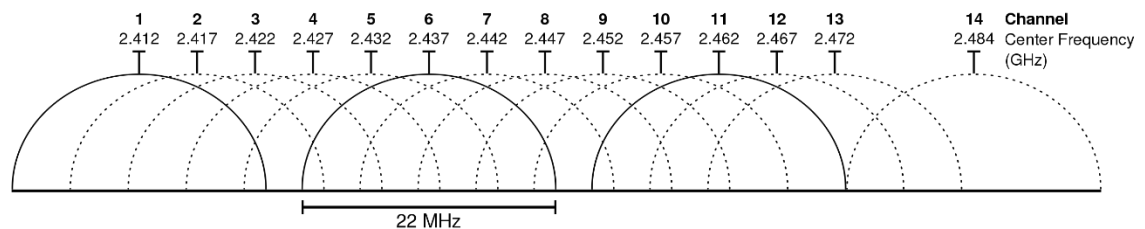


Figure 4. Graphical representation of overlapping 20 MHz channels within the 2.4 GHz band. (Michael Gauthier, n.d.)

The 5GHz band operates on a wider range, but with a fewer covering distance. The channel range is from 36 to 165. It is possible to increase the channel width to gain data transferring speed.

Each WLAN have a Service Set Identifier (SSID) – a human-readable name of the wireless network. It is broadcasted from the wireless router or access point. To prevent unauthorized connection, the password is set up for each SSID.

As it is very easy to intercept data that is being transferred by radio waves, the Wi-Fi Alliance, an organization that is propagating wireless technologies, has invented various security protocols. Nowadays, most wireless networking devices use Wi-Fi Protected Access (WPA) of different generations. After entering a password, the access point generates a pairwise master key (PMK) and shares it with the client. It is then used to encrypt the packets on both sides of the connection.

2.1.6 Wi-Fi MESH

The signal of a radio wave is limited to some distances or obstacles. In large facilities that have multiple floors and offices, lots of access points or wireless routers are needed to cover all the space. To avoid maintaining each device separately and to increase usability from the end-point device perspective, network engineers have invented wireless mesh network topology.

Wi-Fi mesh allows to gather multiple APs together and control them from one device. Therefore, with the corresponding topology, the user is automatically connecting to the closest access point. While without this technology, the host would not change the node until it is out of range of the last connected device. (Google.)

2.1.7 Power over Ethernet

Power over Ethernet (PoE) allows to provide DC power to devices using only ethernet cable. This helps to dispose of power cables. The technology is mostly used for end-point devices such as access points or cameras. (Cisco.)

The power can be imbedded in the ethernet cable with two different ways. The primitive method is to use a PoE injector, an adapter that takes as input ethernet and power cables, and combines them. Another way is to use network device that supports PoE on the interfaces. This method provides monitoring and management on the connected hosts, for example, when a device is frozen and it must be rebooted remotely, it is possible to turn off the PoE to hard reboot.

2.1.8 Virtual Local Area Network

In network topologies with a big variety of devices, it is wise to separate them into different LANs for security and usability reasons. For example, video surveillance can be separated from user computers. The separation can be done in two different ways, by connecting each LAN to a different interface on a router, or by assigning edge interfaces to the VLANs.

A virtual local area network (VLAN) is a network that is virtually split by some functional or logical criteria, such as a group of people or devices. VLANs have the same properties as physical LANs, but they allow to group network nodes that are not physically connected to the same LAN segment. A VLAN can be assigned to any switch port, and unicast, broadcast, and multicast packets are only routed and flooded to the VLAN's end stations. Each VLAN is treated as a separate logical network. (Cisco, VLANs Overview.)

The most commonly used protocol for VLANs is IEEE 802.1Q. It gained popularity for multivendor support. The protocol operates on the data link layer. IEEE802.1Q adds a 32-bit portion of data that consists of: which protocol is used, a priority of the frame, Canonical Format Indicator that indicated whether the MAC address is in canonical format or not and VLAN identifier. Figure 5 demonstrates how the VLAN tag is embedded into a frame.

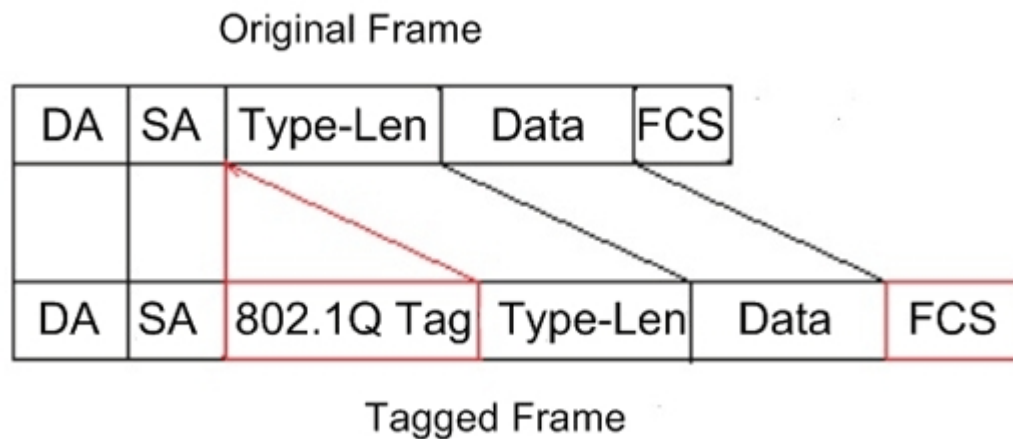


Figure 5. VLAN tag in a frame. (Hewlett Packard, n. d.)

To operate properly, the network devices must be configured specially. Firstly, the VLAN must be created on each of them by providing the VLAN identifier, a number between 0 – 4095. Afterwards, interfaces that will work with VLANs must be switched to one of two modes: tagged or untagged. If an interface is configured as tagged, it will compare the 802.1Q tag with the list of allowed VLANs, if there is a match, the data is transferred to the next hop without any changes, otherwise, it is dropped. If the interface is in untagged mode, the

network device will remove the VLAN tag from the frame and after send it to the connected host, in case their tags are matching. An untagged port must be assigned with only one VLAN id, while tagged ports might have several. By default, all the interfaces are assigned to 1 VLAN id as untagged.

A network segmentation is one of the most common security measures. It helps to restrict access to a list of devices which must be protected, such as servers or networking equipment. Without proper routing between networks, the communication is impossible, since the router does not know where to send the packets. If an intruder will scan the network, it also will show only the devices inside the VLAN that a host is connected.

2.1.9 Firewall

A firewall is a network security instrument which analyzes inbound and outbound traffic and chooses whether certain types of data should be permitted or prohibited based on a set of security rules. (Cisco.)

The data flow can be blocked by different parameters: source or destination address, port number, incoming or outgoing traffic on a specific network interface. The routing device compares the packet with the firewall rules and decides whether to send it further or drop it.

For small LANs, it is unnecessary to have a firewall as a separate device. Most routers provide firewall functions.

2.2 Virtual Private Networks

A virtual private network (VPN) establishes a connection or a tunnel between private networks across WAN. It is beneficial to use this technology as with the help of security protocols it encrypts the traffic, therefore the intercepted data will not be compromised. Likewise, it connects several private networks or independent hosts as if they are connected locally. The most known protocols

are: Layer 2 Tunneling Protocol (L2TP), Point-To-Point Protocol (PPTP), Secure Sockets Layer (SSL), OpenVPN and IPsec.

2.2.1 VPN topologies

The two most common types of VPN usage are host-to-network and site-to-site. A host-to-network topology is where a single device is connected to the private network across wan. This is used to access local area network devices while outside the office or home. A site-to-site topology is used to connect several private networks across the WAN, for example restaurants that are located in different parts of the city.

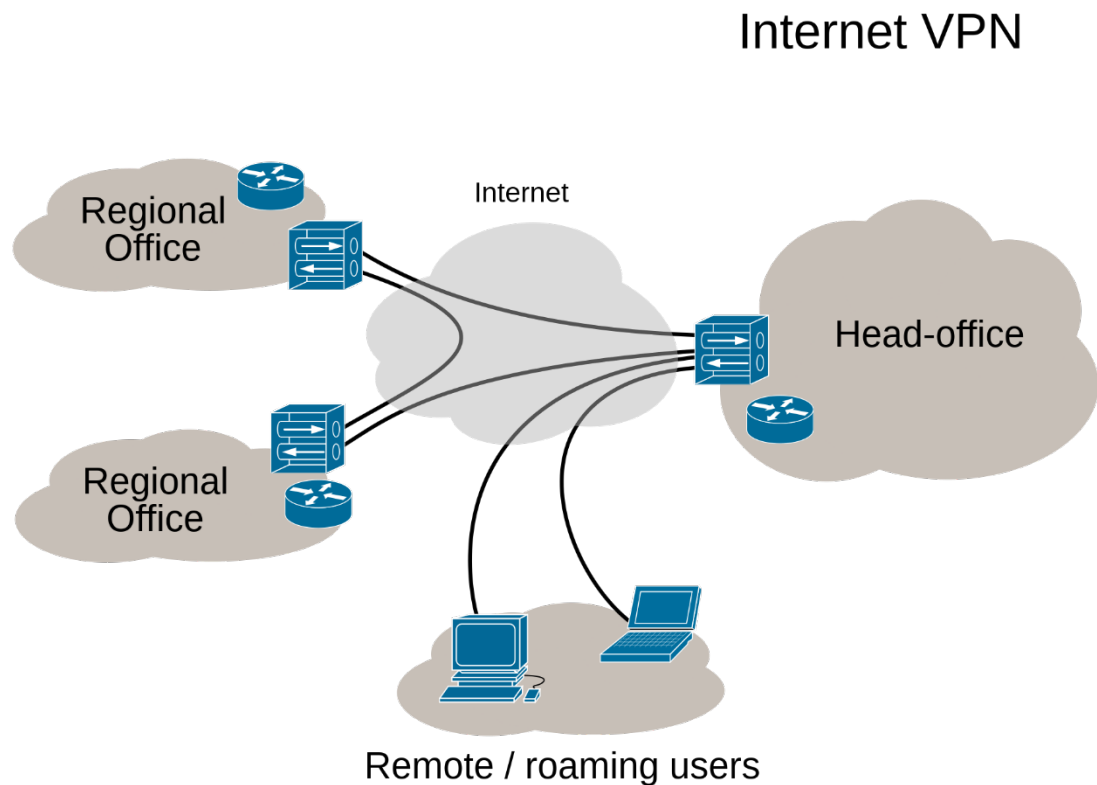


Figure 6. VPN site-to-site and host-to-network (Ludovic, 2010)

Figure 6 represents an example of both topologies implemented. Several facilities are connected together over public network.

2.2.2 Generic Routing Encapsulation

Generic routing encapsulation (GRE) is one of the tunnelling protocols. It is used to transfer encapsulated IP packets over a network. (Cloudflare.) Its main advantages are the possibility to transfer broadcast and multicast traffic, the capability of encapsulation of any Layer 3 protocol, and its simplicity in configuration. However, GRE doesn't provide any encryption, it is used in a pair with some security protocols.

2.2.3 GRE over IPsec

Internet Protocol Security (IPsec) is a combination of network security protocols that provides encryption and authentication of traffic between two nodes. It is commonly used to configure VPN between nodes. The process of securing the data consists creating the tunnel with internet key exchange (IKE) and then encrypt the packets with encapsulating security payload (ESP) protocol. (Bhardwaj.)

IPsec supports DES, 3DES and AES encryption algorithms. Nowadays, it is recommended to use AES out of this list with a key length of 256. For the authenticating, it is either MD5 or SHA1, while the second option is favored for greater security.

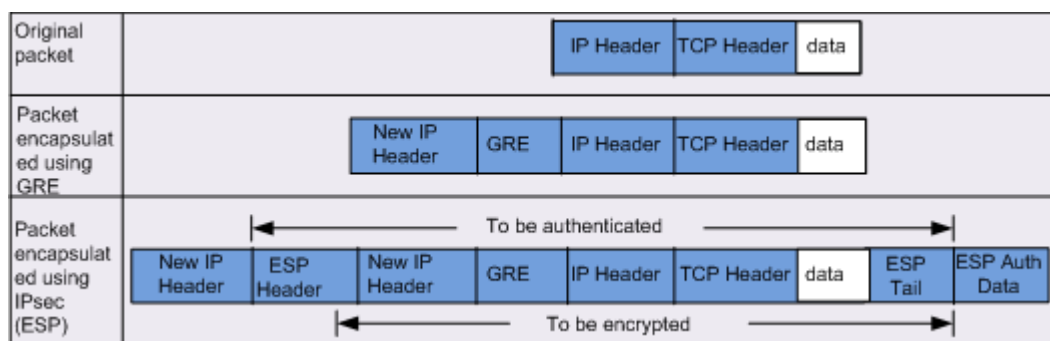


Figure 7. GRE over IPsec encapsulation mode (tunnel mode). (Huawei 2019)

As can be seen from the figure 7, the default packet is firstly encapsulated by GRE for transporting by adding to additional segments. Secondly, it is encrypted with the help of IPsec to secure the transfer.

2.2.4 OpenVPN

As the previous VPN topology is suitable for site-to-site topology, some users might want to connect to the local network from the outside just their computers. OpenVPN has perfectly suited this demand. It is user friendly, as it has a graphical user interface and it is simple to configure on a host by running premade configuration file.

OpenVPN is a VPN protocol, such as PPTP or L2TP. It is open source, though it has paid ready solutions for businesses and personal use to mitigate the configuration of server and client to the provider of the service.

3 PRACTICAL PART

The practical part will demonstrate the process of building a WAN for a restaurant franchise. I will present the background for the network demands, the overall topology of the WAN, steps on configuring routers and switches on sites and a budget list of the network devices.

3.1 Background of the restaurants

A restaurant is a public place with hundreds or even thousands of daily visitors. People come there often not just to eat, but have a rest, meet friends, in other words enjoy their time. While the guests are relaxing, the employees are doing just the opposite. During the rush hours it can be so that everyone is working on its limit. Everyone and everything. When the rooms are crowded with clients and the workers are busy with the orders, each of them is using a network. While some kids might want to watch a cartoon in a high quality, a manager is accessing the video server to get old footage of someone stealing a potato from the kitchen. This is an example of how the restaurants can be overloaded with traffic.

When creating a local network for a restaurant, there are lots of aspects to be considered but the most important are security and redundancy. Since it is an

accumulation of people, there will possibly be malicious clients. Furthermore, the network can easily be jammed during the rush hour if every client will start using the guest Wi-Fi.

3.1.1 The data flow in the restaurant

In restaurants, various devices are used. The most essential computer devices are the points of sale as orders are typed there by waiters and then it is sent to the kitchen, it calculates and prints the receipt and sends the billing data to the enterprise resource planning (ERP) database installed on the main server where all the accounting is held. If something goes wrong, it won't be possible to pay for the order or scan the discount card. From the networking point of view, points of sales are just computers, therefore no specific configuration is needed.

Waiters have phones connected to the LAN using Wi-Fi. Smartphones would have a special app that operates with the sales points to put the order remotely and share it with the kitchen. Guests might want to use free Wi-Fi. Traffic is segmented to a separate network, the guest VLAN. With no routes to LAN, intruders will not be able to access the equipment. Furthermore, all the guest's data is transferred to the public Wi-Fi access management system to collect data about the clients to understand future business tactics.

As for any public place, there must be video surveillance. To store and provide the requested footage from the camera there must be a video server and controller. The video surveillance footage is copied to the main server in office.

3.1.2 Data flow in the office

In the office, there is the main server where the ERP is installed and run. For usability reasons, all the work with that system should be done on the server via Remote Desktop Protocol. By selecting this strategy, it is possible to save money on buying less powerful computers for the office and managers. Also, the work

could be done remotely, by connecting with OpenVPN to the office network from the home computer.

3.2 Overall topology

All the restaurants are connected to the office via GRE over IPsec. The office contains the main server with ERP and video server that collects footage from all the cameras. For safety and usability reasons – all the employees will use the RDP to work with the installed ERP.

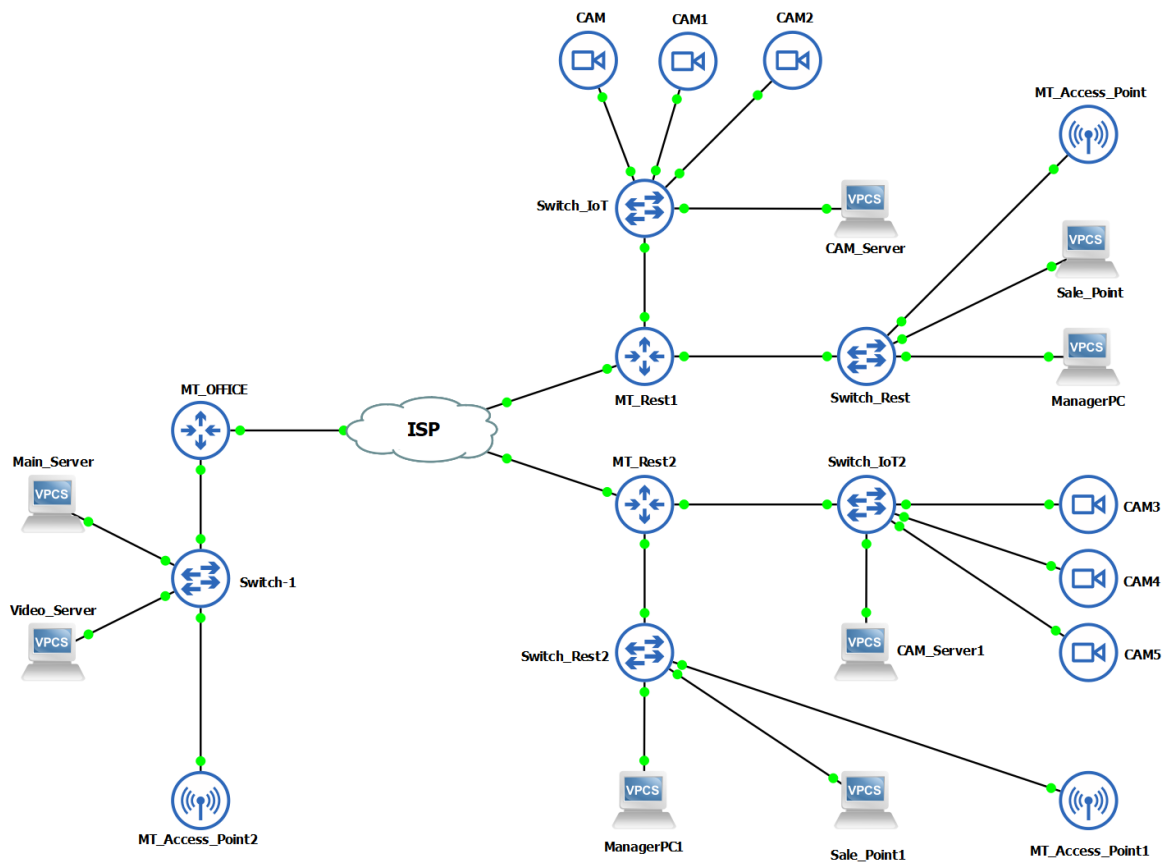


Figure 8. Overall logical topology.

There is a management VLAN in which all the networking devices have assigned IP addresses. This method provides additional security. If any device is compromised, the attacker will still need to guess the network address to access the networking equipment. Accessing the configuration panel from other VLANs must be forbidden. For a remote connection, it is enough to connect to a router and then use SSH in its console.

I have decided to build this project using MikroTik networking devices. It is a Latvian company that has developed its operating system (RouterOS) and hardware. The main advantages of using MikroTik are the low price and flexibility of the RouterOS, it can run scripts that are written by the same rules as in any modern programming language. The configuration is proceeded either by a command-line interface (CLI) or graphical user interface (GUI) app called WinBox.

Each facility has its network address for the LAN and defaults IP pools for internal VLANs. To standardize the configuration, some essential network equipment has static IP addresses. The IP pools are presented in Table 2.

Table 2. IP pools.

Network name	Network address	Host name	Ip address
	VLAN ID		
MAN	172.16.0.0/16	172.16.0.0 – 172.16.255.255	
		Office	172.16.234.0/24
		Restaurant 1	172.16.1.0/24
		Restaurant 2	172.16.2.0/24
		Restaurant 3	172.16.3.0/24
		Restaurant 4	172.16.4.0/24
		Restaurant 5	172.16.5.0/24
VLAN IoT	172.16.65.0/24	172.16.65.1 - 172.16.65.254	
	65	Router	172.16.65.1
		Video Server	172.16.65.6
		DHCP pool	172.16.65.11 - 240
VLAN Guest	192.168.0.0/23	192.168.0.1 - 192.168.1.254	
	68	Router	192.168.0.1
		DHCP pool	192.168.0.11 - 1.240
VLAN Admin	172.16.66.0/24	172.16.66.1 - 172.16.66.254	
	66	Router	172.16.66.1
		Switch	172.16.66.10
		Switch_IoT	172.16.66.11
LAN	172.16.x.0/24	172.16.x.1 - 172.16.x.254	
	1	Router	172.16.x.1
		DHCP	172.16.x.11 – 240

OpenVPN	172.16.235.0/24	172.16.235.10 – 172.16.235.250
----------------	-----------------	--------------------------------

I built this project virtually using GNS3 and VMware Workstation. I used my laptop's network adapter as an ISP router. The 10.0.0.0\8 network is used as a public network in upcoming chapters.

3.3 Configuring the office

This chapter includes a configuration of the network and a topology overview for the office of the restaurant franchise.

3.3.1 Topology description

The office logical topology is created as simple as possible to elevate fault tolerance. As shown in Figure 9, It has one switch that connects all the devices. All the workstations in the office are connected with WLAN via access points. Video and main servers must be contained in a server cabinet together with a switch and router to restrict unauthorized physical access. The cabinet has an uninterruptable power supply (UPS). The main server has static IP – of 172.16.234.5, while the video server has 172.16.234.6.

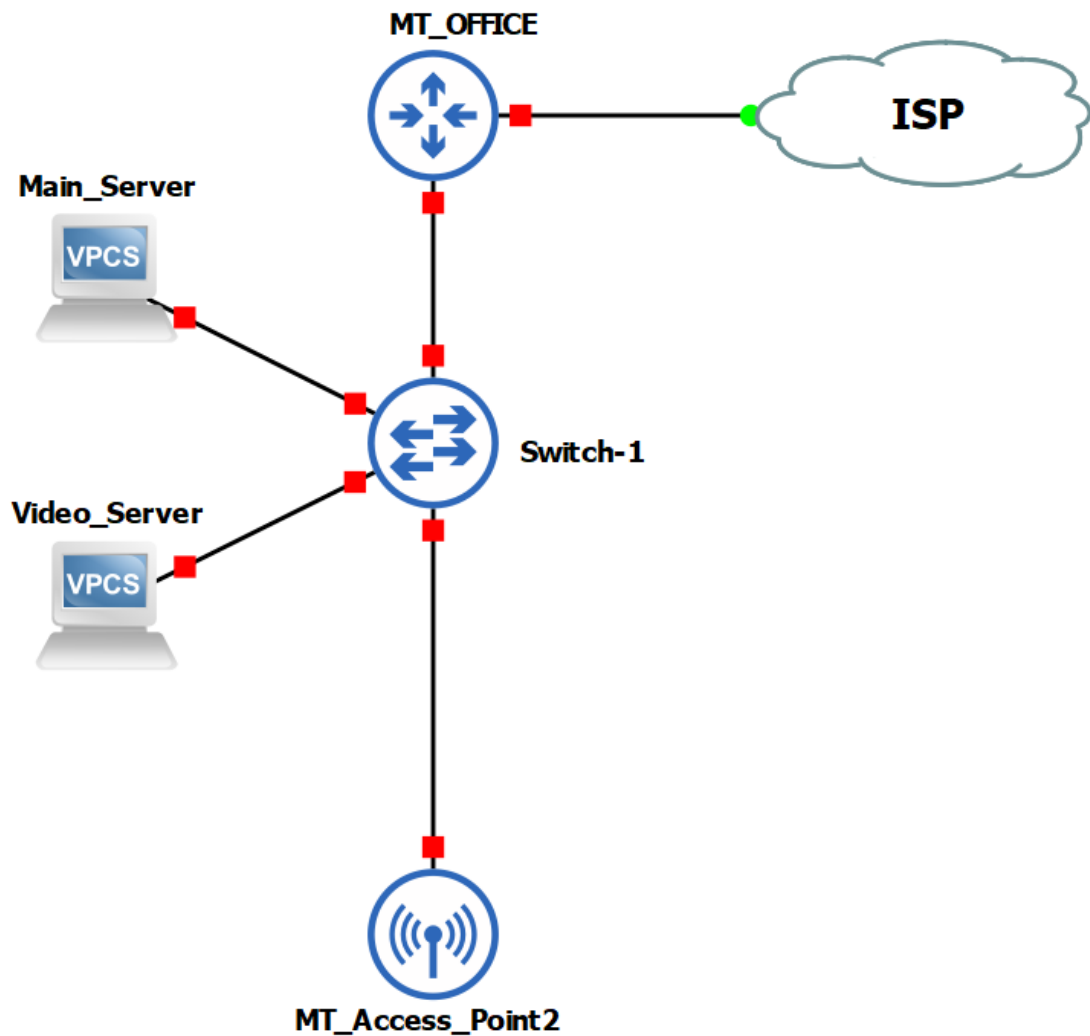


Figure 9. Office logical topology.

One 24 gigabit port switch should be enough for such a topology where all endpoint devices are connected wirelessly. The switch has PoE interfaces to power the APs. The MikroTik router OS has embedded controller features for MikroTik APs.

3.3.2 Router configuration

In this part, I will describe the configuration of a router using WinBox.

Firstly, I introduce what physical and logical interfaces there are on the router in the Figure 10. The first port on the device is connected to the Internet. It is renamed to ether1-WAN to be an easily recognizable in the configuration. All other physical interfaces and VLANs are assigned to the bridge named local. In RouterOS, a VLAN can be assigned only to one interface, either physical or logical.

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
DR	<> <ovpn-Denis>	OVPN Server Binding	1500			0 bps	0 bps	0
R	ether1-WAN	Ethernet	1500		101.2 kbps	6.0 kbps	7	9
RS	ether2	Ethernet	1500		0 bps	0 bps	0	0
RS	ether3	Ethernet	1500		0 bps	0 bps	0	0
RS	ether4	Ethernet	1500		0 bps	0 bps	0	0
	gre-tunnel_Rest_1	GRE Tunnel	1476	65535	0 bps	0 bps	0	0
	gre-tunnel_Rest_2	GRE Tunnel	1476	65535	0 bps	0 bps	0	0
R	local	Bridge	1500	65535	0 bps	0 bps	0	0
R	vlan_Admin	VLAN	1500	65531	0 bps	0 bps	0	0
R	vlan_Guest	VLAN	1500	65531	0 bps	0 bps	0	0
R	vlan_loT	VLAN	1500	65531	0 bps	0 bps	0	0
R	loopback	Bridge	1500	65535	0 bps	0 bps	0	0

Figure 10. List of interfaces.

Some interfaces are labelled with the interface lists that are presented in Figure 11. It will help to apply rules and policies to the groups of interfaces, not separately to each of them. It also provides a more easily readable appearance.

List	Interface
GRE	gre-tunnel_Rest_1
GRE	gre-tunnel_Rest_2
LAN	ether2
LAN	ether3
LAN	ether4
LAN	local
WAN	ether1-WAN

Figure 11. Interface lists

All the logical interfaces have an assigned IP address, most of them are default gateways for networks.

	Address	Network	Interface
D	10.0.0.11/8	10.0.0.0	ether1-WAN
	172.16.65.1/24	172.16.65.0	vlan_loT
	172.16.66.1/24	172.16.66.0	vlan_Admin
	172.16.234.1/24	172.16.234.0	local
D	172.16.235.1	172.16.235.238	<ovpn-Denis>
	172.22.22.1/30	172.22.22.0	gre-tunnel_Rest_1
	172.22.22.5/30	172.22.22.4	gre-tunnel_Rest_2
	192.168.0.1/23	192.168.0.0	vlan_Guest

8 items

Figure 12. Address List for Office Router.

The letter “D” in the table from Figure 12, which represents the list of assigned addresses, stands for dynamic allocation of the IP address. For example, the address 10.0.0.11 is assigned by the ISPs DHCP server.

There are local DHCP servers for LAN, IoT VLAN and Guest VLAN, which can be seen in Figure 13. Each of them has an IP pool capable to provide 230 IP addresses for the connections. Notice that Guest VLAN has a completely different network, this is another small precaution for securing the premises. There is also a pool of addresses for OpenVPN services. I suggest to leave some free addresses in the pool for special cases, for example, 172.16.234.5 is assigned to the main server, or 172.16.235.2-5 can be used for administrator’s accounts over VPN.

Name	Interface	Relay	Lease Time	Address Pool
dhcp_Guest	vlan_Guest		00:10:00	pool_dhcp_Guest
dhcp_loT	vlan_loT		00:10:00	pool_dhcp_CAM
dhcp_LAN	local		00:10:00	pool_dhcp_LAN

3 items

Name	Addresses
pool_dhcp_CAM	172.16.65.11-172.16.65.240
pool_dhcp_Guest	192.168.0.2-192.168.1.254
pool_dhcp_LAN	172.16.234.10-172.16.234.240
pool_openvpn	172.16.235.11-172.16.235.240

Figure 13. DHCP servers and IP pools.

The office router has an OpenVPN server running to allow the employees to connect to the server from any point of the world securely. Figure 14 shows its parameters. To connect to the office via OpenVPN it is required to use generated

CA and client certificates together with the credentials that are created separately for each user. New connections will get an IP address from the “pool_openvpn”.

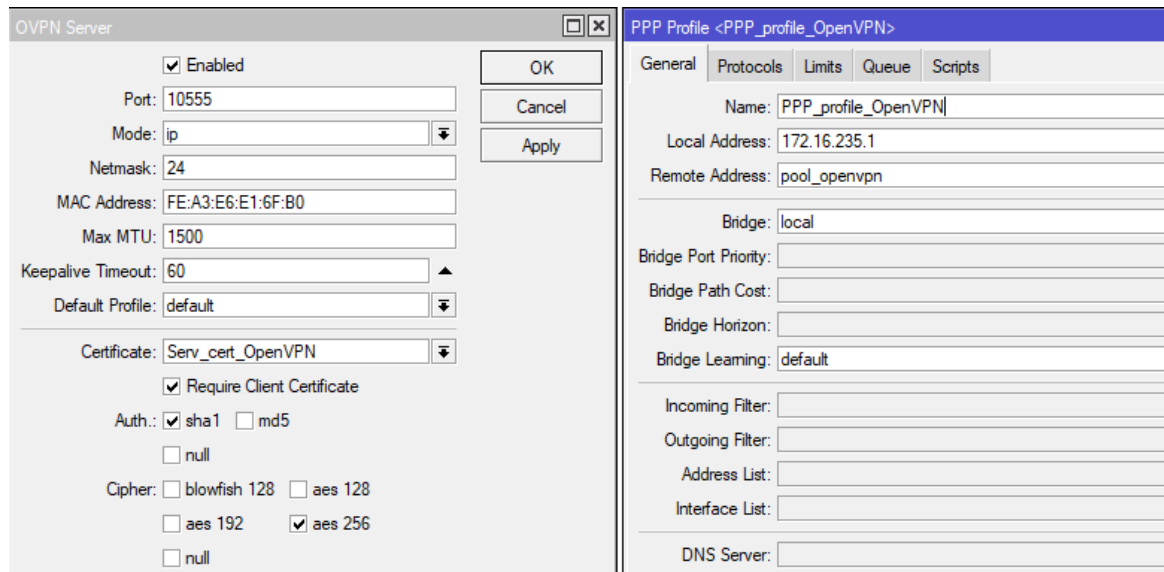


Figure 14. OpenVPN server configuration.

The following lines form a configuration file for OpenVPN clients:

Client – Specify that it is a client

dev tun – Choose which interface to use TAP/TUN

proto tcp – Which protocol to use.

remote 10.0.0.11 10555 – Public IP address with the port number of the VPN server.

resolv-retry infinite – Set the amount of tries to connect

cipher AES-256-CBC – Select the cryptographic cypher

remote-cert-tls server – Verify the server certificate

auth-user-pass – Enable authentication with user credentials

verb 3 – Set the verbosity of logging

route 172.16.234.0 255.255.255.0 – Create a static route to the network

route 172.16.1.0 255.255.255.0 172.16.235.1 – Create a static route to the network

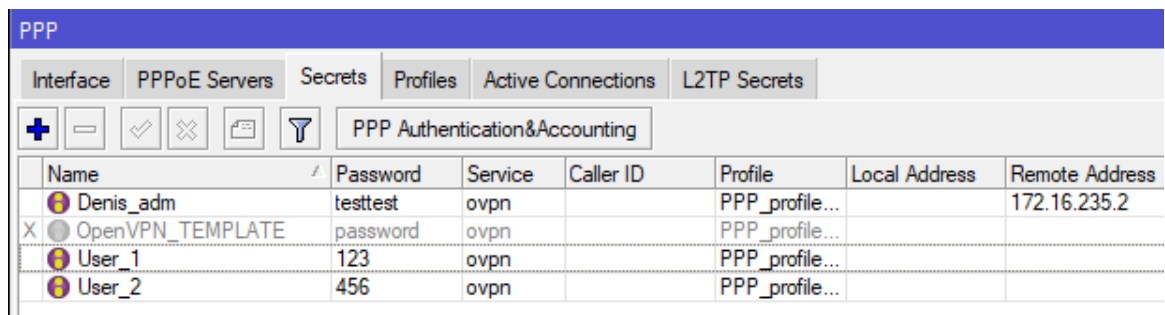
route 172.16.2.0 255.255.255.0 172.16.235.1 – Create a static route to the network

<ca> ----- CERTIFICATE----- </ca> - Enter the certificate authority that was exported from the MikroTik router

<cert> ----- CERTIFICATE----- </cert> - Enter the client certificate that was exported from the MikroTik router

<key> ----- CERTIFICATE----- </key> - Enter the private key that was exported from the MikroTik router

I have created an admin account and assigned it a static IP address. Therefore, this IP address is added to the access list in the firewall, while other OpenVPN users are only allowed to access the server. Figure 15 has an example of the users' list in RouterOS.



The screenshot shows the RouterOS configuration window for PPP. The 'Secrets' tab is selected, and the 'PPP Authentication & Accounting' section is active. A table lists the configured users:

Name	Password	Service	Caller ID	Profile	Local Address	Remote Address
Denis_adm	testtest	ovpn		PPP_profile...		172.16.235.2
X OpenVPN_TEMPLATE	password	ovpn		PPP_profile...		
User_1	123	ovpn		PPP_profile...		
User_2	456	ovpn		PPP_profile...		

Figure 15. List of OpenVPN users.

Speaking of VPN, one of the most important parts of this project is the GRE tunnels secured with IPsec. After pointing the GRE with a public IP of a restaurant, it is required also to provide an IP network for the new tunnel which is 172.22.22.0/30. With the subnet mask of 30, there are only 2 addresses available for hosts. There is a different network for each new tunnel. Figure 16 includes the GRE setup window.

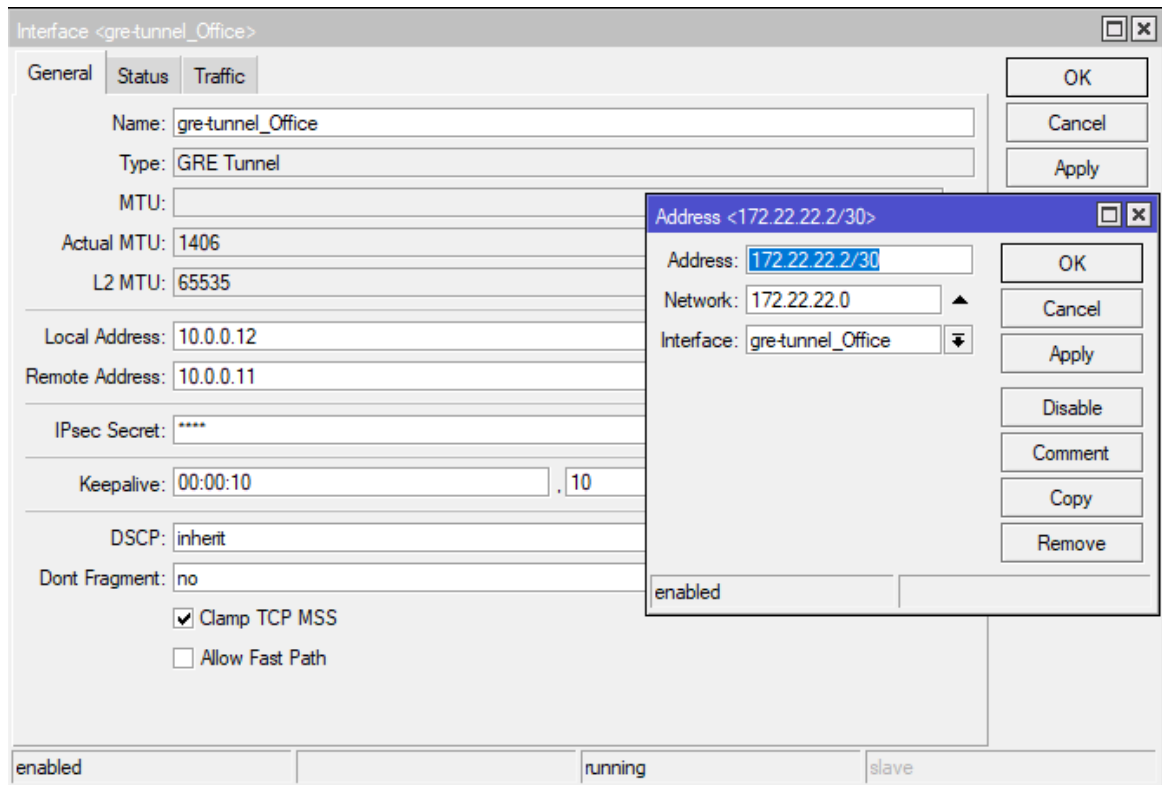


Figure 16. GRE tunnel interface GUI.

IPsec is turned on by providing a pre-shared key, or password, which I would suggest creating with a random password generator and then storing in some safe folder. As shown in Figure 17, the IPsec is set up to use at least sha256 for authentication, AES-256 for encryption and modp2048 for the DH algorithm. This will provide the highest level of security for the tunnel.

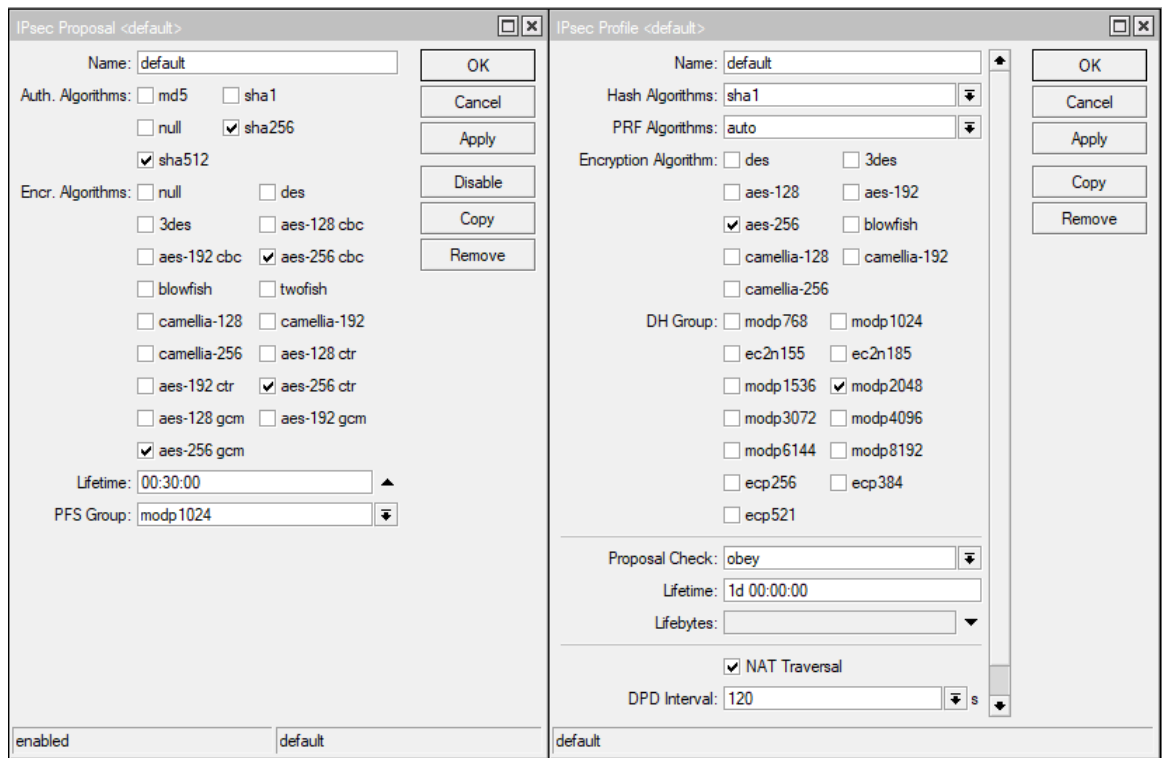


Figure 17. IPsec configuration.

To keep things simple, I decided to not use dynamic routing protocols. In restaurants, there are no regularly changing devices. Therefore, the static routes between the LANs are enough for this project.

All the traffic coming out to the WAN interface comes through NAT, so the source address is changed to the router's public address which is 10.0.0.11 in this case. There is also another rule in the NAT table, as can be seen in Figure 18. It is a destination network address translation to access the video server from the WAN. It is needed for the camera surveillance application access outside the local network.

The screenshot shows the 'Firewall' configuration window with the 'NAT' tab selected. The NAT table is visible with the following entries:

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Interface List
0	masquer...	srcnat							WAN
... For Video Server									
1	dst-nat	dstnat			6 (tcp)		10666		

Figure 18. NAT table.

I configured the firewall rules with the principle of least privilege. It means anything or anyone should have as minimal access as possible without influencing operating channels. In other words, forbid everything and then allow as least as possible. The final list of firewall rules is represented in Figure 19.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface List	Out. Interface List
	defconf: accept established,related								
1	✔ acc...	input							
	defconf: drop invalid								
2	✘ drop	input							
	defconf: accept ICMP								
3	X ✔ acc...	input			1 (ic...				
	Video Server								
4	✔ acc...	input			6 (tcp)		10666	WAN	
	OpenVPN								
5	✔ acc...	input			6 (tcp)		10555	WAN	
	accept OpenVPN admin connection								
6	✔ acc...	input	172.16.235.2						
	accept from GRE only to server								
7	✔ acc...	input		172.16.234.5				GRE	
	accept from OpenVPN only to server								
8	✔ acc...	input	172.16.235.0/24	172.16.234.5					
	defconf: drop all not coming from LAN								
9	✘ drop	input						!LAN	
	defconf: accept in ipsec policy								
10	✔ acc...	forward							
	defconf: accept out ipsec policy								
11	✔ acc...	forward							
	defconf: accept established,related, untracked								
12	✔ acc...	forward							
	Drop from guest not to WAN								
13	✘ drop	forward	192.168.0.0/23						!WAN
	defconf: drop invalid								
14	✘ drop	forward							
	defconf: drop all from WAN not DSTNATed								
15	✘ drop	forward						WAN	

Figure 19. Firewall Filter Rules.

In the first row, the router will pass through all the traffic that is already established. Next, it will drop invalid packets. After there are two allowance rules for OpenVPN and video server. Then, there is a rule that would allow OpenVPN admin profile to communicate with the router, while the rows after that grant the permission to access only the server to everyone in the OpenVPN network or hosts from the GRE tunnels. 9th rule drops all the traffic coming not from LAN. Lastly, there is a forbidding rule for guest VLAN. It drops all the traffic that is not

going to the WAN interface list. Finally, the last rule drops all the packets that are not confirmed by destination NAT, which in this build everything except traffic coming to the video server.

The final step in completing the configuration is to set up the CAPsMAN, access points controller built-in RouterOS. For each SSID there must be created a separate configuration. The configurations are presented in Figure 20. I have assigned Wi-Fi for employees to the LAN, while the guests to the 68th VLAN. There is also SSID for IoT devices that might be in use. Though the name is hidden, not broadcast, it must be typed manually to initialize a connection. Furthermore, the country and installation area, inside or outside, should be selected, so the router can automatically configure channels. Finally, the password is set for LAN and IoT SSIDs, the authentication method is WPA2 PSK and the encryption is set to AES CCM.

Name	SSID	VLAN ID	Hide SSID	Load Bal...	Country	Install...	Band	Bridge	Chann▼
cfg_Guest_2	FOR_OUR_LOVELY_GUEST	68			finland	indoor	2ghz-g/n	local	
cfg_Guest_5	FOR_OUR_LOVELY_GUEST	68			finland	indoor	5ghz-n/ac	local	
cfg_LAN_2	OUR_OFFICE	1			finland	indoor	2ghz-g/n	local	
cfg_LAN_5	OUR_OFFICE	1			finland	indoor	5ghz-n/ac	local	
cfg_loT	office_loT_1423		65 yes		finland	indoor	2ghz-g/n	local	

Figure 20. WLAN configurations.

After the configurations are done, they are put for provisioning to the access points and then the AP manager must be enabled. Also, it is advised to specify on which ports the router should listen for new APs advertisements. I switched this function to listen on the local bridge. Figure 21 shows the GUI for the AP's manager.

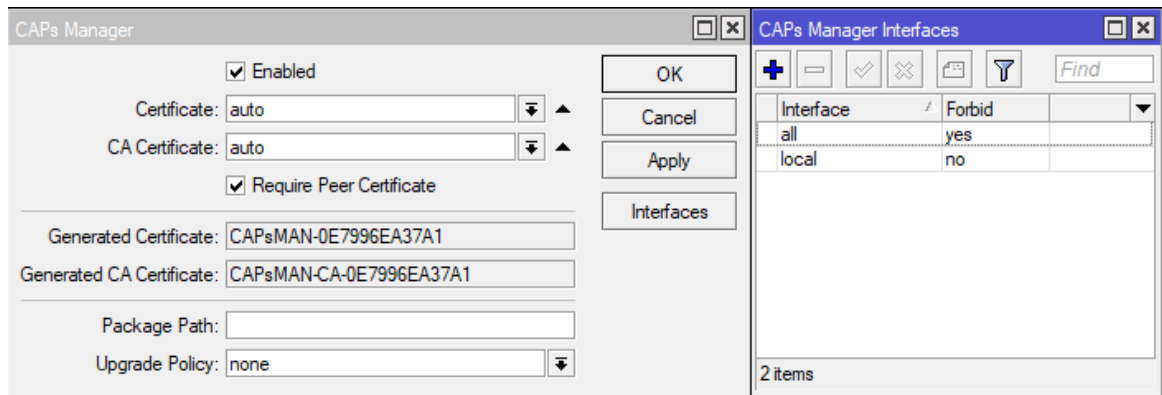


Figure 21. CAPs manager.

From now on, the access point should be provisioned with the configuration automatically. Unfortunately, the virtual image of RouterOS does not provide virtual wireless interfaces for testing, this is why I am not able to test the work of the access points.

3.3.3 Switch configuration

The switch in this project can be any vendor since it only must support VLANs and PoE to fulfil the needs of the topology. Interfaces that are connected to the router and access points must be in trunk mode with the following allowed VLAN IDs: 1, 65, 66 and 68. Any other connected ports should be in access mode with default 1 VLAN.

A logical interface is created in VLAN 66 Admin. The switch has a static IP address assigned to it, 172.16.66.10. This should be the only way to access the switch remotely. It can be easily done using SSH from the router.

3.4 Configuring the restaurant

This chapter introduce setting up process for network devices in the restaurant.

3.4.1 Overall topology of the restaurant

The site topology has two separated switches for different purposes. They are placed in the same cabinet and separated only logically by assigning VLANs to

interfaces. This way, in case one of the switches is ran out of free ports, the other switch can still be used. Figure 22 shows the logical topology for the restaurant.

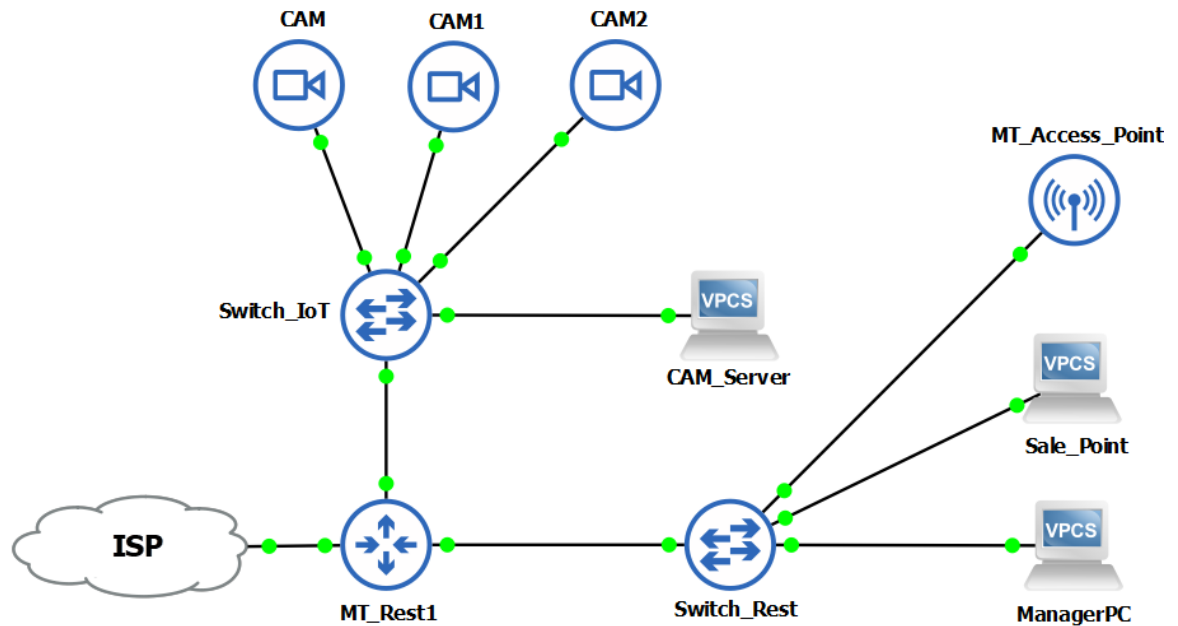


Figure 22. Logical topology of a restaurant.

All the sale points are connected with an ethernet cable to the switch to increase redundancy. Employees use work Wi-Fi for connection. Each room have an Access Point for stable and fast connection. All APs have dual-band and provide 2 SSIDs: guests and workers. They are powered by power over ethernet (PoE) from the Switch_Rest. Thus, the switch must have PoE ports. Therefore, all the cameras are connected to another switch that also has PoE to power the equipment. The video server is connected to the same switch as the surveillance with two interfaces to communicate in two VLANs: IoT and LAN.

3.4.2 Network configuration

The configuration in a restaurant does not differ much from that of the Office. A few details should be changed and some features are not used at all.

For easy implementation, the configuration from the office router can be copied. All the IP addresses then should be changed: LAN, static routes, GRE tunnel, IP pool. OpenVPN server is not implemented, since there is no need for a remote

connection for the employees. Besides the IP address, the firewall should get rid of allowance rules for OpenVPN. Lastly, it is wise to change the admin password.

The switches are configured so that the interfaces that are looking to the router or access points are configured in trunk mode with allowed 1, 65, 66 and 68 VLANs. Both switches have an IP address assigned to the logical interface VLAN 66 for administration.

The IoT switch has ports with PoE which are assigned to VLAN ID 65 for cameras and two ports are assigned to 65 and 1 VLANs for the video server. The other switch has access points connected to the trunk ports. All other interfaces are assigned to VLAN ID 1 for LAN communication.

3.5 List of hardware and budgets

For this project, I decided to use cheaper solutions as restaurants do not produce large amounts of traffic. The second parameter for consideration was mobility and ease of installation. In my opinion, MikroTik fits these criteria the best. Therefore, it is possible to implement this project using any other vendor as there are only multivendor protocols, except the AP controller.

I selected Mikrotik RouterBOARD hEX S, shown in Figure 23, as a restaurant router solution. It has 5 gigabit ethernet interfaces together with an SFP port which should be used for connection to ISP. It is cheap and small in size but has quite impressive computing powers. There is a dual-core 880 MHz CPU together with 256 MB RAM, this is enough for maintaining all the traffic generated in a restaurant and even more. Additionally, it has built-in IPsec hardware encryption. The price of the model is EUR 70.

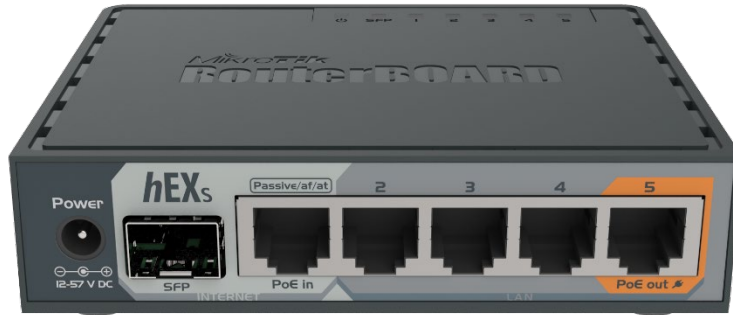


Figure 23. Mikrotik RouterBOARD hEX S (Mikrotik)

The specifications of the Mikrotik RouterBOARD hEX S are listed in Table 3.

Table 3. Mikrotik RouterBOARD hEX S specifications.

Product code	RB760iGS
CPU nominal frequency	880 MHz
CPU core count	2
CPU threads	4
Size of RAM	256 MB
Storage size	16 MB
10/100/1000 Ethernet ports	5
SFP cages	1
IPsec hardware acceleration	yes
Supported input voltage	DC and PoE in: 12 - 57 V
PCB temperature monitor	Yes
Voltage monitor	Yes
Operating temperature	-40°C to +70°C
Dimensions	113 x 89 x 28 mm
Operating system	RouterOS
Max power consumption	24 W
Max power consumption without attachments	6 W

For the office, I have chosen CCR2004-16G-2S+PC, which is shown in Figure 24. It has a quad-core processor working together with 4 GBs of RAM. It is enough to handle the communication of several facilities with the server located behind it. There are two SFP+ interfaces with 10 Gbps full-duplex lines. This is especially needed because the video server is collecting all the footage from the restaurants in live mode. The approximate price of the model is EUR 400.

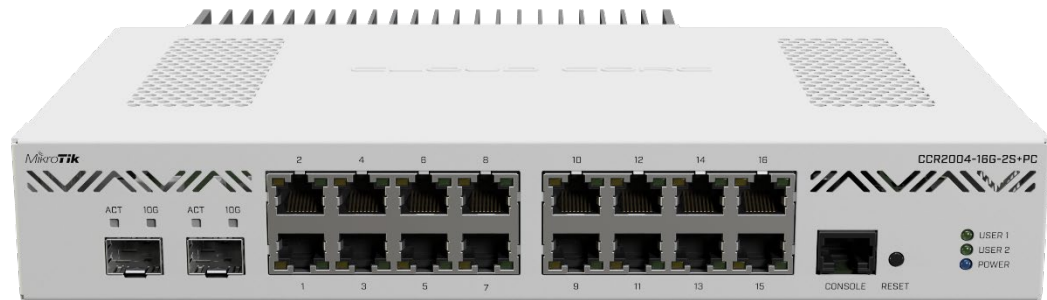


Figure 24. CCR2004-16G-2S+PC. (Mikrotik)

The specifications of the MikroTik CCR2004-16G-2S+PC are listed in Table 4.

Table 4. MikroTik CCR2004-16G-2S+PC specifications.

Product code	CCR2004-16G-2S+PC
CPU nominal frequency	1.2 GHz
CPU core count	4
Size of RAM	4 GB
Storage size	128 MB
10/100/1000 Ethernet ports	16
SFP+ cages	2
Supported input voltage	36-57 V (DC jack) 36-57 (2-pin terminal)
PCB temperature monitor	Yes
Voltage monitor	Yes
Operating temperature	-20°C to +60°C
Dimensions	272 x 195 x 44 mm
Operating system	RouterOS
Max power consumption	36 W
Max power consumption without attachments	30 W

I selected CRS328-24P-4S+RM as a switch for both office and restaurants (Figure 25). The main consideration explaining my choice is the PoE accessible on all ethernet ports with a total of 450 W available while the price is below average with the same specifications. Another feature that might help in critical situations is the Dial boot. The switch has RouterOS and SwitchOS, this allows to use it as a router if something happens to the main router. The configuration can easily be copied from the backup and installed in one moment. The approximate price of the model is EUR 350.



Figure 25. CRS328-24P-4S+RM. (Mikrotik)

The specifications of the MikroTik CRS328-24P-4S+RM are listed in Table 5.

Table 5. MikroTik CRS328-24P-4S+RM specifications.

Product code	CRS328-24P-4S+RM
CPU nominal frequency	800 MHz
CPU core count	1
Size of RAM	512 MB
Storage size	16 MB
10/100/1000 Ethernet ports	24
SFP+ cages	4
Supported input voltage	100 - 240 V
PCB temperature monitor	Yes
Voltage monitor	Yes
Operating temperature	-20°C to +60°C
Dimensions	443 x 300 x 44 mm
PoE-out ports	Ether1-Ether24
Operating system	SwOS / RouterOS (Dual boot)
Max power consumption	494 W
Max power consumption without attachments	44 W

I have chosen MikroTik cAP XL ac as the indoor access point, it is presented in Figure 26. It is a dual-band access point that is presumably low cost and can be controlled by CAPsMAN implemented in RouterOS. There is a PoE gigabit interface. This device is suitable to use in both office and restaurants. The approximate cost of the model is EUR 75.



Figure 26. MikroTik cAP XL ac. (MikroTik)

The specifications of the MikroTik cAP XL ac are listed in Table 6.

Table 6. MikroTik cAP XL ac specifications.

Product code	RBcAPGi-5acD2nD-XL	
CPU nominal frequency	710 MHz	
CPU core count	4	
Size of RAM	128 MB	
Storage size	16 MB	
10/100/1000 Ethernet ports	2	
Wireless	2.4 GHz	5 GHz
Mx data rate	300 Mbit/s	867 Mbit/s
Supported protocol	802.11b/g/n	802.11a/n/ac
Antenna gain	6 dBi	5.5 dBi
Supported input voltage	18-57 V	
IPsec hardware acceleration	Yes	
Operating temperature	-40°C to 70°C	
Dimensions	191 x 42 mm	
Operating system	RouterOS	
Max power consumption	24 W	
Max power consumption without attachments	11 W	

Lastly, I choose MikroTik wAP ac as an outdoor access point for the restaurant's terrace (Figure 27). It is an outdoor version of cAP XL ac with an IP waterproof rating of 54 which stands for complete protection against water splashing. Also, it

has less powerful antennas built-in. The approximate cost of the model is EUR 75.



Figure 27. MikroTik wAP ac. (MikroTik)

The specifications of the MikroTik wAP ac are listed in Table 6.

Table 7. MikroTik wAP ac specifications.

Product code	RBwAPG-5HacD2HnD	
CPU nominal frequency	488-896 (auto) MHz	
CPU core count	4	
Size of RAM	128 MB	
Storage size	16 MB	
10/100/1000 Ethernet ports	2	
Wireless	2.4 GHz	5 GHz
Mx data rate	300 Mbit/s	867 Mbit/s
Supported protocol	802.11b/g/n	802.11a/n/ac
Antenna gain	2.5 dBi	2.5 dBi
Supported input voltage	10-57 V	
IPsec hardware acceleration	Yes	
Operating temperature	-40°C to 70°C	
IP waterproof	IP54	
Dimensions	185 x 85 x 30 mm	
Operating system	RouterOS	
Max power consumption	10 W	
Max power consumption without attachments	9 W	

It is always important to choose reliable hardware at least at the most critical points, the routers. The mobility and compatibility of MikroTik equipment inside its ecosystem allow it to easily and quickly replace not working devices in a critical moment.

The approximate cost of networking equipment for the office would be EUR 1000 except for the costs of the consumables and installation. For a single restaurant, the relative price is EUR 1300.

4 CONCLUSION

The technologies nowadays have evolved exponentially compared to the last 20 years. Without computers, now it will not be impossible to buy something at a grocery store if the cashier stopped working. All the life support infrastructures are completely dependent on the machines. This all can be possible mainly because of the Internet as it allows machines to communicate.

These days people spend years studying networks, as there are an enormous number of aspects to pay attention to. Configuring the LAN is a responsible role because leaving a security breach might cost a company a huge sum. In this project, I tried to cover all three sides of a successfully working network: functionality, security and usability. In the theory part, I gained basic knowledge of the necessary protocols and mechanisms for building local and metropolitan area networks. Therefore, I implemented theoretical knowledge together with my practical experience to virtually design and plan a network for a restaurant franchise consisting of the office with the main server and indefinitely restaurants. I used the GNS3 network software simulator together with the VMware workstation to recreate the project in the virtual environment. For this project, I have chosen to use MikroTik networking devices. This vendor provides the graphical interface application WinBox which I used to configure the equipment.

The topology is tested in the virtual lab environment, though the implementation of my project in real life might face some difficulties. Due to restricted functionality, I was not able to test the wireless connectivity and provisioning of

the configuration to the access points. Furthermore, the guest Wi-Fi is most likely to use some public Wi-Fi management company solutions or different vendors might want access to its devices, therefore some firewall rules and default gateways must be considered. Finally, different vendors of endpoint devices might want access to their devices so the firewall should have opened ports for them. It is wise to build large-scale networks with a team of professionals where each member would have some specialization in various spheres such as routing or security. At present, there are excessive lists of technologies being used in modern systems, though they must be used as the demand grows.

REFERENCES

Bhardwaj, R. n. d. GRE over IPsec vs IPsec over GRE: Detailed Comparison. WWW document. Available at: <https://ipwithease.com/gre-over-ipsec-vs-ipsec-over-gre/> [Accessed 6 March 2022]

Bluecat. n. d. What is DHCP? WWW document. Available at: <https://bluecatnetworks.com/glossary/what-is-dhcp/> [Accessed 2 March 2022]

Cisco. n. d. What is Lan? WWW document. Available at: <https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html> [Accessed 2 March 2022].

Cisco. n. d. What is Power over Ethernet (PoE)? WWW document. Available at: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-power-over-ethernet.html> [Accessed 3 March 2022]

Cisco. n. d. Configuring VLANs. WWW document. Available at: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/layer2/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Layer_2_Switching_Configuration_Guide_Release_5-x_chapter4.html#:~:text=A%20VLAN%20is%20a%20group,on%20the%20same%20LAN%20segment. [Accessed 3 March 2022]

Cisco. n. d. What is Firewall? WWW document. Available at: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html> [Accessed 3 March 2022]

Cloudflare. n. d. What is GRE? WWW document. Available at: <https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/> [Accessed 6 March 2022]

CompTIA. n. d. What is NAT? WWW document. Available at:

<https://www.comptia.org/content/guides/what-is-network-address-translation>

[Accessed 2 March 2022]

Google Nest Help. n. d. What is a mesh network? WWW document. Available at:

<https://support.google.com/googlenest/answer/7182746?hl=en#:~:text=A%20mesh%20network%20is%20a,Fi%20sources%20are%20called%20points>. [Accessed

3 March 2022]

Kaspersky. n. d. What is an IP Address - Definition and Explanation. WWW

document. Available at: <https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address> [Accessed 2 March 2022]

Mikrotik. n. d. hEX S. WWW document. Available at:

https://mikrotik.com/product/hex_s [Accessed 1 April 2022]

Mikrotik. n. d. CCR2004-16G-2S+PC. WWW document. Available at:

https://mikrotik.com/product/ccr2004_16g_2s_pc [Accessed 1 April 2022]

Mikrotik. n. d. CRS328-24P-4S+RM. WWW document. Available at:

https://mikrotik.com/product/crs328_24p_4s_rm [Accessed 1 April 2022]

Mikrotik. n. d. cAP XL ac. WWW document. Available at:

https://mikrotik.com/product/cap_xl_ac [Accessed 1 April 2022]

Mikrotik. n. d. wAP ac. WWW document. Available at:

https://mikrotik.com/product/wap_ac [Accessed 1 April 2022]

Techopedia. 2020. Wireless Local Area Network (WLAN). WWW document.

Available at: <https://www.techopedia.com/definition/5107/wireless-local-area-network-wlan> [Accessed 3 March 2022]