Project objectives

The main task of this project is to design and implement a network topology to support the operation of the company's LAN and Remote networks. In order to build the topology, there are several devices that were used: four 2911 Routers, five 2960-24TT Switches, five PCs, four Printers, Laptop and a Server.

IP Addressing

In order to properly assign the subnets across the departments, the base IP address was divided following the best-practice according to the amount of hosts required per the division. Additionally, the IPv6 address was configured for all the devices. The main network was built on 192.168.72.0/24 base IPv4 address, the remote network using 10.10.1.0/16 as the base IPv4. The GUA address for IPv6 is 2001:db8:1::/64.

The network consists of the following departments with corresponding endpoint devices:

1) **Sales**: 50 PCs + 2 Printers + 2 laptops = 54 hosts (56 IPs)

   Subnet: 192.168.72.0/26; Range: 192.168.72.1 - 192.168.72.62

   IPv6: 2001:db8:1:10::/64

2) **Product Management**: 55 PCs + 3 Printers + 2 laptops = 60 hosts (62 IPs)

   Subnet: 192.168.72.64/26; Range: 192.168.72.65 - 192.168.72.126

   IPv6: 2001:db8:1:20::/64

3) **Finance**: 23 PCs + 2 printers + 2 laptops = 27 hosts (29 IPs)

   Subnet: 192.168.72.128/27; Range: 192.168.72.129 - 192.168.72.158

   IPv6: 2001:db8:1:30::/64

4) **HR**: 2 PCs + 1 printer = 3 hosts (5 IPs)

Subnet: 192.168.72.160/29; Range: 192.168.72.161 - 192.168.72.166

IPv6: 2001:db8:1:40::/64

Each subnet should be big enough to support the amount of hosts in each department, plus two IPs for the subnet name and broadcast as well. As a result, by picking the minimum sufficient number of IPs to support the department, starting with the department with the biggest number of hosts, each subnet was assigned with an appropriate address and subnet mask. In order for routers to operate, each connection between two of them also requires its own subnet.

1) **R1 - Main Router**: 192.168.72.168/30;

Range: 192.168.72.169 - 192.168.72.170

IPv6: 2001:db8:1:100::/64

2) **R2 - Main Router**: 192.168.72.172/30;

Range: 192.168.72.173 - 192.168.72.174

IPv6: 2001:db8:1:101::/64

3) **Main Router - Remote router**: 192.168.72.176/30;

Range: 192.168.72.177 - 192.168.72.178

IPv6: 2001:db8:1:102::/64

Due to the small number of devices in the Remote network, the subnet mask for it was also limited: 10.10.1.0/29; Range: 10.10.1.1 - 10.10.1.6; IPv6: 2001:db8:1:200::/64.

Following is the Addressing Table describing the IPv4 and IPv6 assigned to every usable interface of each device in the network.

Device	Interface	IP Address / Prefix		Default Gateway
R1	Gi0/1.10	192.168.72.1	255.255.255.192	-

		2001:db8:1:10::1/64		
	Gi0/2.20	192.168.72.65	255.255.255.192	-
		2001:db8:1:20::1/64		
	Gi0/0	192.168.72.169	255.255.255.252	-
		2001:db8:1:100::1/64		
		FE80::1		
R2	Gi0/1.30	192.168.72.129	255.255.255.224	-
		2001:db8:1:30::1/64		
	Gi0/2.40	192.168.72.161	255.255.255.248	-
		2001:db8:1:40::1/64		
	Gi0/0	192.168.72.173	255.255.255.252	-
		2001:db8:1:101::1/64		
		FE80::2		
R3 (Main Router)	Gi0/1	192.168.72.170	255.255.255.252	-
		2001:db8:1:100::2/64		
	Gi0/2	192.168.72.174	255.255.255.252	-
		2001:db8:1:101::2/64		
	Gi0/0	192.168.72.177	255.255.255.252	-
		2001:db8:1:102::1/64		
		FE80::3		
R4 (Remote)	Gi0/0	192.168.72.178	255.255.255.252	-
		2001:db8:1:102::2/64		
	Gi0/1	10.10.1.1	255.255.255.248	-
		2001:db8:1:200::1/64		

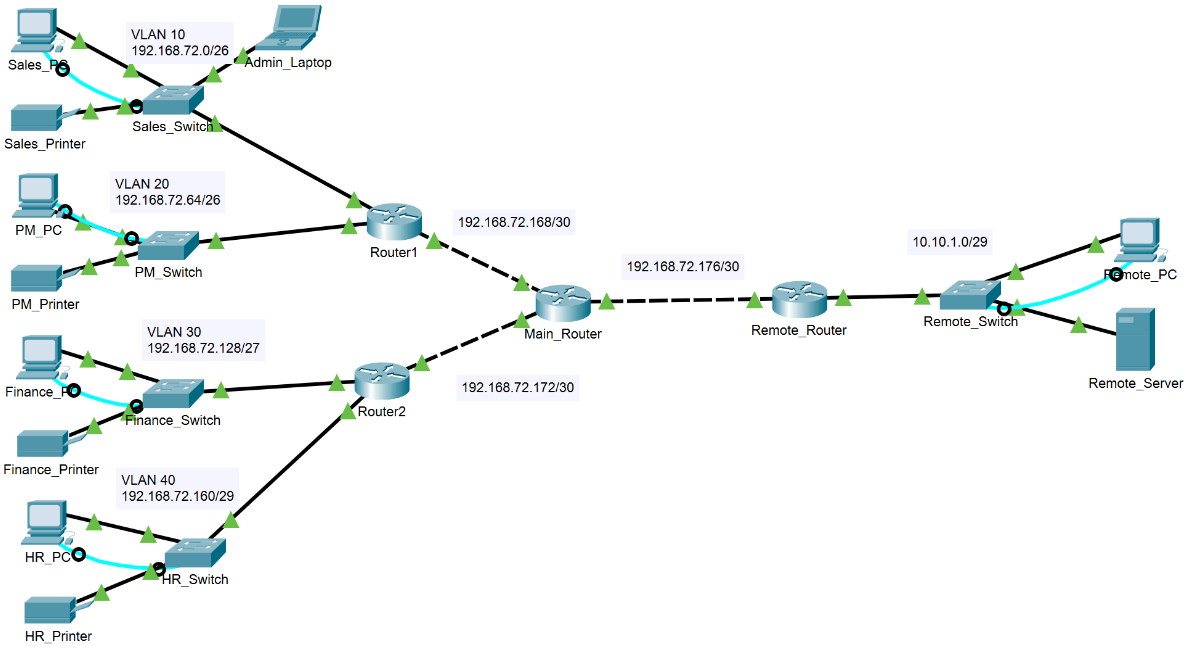
		FE80::4		
S1 (Sales)	VLAN60	192.168.72.62	255.255.255.192	192.168.72.1
		2001:db8:1:10::62/64		FE80::1
S2 (PM)	VLAN60	192.168.72.126	255.255.255.192	192.168.72.65
		2001:db8:1:20::62/64		FE80::1
S3 (Finance)	VLAN60	192.168.72.158	255.255.255.224	192.168.72.129
		2001:db8:1:30::62/64		FE80::2
S4 (HR)	VLAN60	192.168.72.166	255.255.255.248	192.168.72.161
		2001:db8:1:40::62/64		FE80::2
S5 (Remote)	VLAN1	10.10.1.6	255.255.255.248	10.10.1.1
		2001:db8:1:200::62/64		FE80::4
PC Sales	Fa0	192.168.72.2	255.255.255.192	192.168.72.1
		2001:db8:1:10::2/64		FE80::1
PC PM	Fa0	192.168.72.66	255.255.255.192	192.168.72.65
		2001:db8:1:20::2/64		FE80::1
PC Finance	Fa0	192.168.72.130	255.255.255.224	192.168.72.129
		2001:db8:1:30::2/64		FE80::2
PC HR	Fa0	192.168.72.162	255.255.255.248	192.168.72.161
		2001:db8:1:40::2/64		FE80::2
PC Remote	Fa0	10.10.1.2	255.255.255.248	10.10.1.1
		2001:db8:1:200::2/64		FE80::4
Printer Sales	Fa0	192.168.72.3	255.255.255.192	192.168.72.1
		2001:db8:1:10::3/64		FE80::1

Printer PM	Fa0	192.168.72.67	255.255.255.192	192.168.72.65
		2001:db8:1:20::3/64		FE80::1
Printer Finance	Fa0	192.168.72.131	255.255.255.224	192.168.72.129
		2001:db8:1:30::3/64		FE80::2
Printer HR	Fa0	192.168.72.163	255.255.255.248	192.168.72.161
		2001:db8:1:40::3/64		FE80::2
Laptop Admin	Fa0	192.168.72.10	255.255.255.192	192.168.72.1
		2001:db8:1:10::10/64		FE80::1
Server Remote	Fa0	10.10.1.3	255.255.255.248	10.10.1.1
		2001:db8:1:200::3/64		FE80::4

Table 1 - Addressing Table for the topology

For the IPv6 address for routers, the unique link-local address was assigned for each router on each of their usable interfaces.

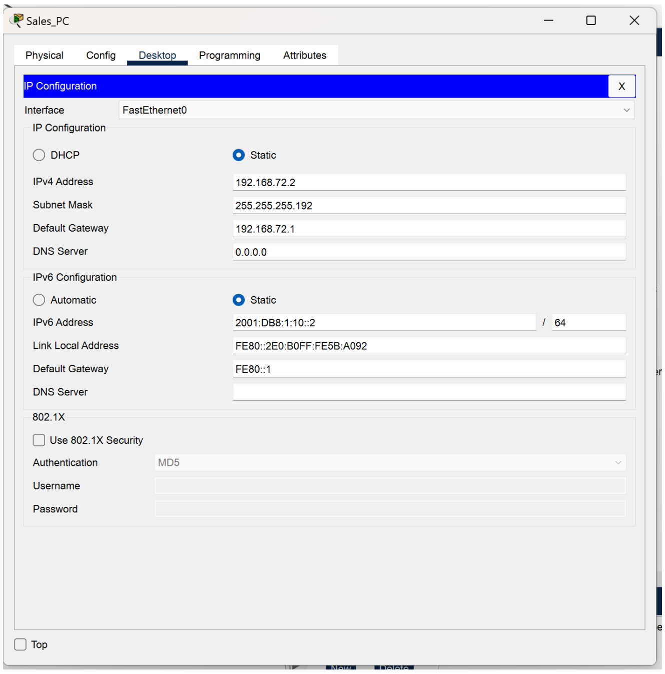
After assigning the IPs, the following topology was built in order to link all the devices. For simplicity purposes, only one device of each kind was implemented in order to represent each subnet. Different devices were connected with Copper Straight-Through cable, while similar devices shared the cross-over.



Picture 1 - Network Diagram

Configuration

Starting with PCs, laptop, printers and server, configuration was limited by changing their label and assigning both v4 and v6 IP addresses, including the default gateways and subnet mask/prefix.



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.72.2
Subnet Mask	255.255.255.192
Default Gateway	192.168.72.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	2001:DB8:1:10::2 / 64
Link Local Address	FE80::2E0:B0FF:FE5B:A092
Default Gateway	FE80::1
DNS Server	

802.1X

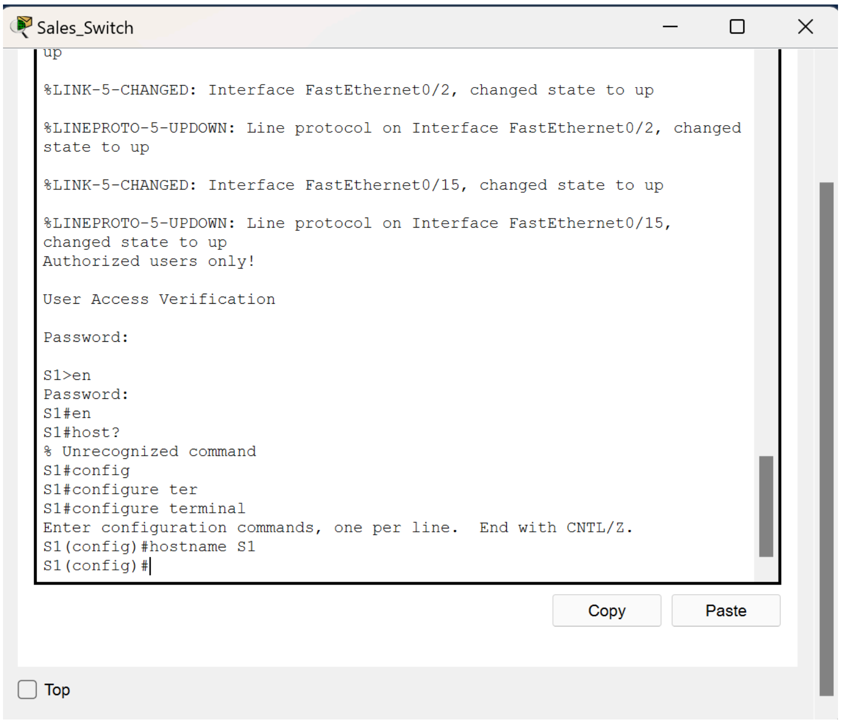
□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

Picture 2 - PC1 configuration example

Configuration process for switches and routers is almost identical. Firstly, after entering the privilege EXEC mode, go to terminal configuration mode and change the hostname to a proper identification.



```
up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15,
changed state to up
Authorized users only!

User Access Verification

Password:

S1>en
Password:
S1#en
S1#host?
% Unrecognized command
S1#config
S1#configure ter
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#hostname S1
S1(config)#
```

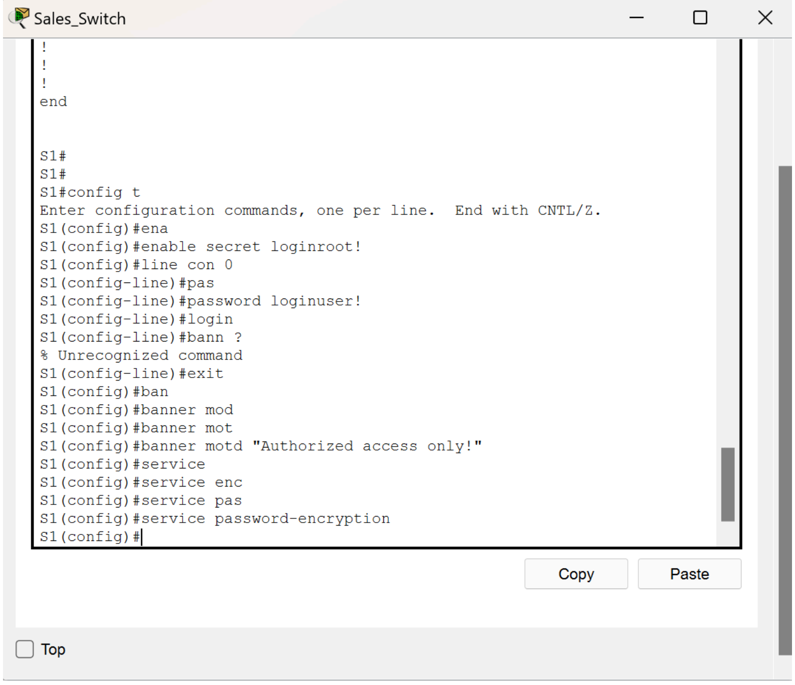
Picture 3 - hostname change

After that, the configuration of basic security takes place. For this purpose, the encrypted password for privilege EXEC mode, password for the console line and the welcoming banner with Message of the Day was implemented. Moreover, all the plaintext passwords were encrypted with corresponding service.

For all the devices, the credentials are:

Console line: **loginuser!**

Privilege EXEC mode: **loginroot!**



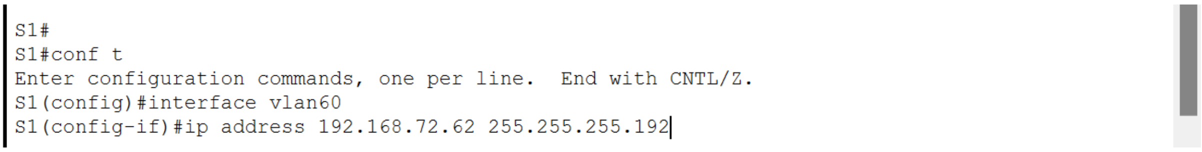
```
!
!
!
end


S1#
S1#
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ena
S1(config)#enable secret loginroot!
S1(config)#line con 0
S1(config-line)#pas
S1(config-line)#password loginuser!
S1(config-line)#login
S1(config-line)#bann ?
% Unrecognized command
S1(config-line)#exit
S1(config)#ban
S1(config)#banner mod
S1(config)#banner mot
S1(config)#banner motd "Authorized access only!"
S1(config)#service
S1(config)#service enc
S1(config)#service pas
S1(config)#service password-encryption
S1(config)#
```

Picture 4 - basic security implementation

Next, the IPs should be assigned. The process is almost the same for routers and switches, the only difference is the interfaces that should have an IP. For switches, only a virtual interface VLAN should have an IP in order to be available for remote access and configuration. However, the router should have all usable interfaces assigned with an ip, each one corresponding to the subnets it connects to. Additionally, in order to use both IPv4 and IPv6, the dual mode on switches should be activated and the device should be reloaded afterwards:

```
sdm prefer dual-ipv4-and-ipv6 default

reload
```

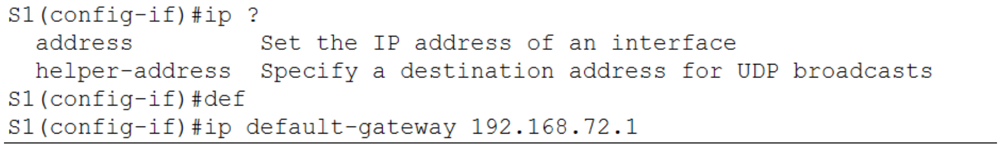
The IPv4 configuration looks like this.



```
S1#
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface vlan60
S1(config-if)#ip address 192.168.72.62 255.255.255.192
```

Picture 5 - IPv4 assignment

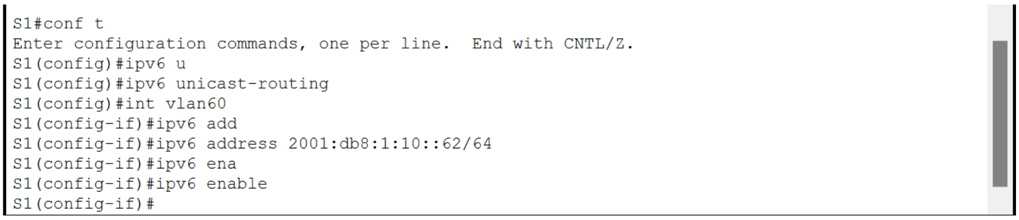
The “**no shutdown**” command is used to enable the interface and make it work. For switch, the default gateway should also be specified.



```
S1(config-if)#ip ?
  address         Set the IP address of an interface
  helper-address  Specify a destination address for UDP broadcasts
S1(config-if)#def
S1(config-if)#ip default-gateway 192.168.72.1
```

Picture 6 - default gateway assignment

The IPv6 is configured in a similar way.

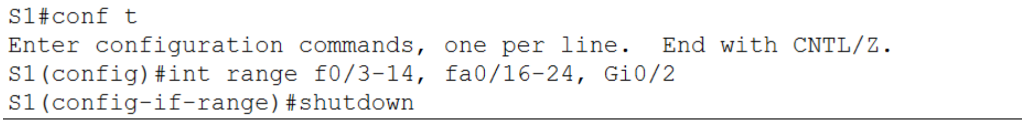


```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ipv6 u
S1(config)#ipv6 unicast-routing
S1(config)#int vlan60
S1(config-if)#ipv6 add
S1(config-if)#ipv6 address 2001:db8:1:10::62/64
S1(config-if)#ipv6 ena
S1(config-if)#ipv6 enable
S1(config-if)#
```

Picture 7 - IPv6 configuration

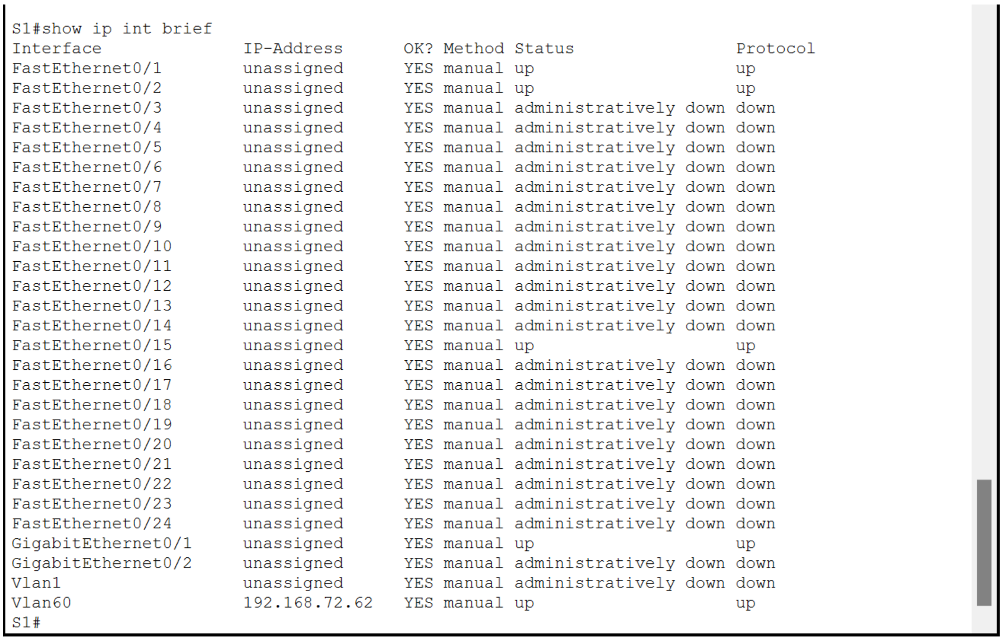
For the routers it is a good practice to also specify the link local address by “**ipv6 address FE80::1 link-local**” command.

After the IP addresses are assigned, for security purposes all unused interfaces should be shutted down.



```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range f0/3-14, fa0/16-24, Gi0/2
S1(config-if-range)#shutdown
```

Picture 8 - interfaces shutdown



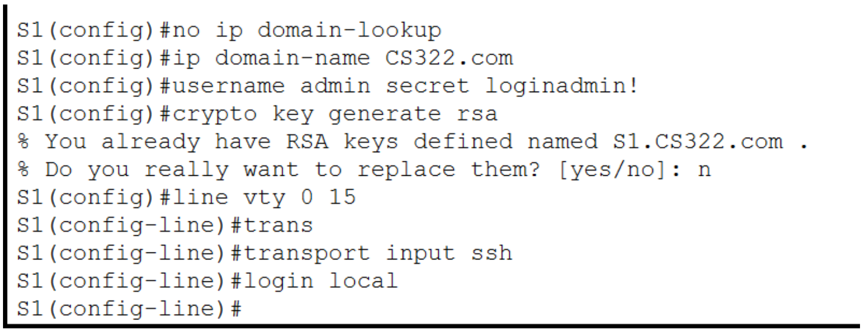
```
S1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual up                    up
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
Vlan60                 192.168.72.62   YES manual up                    up
S1#
```

Picture 9 - interfaces status at switch

SSH Configuration

In order to be able to connect to the device remotely and securely, the ssh connection should be established. To do so, the dns domain name should be assigned, the admin (or any other) user should be created with an encrypted password assigned, the rsa crypto key should be generated, and also the virtual lines should be turned into ssh mode for incoming requests.

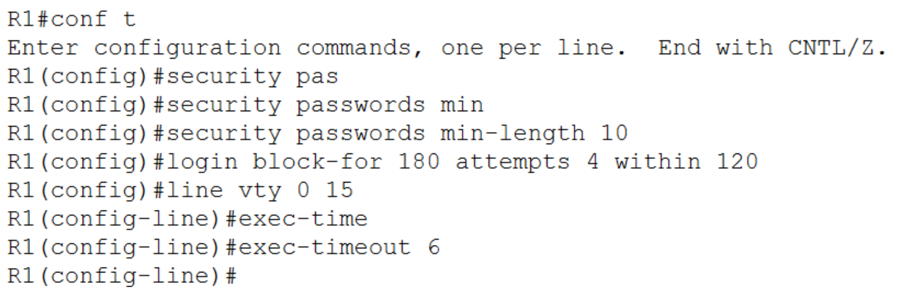
The admin password is: **loginadmin!**



```
S1(config)#no ip domain-lookup
S1(config)#ip domain-name CS322.com
S1(config)#username admin secret loginadmin!
S1(config)#crypto key generate rsa
% You already have RSA keys defined named S1.CS322.com .
% Do you really want to replace them? [yes/no]: n
S1(config)#line vty 0 15
S1(config-line)#trans
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#
```

Picture 10 - ssh configuration

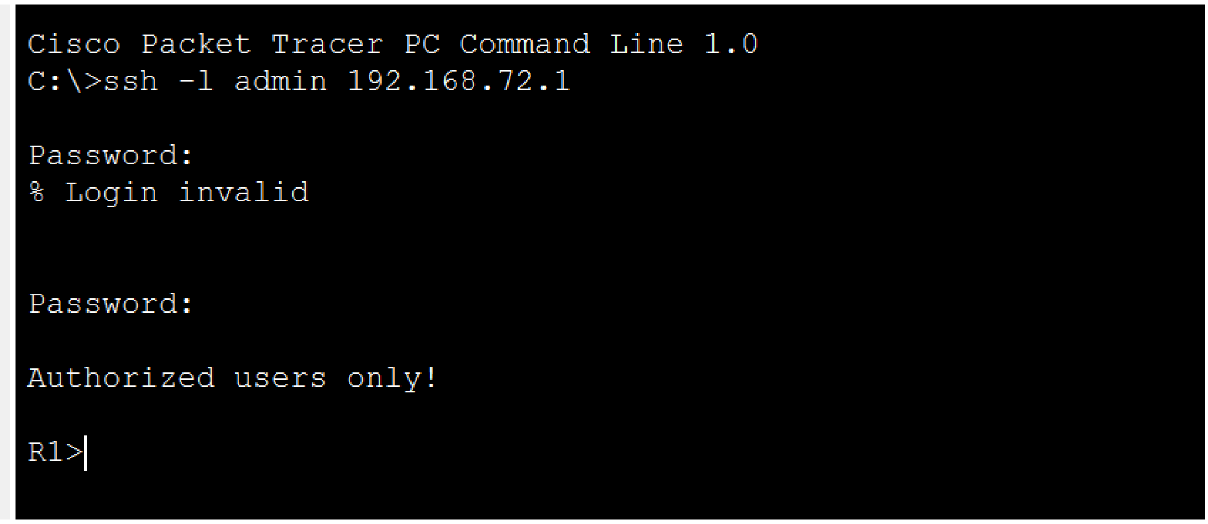
For additional security, the minimal length for passwords, blocking after unsuccessful connection attempts, and execution timeout can be enabled on routers.



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#security pas
R1(config)#security passwords min
R1(config)#security passwords min-length 10
R1(config)#login block-for 180 attempts 4 within 120
R1(config)#line vty 0 15
R1(config-line)#exec-time
R1(config-line)#exec-timeout 6
R1(config-line)#
```

Picture 11 - additional security

Now, users can access the router or switch remotely using the ssh connection and logging in as admin.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.72.1

Password:
% Login invalid


Password:

Authorized users only!

R1>
```

Picture 12 - ssh connection test

VLAN Configuration

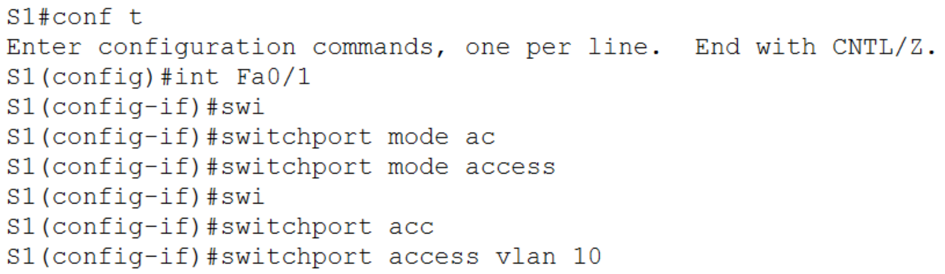
In order to properly segregate the network, different VLANs were assigned to different departments.

1) Sales: 10
2) Product Management: 20
3) Finance: 30

4) HR: 40

Plus, VLAN 60 is for Management and VLAN 99 is Native.

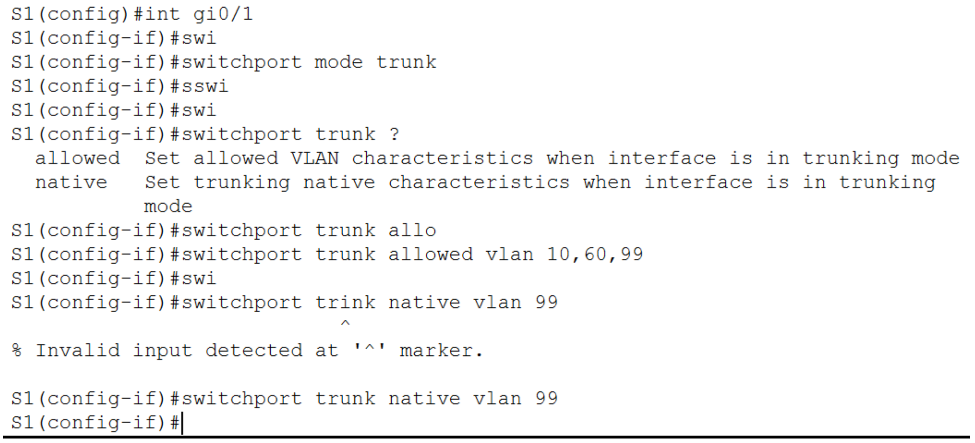
In order to configure the VLANs, first they were created using the ″**vlan 10**″ command and renamed using the ″**name Sales**″ command. Afterwards, each interface on switch was assigned either to access or trunk mode. Each interface looking to the endpoint device was changed to access mode and assigned with a vlan.



```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int Fa0/1
S1(config-if)#swi
S1(config-if)#switchport mode ac
S1(config-if)#switchport mode access
S1(config-if)#swi
S1(config-if)#switchport acc
S1(config-if)#switchport access vlan 10
```

Picture 13 - vlan assignment

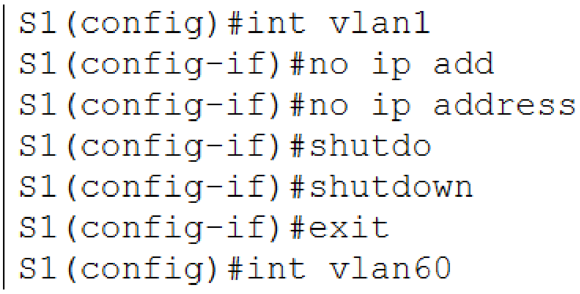
For an interface looking at the router, the trunk mode was activated, allowing only existing vlans and setting 99 vlan as native for all untagged packages.



```
S1(config)#int gi0/1
S1(config-if)#swi
S1(config-if)#switchport mode trunk
S1(config-if)#sswi
S1(config-if)#swi
S1(config-if)#switchport trunk ?
  allowed  Set allowed VLAN characteristics when interface is in trunking mode
  native   Set trunking native characteristics when interface is in trunking
           mode
S1(config-if)#switchport trunk allo
S1(config-if)#switchport trunk allowed vlan 10,60,99
S1(config-if)#swi
S1(config-if)#switchport trink native vlan 99
                           ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport trunk native vlan 99
S1(config-if)#
```

Picture 14 - trunk mode

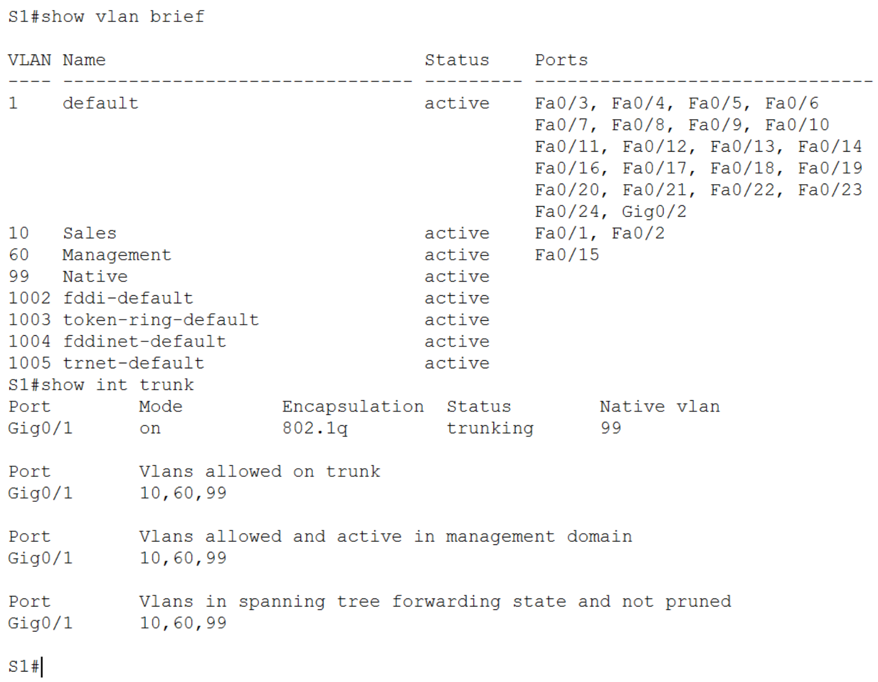
Finally, to make the switch only available by management vlan users, a new virtual interface VLAN60 was created and the IP of the switch was assigned to it. Moreover, as a showcase, the laptop is connected on Fa0/15 and has vlan 60 assigned to it so be able to ping and remotely connect to the switch.



```
S1(config)#int vlan1
S1(config-if)#no ip add
S1(config-if)#no ip address
S1(config-if)#shutdo
S1(config-if)#shutdown
S1(config-if)#exit
S1(config)#int vlan60
```

Picture 15 - creation of virtual interface

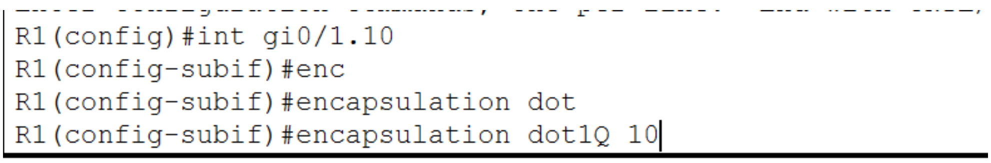
The result of switch vlan configuration is the following:



```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
10   Sales                            active    Fa0/1, Fa0/2
60   Management                       active    Fa0/15
99   Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/1      10,60,99

Port        Vlans allowed and active in management domain
Gig0/1      10,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,60,99

S1#
```

Picture 16 - switch vlan configuration

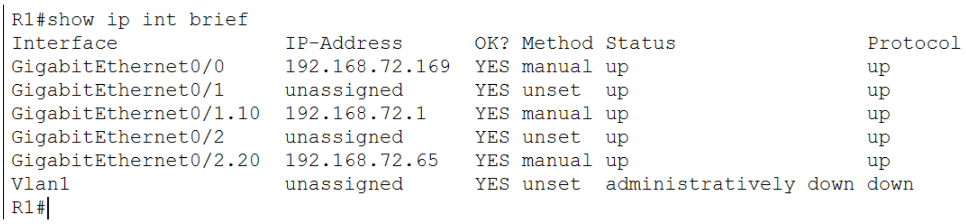
Talking about the router, the encapsulation should be added in order to perform the inter-vlan routing. To do so, firstly create the sub interface by **"int Gi0/1.10"** command. The encapsulation for specific vlan id should be enabled. After that, it should be assigned with an IP address as was explained before.



```
R1(config)#int gi0/1.10
R1(config-subif)#enc
R1(config-subif)#encapsulation dot
R1(config-subif)#encapsulation dot1Q 10
```

Picture 17 - router encapsulation

The result of router configuration is following:

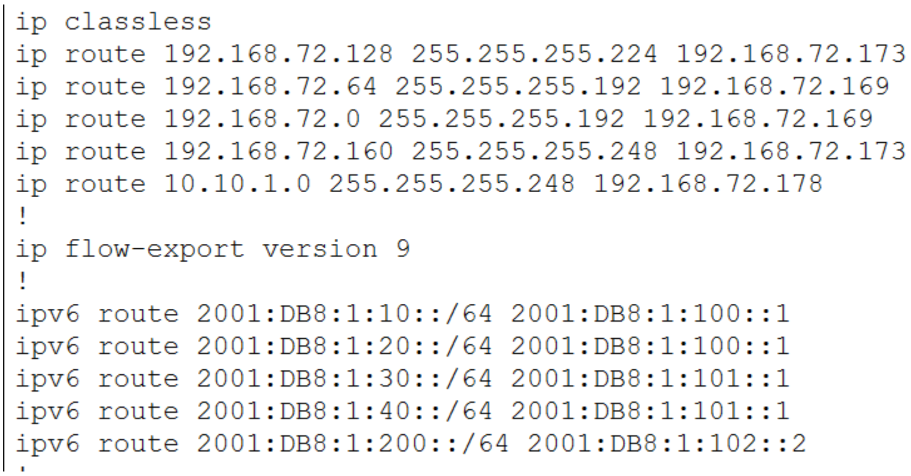


```
R1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.72.169  YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/1.10  192.168.72.1    YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/2.20  192.168.72.65   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

Picture 18 - router interfaces assignment

IP Routing

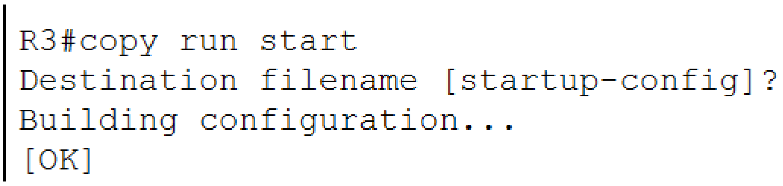
Since each router pair has its own subnet to communicate, each router is unaware of the subnet topology beyond their connections. In order to allow routers to translate the packages from and to the subnets they do not know about, the static routes should be assigned to correct mapping. The simple command allows to specify the name of the subnet and the corresponding IP for the package to be sent to on the next step. Static routes should be implemented for each router to inform them about the subnets that are out its range. For instance, the main router needs to know about all subnets for 4 divisions as well as about the remote network subnet. Moreover, since topology works in dual mode, the same procedure should take place for IPv6 routing.



```
ip classless
ip route 192.168.72.128 255.255.255.224 192.168.72.173
ip route 192.168.72.64 255.255.255.192 192.168.72.169
ip route 192.168.72.0 255.255.255.192 192.168.72.169
ip route 192.168.72.160 255.255.255.248 192.168.72.173
ip route 10.10.1.0 255.255.255.248 192.168.72.178
!
ip flow-export version 9
!
ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:100::1
ipv6 route 2001:DB8:1:20::/64 2001:DB8:1:100::1
ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:101::1
ipv6 route 2001:DB8:1:40::/64 2001:DB8:1:101::1
ipv6 route 2001:DB8:1:200::/64 2001:DB8:1:102::2
```

Picture 19 - IPv4 and IPv6 static routes for main router

After all the configurations, the configuration file should be saved into the startup configuration file in order to be available after the device reload.



```
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Picture 20 - startup configuration saving

Conclusion

As a result, the created network allows to create multiple departments with different amounts of hosts supported, each of those will be isolated on both 2 and 3 levels by subnetting and VLANs. Additionally, it operates in dual mode allowing it to use both IPv4 and IPv6 topologies. As the process of initial configuration is almost identical across all switches and routers, an intermediate configuration file was copied and migrated across the devices. Enabled SSH allows connections to switches and routers remotely with secured connection.

Built topology is scalable and gives the opportunity to expand the network with addition of new subnets, hosts or remote networks.

Credentials for all the devices:

Console line: **loginuser!**

Privilege EXEC mode: **loginroot!**

Admin password for SSH: **loginadmin!**