Week 2 Portfolio

# Networking Virtual Machines:

Is made up of all the same hardware, but in this case, they are virtualized. A Virtual Network consists of one or more virtual machines that are used to send and receive data from another virtual machine.

# Virtual Switches:

Virtual Switches are responsible to connect virtual machines to the virtual network. They almost the same as physical switches, with some limitations and controls to connect virtual machines.

# VPN:

VPN is a service that you sign up online, and with the creation of your account, the VPN service should be online. VPN in action takes the Internet connection and creates a more secure environment to use the internet, with it you can be safer and anonymous and helps around blocks and censored sites. The VPN change the IP address and creates a temporary one and hides the true IP address.

# VPS:

VPS hosting, is a virtual and private server. VPS is also one of the several types od web hosting but this one is private. If you want to have a web site in the web you need to find a server to drop it, so the VPS is a virtual server that you don’t need the hardware to run the server.

# Routing Tables:

Routing tables contain all the information necessary to forward a packet along the path to the destination. The packets contain information about the origin and the destination.

After the packet is received the network examines the routing table to provide the best match for the destination, after the table provides the device all the instructions for sending the packet too the next stop and continues across the network.

# NAT and PAT:

NAT (Network Address Translation) provides a one-to-one translation from IP Address.

Normally used in organization that wants to give internal system access in the private address, in the NAT situation the firewall will have a table like the IP.

PAT (Port Address Translation) uses the many-to-one relationship. This is commonly used on a firewall when a corporation wants all IP addresses in its internal network to use a single IP address. If a company wants to use the same IP address to all the computers in the company.

# VLAN:

VLAN (Virtual LAN) abstracts the idea of the LAN, VLAN might comprise a subset of the ports on a switch. By default, systems on one VLAN don’t see the traffic associated with systems on other VLANs on the same network.

VLAN is the same thing as a LAN but is a virtual one.

# VTP:

VTP (VLAN Trunk Protocol), this is the protocol used in the Virtual LAN

# POE & Traffic Filtering:

Power over Ethernet (POE) is a technology that lets network cables carry electrical power.  
For example, a digital security camera normally requires two connections to be made when it is installed: A *network connection*, to be able to communicate with video recording and display equipment  
A *power connection*, to deliver the electrical power the camera needs to operate.

Time and cost savings - by reducing the time and expense of having electrical power cabling installed.  Network cables do not require a qualified electrician to fit them, and can be located anywhere.

# Port Mirroring:

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic such as an intrusion detection system, passive probe or real user monitoring (RUM) technology that is used to support application performance management (APM). Port mirroring on a Cisco Systems switch is generally referred to as *Switched Port Analyzer* (SPAN) or *Remote Switched Port Analyzer* (RSPAN). Other vendors have different names for it, such as *Roving Analysis Port* (RAP) on 3Com switches.

# Load Balancing:

In computing, loadbalancing improves the distribution of workloads across multiple computing resources, such as computers, a computer cluster, network links, central processing units, or disk drives. Load balancing aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource. Using multiple components with load balancing instead of a single component may increase reliability and availability through redundancy. Load balancing usually involves dedicated software or hardware, such as a multilayer switch or a Domain Name System server process.

# Proxy Server:

A proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service. The proxy server may exist in the same machine as a firewall server or it may be on a separate server, which forwards requests through the firewall.

# Content Filter:

On the Internet, content filtering (also known as *information filtering*) is the use of a program to screen and exclude from access or availability Web pages or e-mail that is deemed objectionable. Content filtering is used by corporations as part of Internet firewall computers and by home computer owners, especially by parents to screen the content their children have access to from a computer.

# VPN Concentrator:

A VPN concentrator is a type of networking device that provides secure creation of VPN connections and delivery of messages between VPN nodes.

It is a type of router device, built specifically for creating and managing VPN communication infrastructures.

A VPN concentrator primarily adds the capabilities of a VPN router by adding advanced data and network security to the communications. It can create and manage a large quantity of VPN tunnels.

A VPN concentrator is typically used for creating site-to-site VPN architectures. It can:

-Establish and configure tunnels;

-Authenticate users;

-Assign tunnel/IP addresses to users;

-Encrypt and decrypt data;

-Ensure end-to-end delivery of data;

# Command Line Commands:

-ping: see the ping connection between the pc and the network

-tracert: that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.

-ipconfig: see the ip of the computer to connect to the network

-NS lookup: Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command-line tool is available only if you have installed the TCP/IP protocol.

-dig: Using dig, you can find out what a particular DNS server thinks the given host’s IP address should be, including a lot of other information that is also very helpful.

-arp: Arp allows you to view and modify the ARP cache. If two hosts on the same subnet cannot ping each other successfully, try running the arp -acommand on each computer to see whether the computers have the correct media access control (MAC) addresses listed for each other. You can use Ipconfig to determine a host's correct MAC address.

-nbt stat: MS-DOS utility that displays protocol statistics and current TCP/IP connections using [NBT](https://www.computerhope.com/jargon/n/nbt.htm)([NetBIOS](https://www.computerhope.com/jargon/n/netbios.htm) over [TCP/IP](https://www.computerhope.com/jargon/t/tcpip.htm)), which allow the user to troubleshoot NetBIOS name resolution issues. Normally, name resolution is done when NetBIOS over TCP/IP is functioning correctly. It does this through local cache lookup, WINS or [DNS](https://www.computerhope.com/jargon/d/dns.htm) server query or through [LMHOSTS](https://www.computerhope.com/jargon/l/lmhost.htm) or Hosts lookup.

-netstat: The netstat [command](https://www.lifewire.com/what-is-a-command-2625828) is a [Command Prompt command](https://www.lifewire.com/list-of-command-prompt-commands-4092302) used to display very detailed information about how your computer is communicating with other computers or network devices.

# IP Security:

Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks, using cryptographic security services. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPSec is based on standards developed by the Internet Engineering Task Force (IETF) IPSec working group.

# Remote Access:

Remote access is the ability to get access to a computer or a network from a remote distance. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporation's network. Home users get access to the Internet through remote access to an Internet service provider (IPS).

# SSH (Secure Shell):

This is the home page for the SSH (Secure Shell) protocol, software, and related information. SSH is a software package that enables secure system administration and file transfers over insecure networks. It is used in nearly every data centre, in every larger enterprise.

The SSH protocol uses encryption to secure the connection between a client and a server. All user authentication, commands, output, and file transfers are encrypted to protect against attacks in the network. For details of how the SSH protocol works, see the protocol page. To understand the SSH File Transfer Protocol, see the SFTP page.