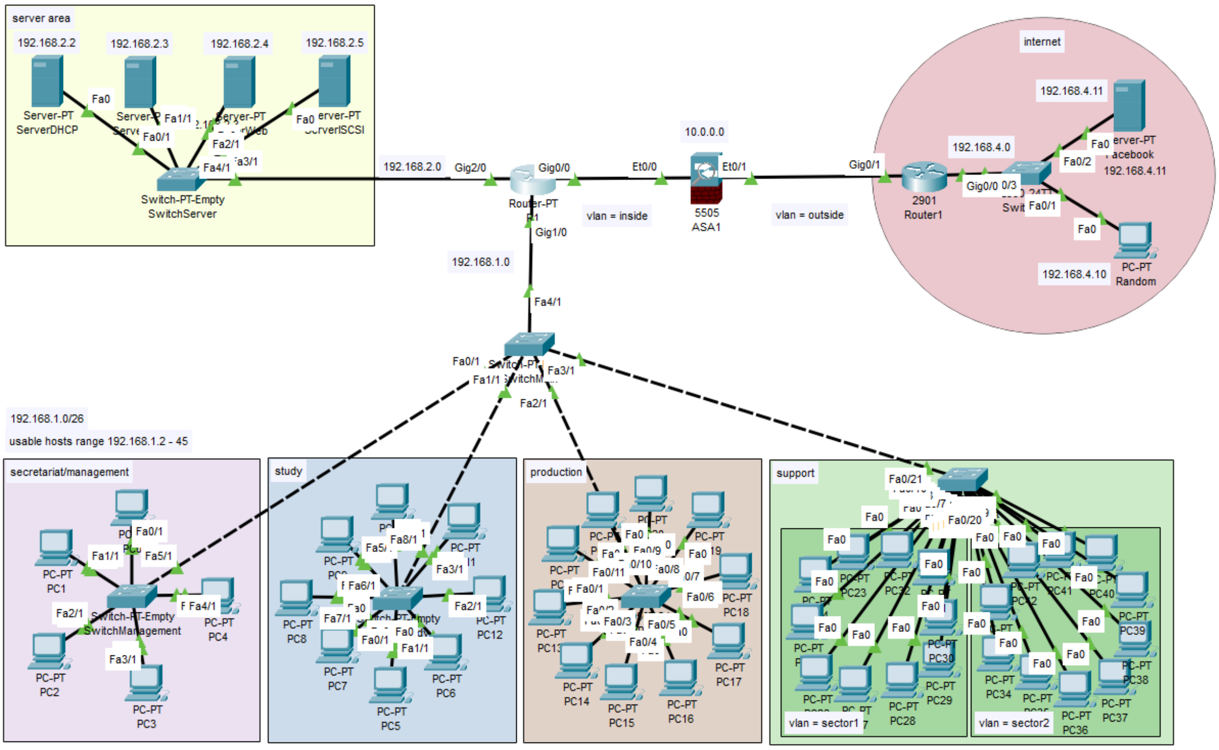


Network Infrastructure Overview

Executive Summary

This document provides an overview of the network infrastructure implemented within the context of the Becode network group project. The network is designed to allow 43 hosts to communicate with one another, exchange data, and connect themselves to the internet while being protected via multiple defense systems. Key highlights of the network infrastructure include:

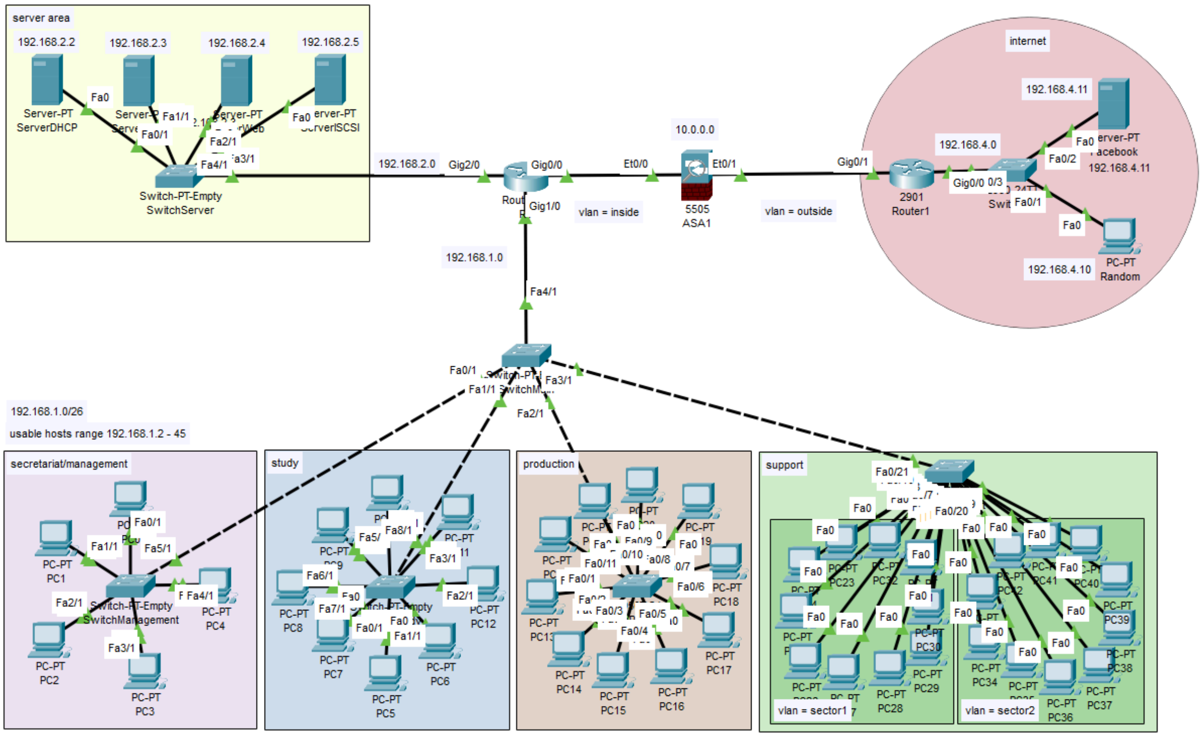
- **Topology**: The network follows the star topology structure, where key routers and switches at the center of the network ensure connectivity for all of the hosts and servers. It allows great stability and scalability while being easy to maintain.
- **Hosts and Connectivity**: All hosts are part of a subnet that has been divided in 5 Vlans. It ensures the hosts won't broadcast their info to the entire network every time, which increases the network's speed and reliability. All these hosts are linked to switches, which are then all linked to a master switch and router.
- **Security Measures**: Vlans ensure all sub-networks are separated from one another. Since only accepted Vlans are enabled on the master switch

interface, it ensures our networks won’t allow unauthorized hosts in the system. Moreover, the hosts and the servers are all protected from the outside internet via an ASA firewall and Access Control Lists (ACL) that ensure our network won’t get reached by unwanted outside communications.

- **Monitoring and Maintenance**: Regular monitoring and maintenance procedures have to be made on the core area containing the main switch, routers and firewall as the entire system relies on them. It seems non-secure, but it seems to us it is easier to maintain a few interfaces than too many as we can concentrate on a small number of critical points.
- **Future Considerations**: Thanks to our topology, future hosts, subnets or servers can be accommodated easily via the creation of new subnets on the actually unused ports of the central routers. Should the router be under too much stress, new layer 3 interfaces can be easily added as well.

Network Architecture

Diagram



Topology

The network architecture follows a star topology comprising the following layers:

- **Core Layer**: On the internal side, this layer consists of one Cisco PT routers linked to two 2960 switches that handle the server and the workstations areas. On the outside side, it contains one ASA firewall that filters the communications between our outside router and the core one.
- **Distribution Layer**: To ensure proper segmentation and distribution of packets, each segment of the network is handled by its own Vlan. All of them are contained in a single subnet.
- **Access Layer**: On the workstation side, this layer contains 4 switches, each of them being connected to one part of the subnet. Each of these manages one Vlan, two in the case of the support area. As for the server area, there is one switch to coordinate all incoming and outgoing traffic.

IP addressing table

Here below are our network's hosts' IP table and their corresponding Vlans :

- **Servers**: 192.168.2.2 up to 192.168.2.5

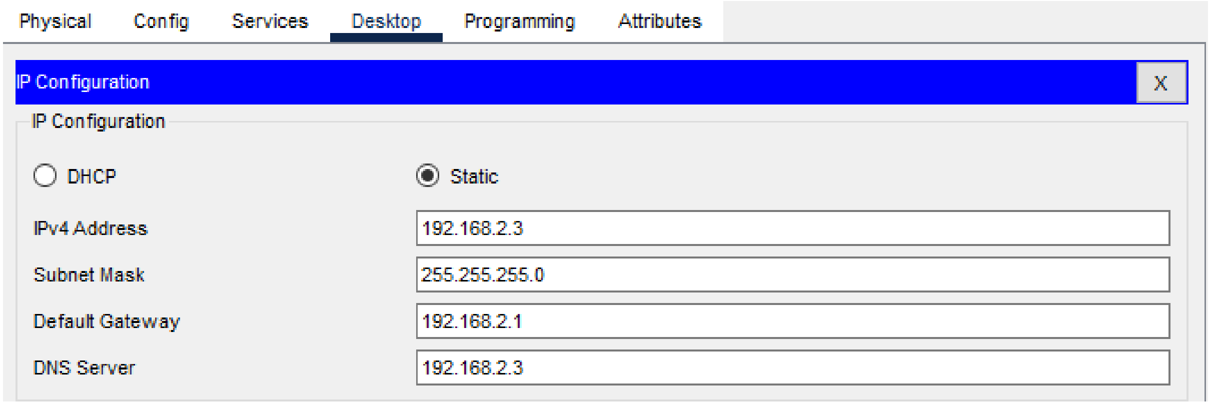
- **Workstations**:
  - Management : 192.168.1.10 up to 192.168.1.14 | VLAN 10
  - Study : 192.168.1.15 up to 192.168.1.22 | VLAN 20
  - Production : 192.168.1.23 up to 192.168.1.32 | VLAN 30
  - Support 1 : 192.168.1.33 up to 192.168.1.42 | VLAN 40
  - Support 2 : 192.168.1.43 up to 192.168.1.52 | VLAN 50
- **Core Devices**:
  - Router facing workstations : 192.168.1.1
  - Router facing servers : 192.168.2.1
  - Router facing firewall : 10.0.0.1

Key devices' configuration

- **Servers**:

  DNS :

1) Create a server device for DNS, in our case in 192.168.2.0 network with ip 192.168.2.3, default gateway 192.168.2.1 and DNS server 192.168.2.3.



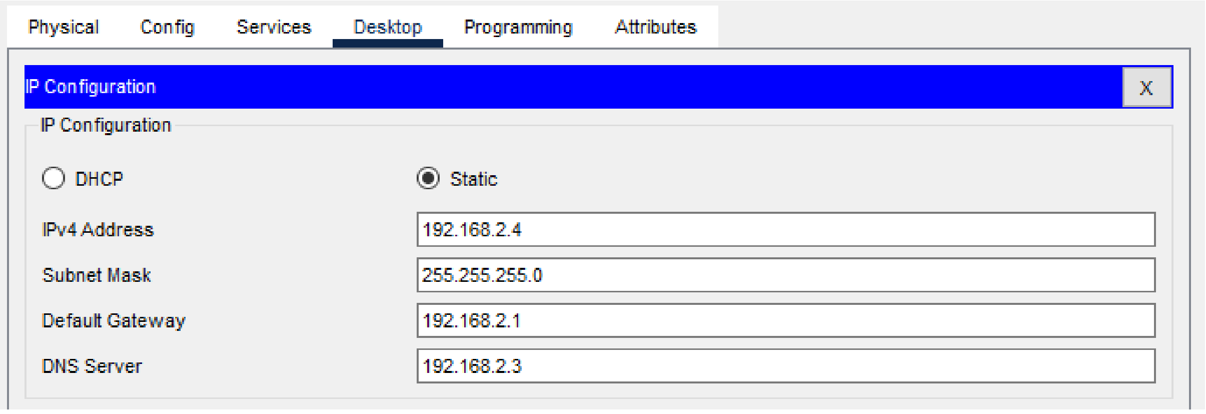
IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.2.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	192.168.2.3

2) Create server web for hosting, in our case in 192.168.2.0 network with ip 192.168.2.4, default gateway 192.168.2.1 and DNS server 192.168.2.3.



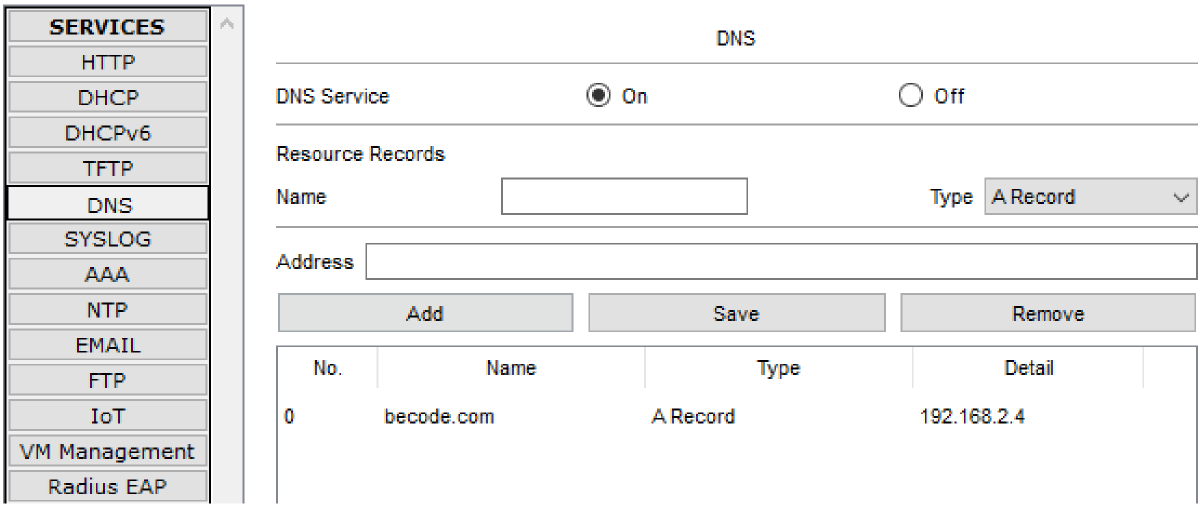
IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.2.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	192.168.2.3

3) Go to services tab from DNS server and enable DNS service with a name and address, in our case becode.com on ip 192.168.2.4 (IP matching webServer IP)



DNS

DNS Service ● On ○ Off

Resource Records

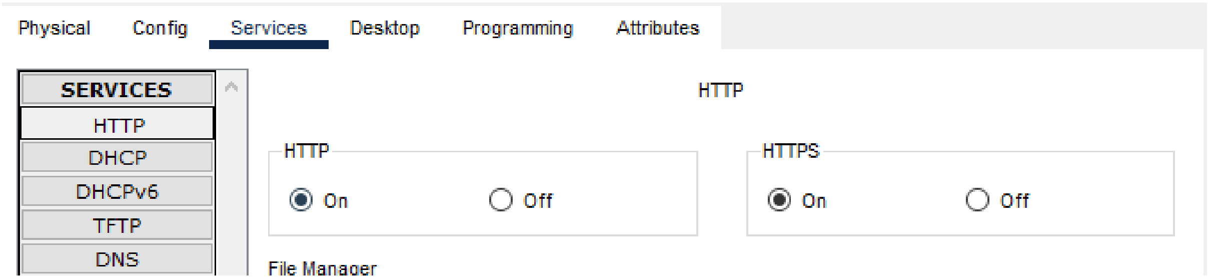
Name

Type A Record

Address

No.	Name	Type	Detail
0	becode.com	A Record	192.168.2.4

4) Turn Service HTTP/HTTPS on

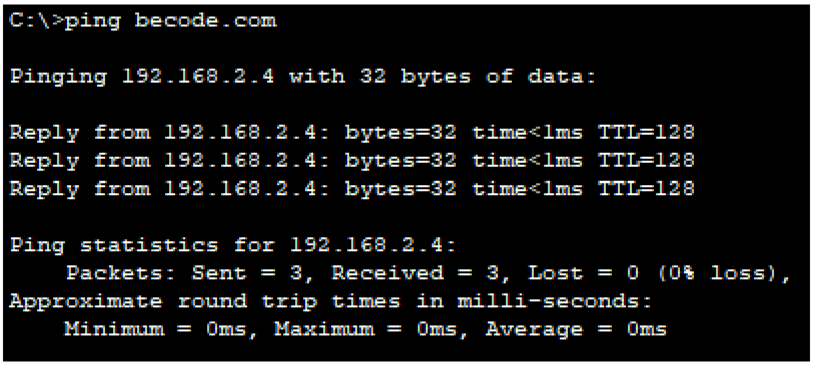


HTTP

HTTP ● On ○ Off

HTTPS ● On ○ Off

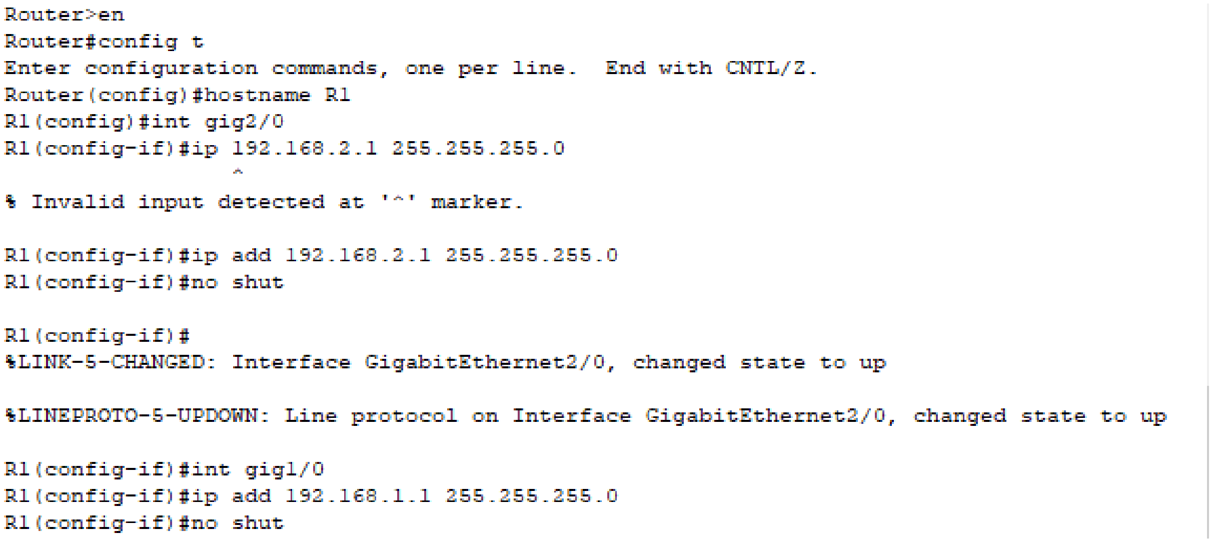
5) Hosts on 192.168.2.0 are now able to visit becode.com



```
C:\>ping becode.com

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

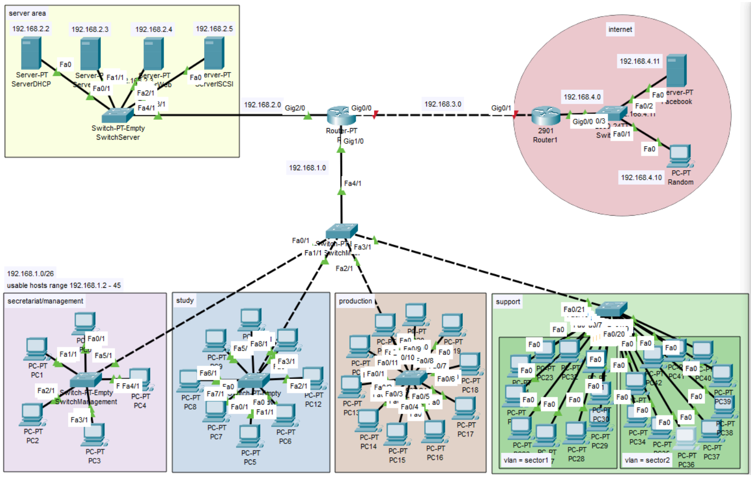
Ahahahahah, je vois qu’on est 2 à a

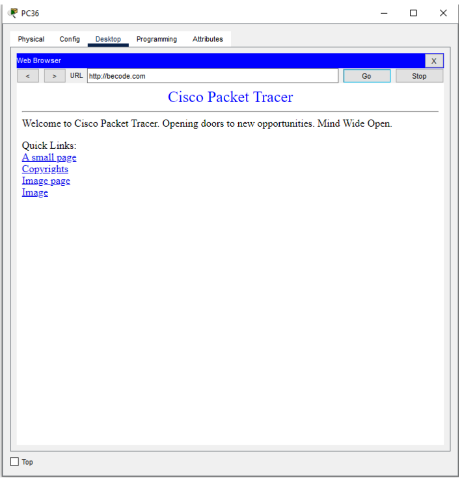
6) Config the main router to allow hosts from 192.168.1.0/26 access to the DNS server.



```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int gig2/0
R1(config-if)#ip 192.168.2.1 255.255.255.0
                 ^
% Invalid input detected at '^' marker.

R1(config-if)#ip add 192.168.2.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up

R1(config-if)#int gig1/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

7) Hosts on 192.168.1.0/26 have access now.





http://becode.com

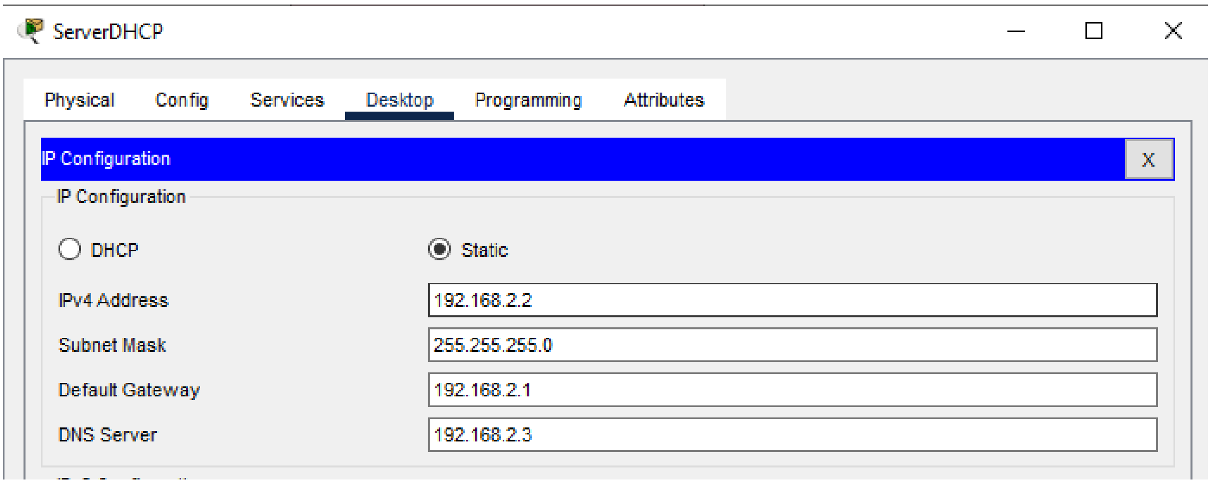
Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

DHCP :

1) Go to config from DHCP server and set IP + default gateway, in our case 192.168.2.2 and 192.168.2.1



IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.2

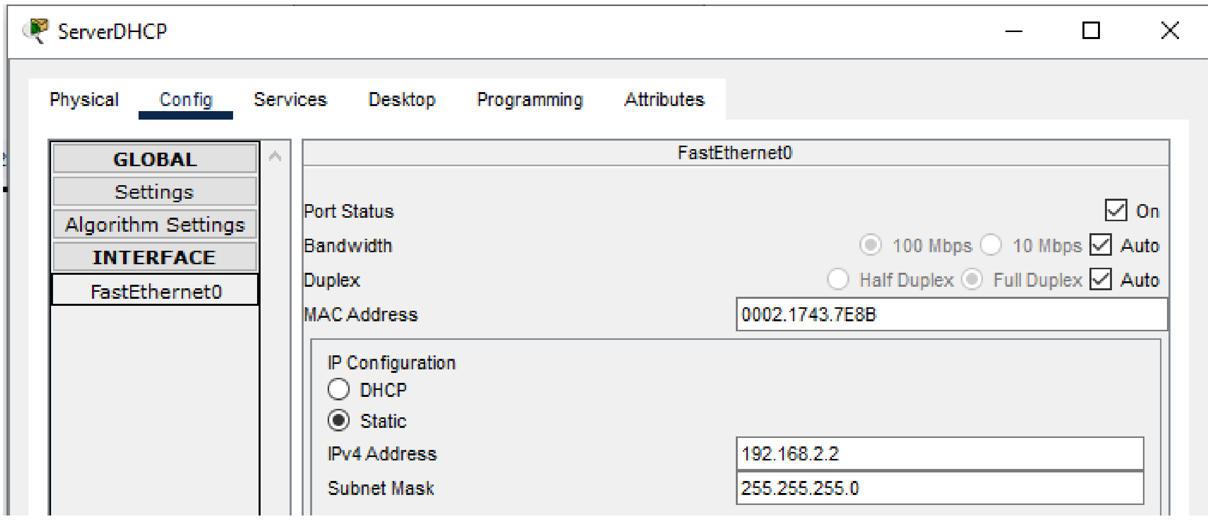
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 192.168.2.3

2) If you're using DNS server, set the IP DNS Server, in our case 192.168.2.3

3) Select the interface of DHCP server and set his own ip inside the network, in our case network 192.168.2.0 so we'll use 192.168.2.3



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 0002.1743.7E8B

IP Configuration

○ DHCP

● Static

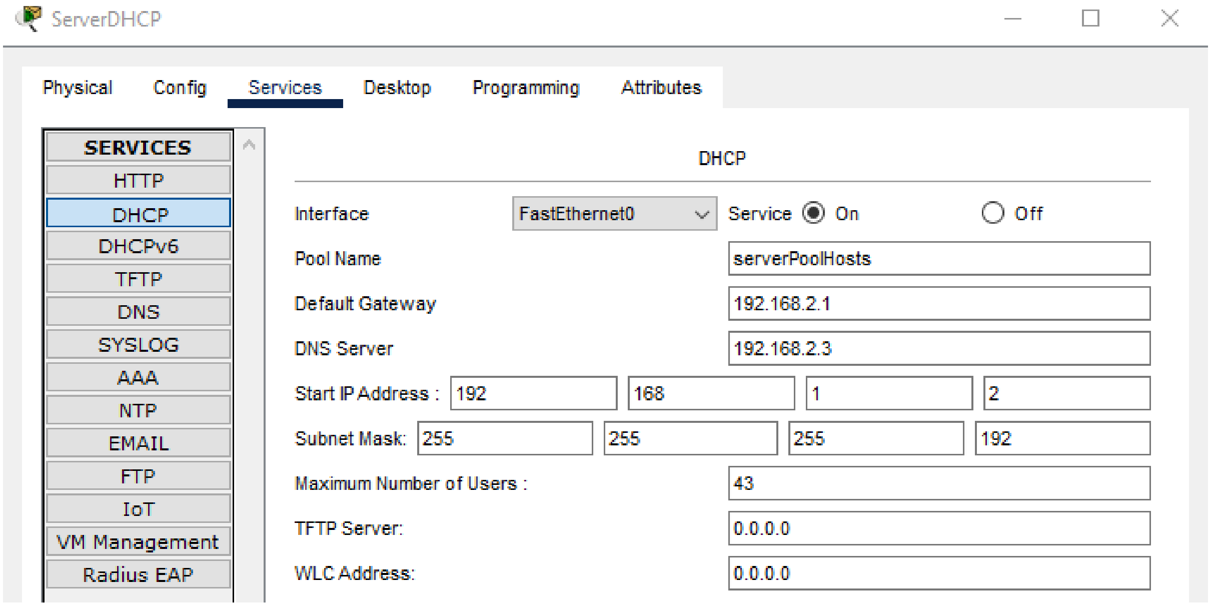
IPv4 Address: 192.168.2.2

Subnet Mask: 255.255.255.0

4) In the Services tab, for DHCP, set Default Gateway and DNS server. Then add your start IP address for DHCP and subnet mask. In our case, we want our host to be in 192.168.1.0 network with 43 hosts maximum, so in our case we'll start our ip at 192.168.1.2 with a subnet mask of 255.255.255.192, which means 62 usable hosts.

5) Still in the DHCP server tab, go to config and select DHCP. Set up default gateway and DNS with the same IP previously used. In our case, gateway 192.168.2.1 and DNS 192.168.2.2

6) Set the maximum number of users at 43 as it's the number of hosts our network will have. It prevents malicious people from using our unused IP.



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name serverPoolHosts

Default Gateway 192.168.2.1

DNS Server 192.168.2.3

Start IP Address : 192 168 1 2

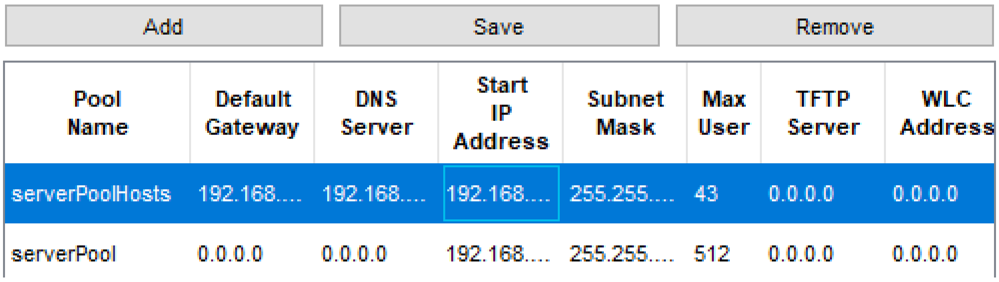
Subnet Mask: 255 255 255 192

Maximum Number of Users : 43

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

7) Click on Add.

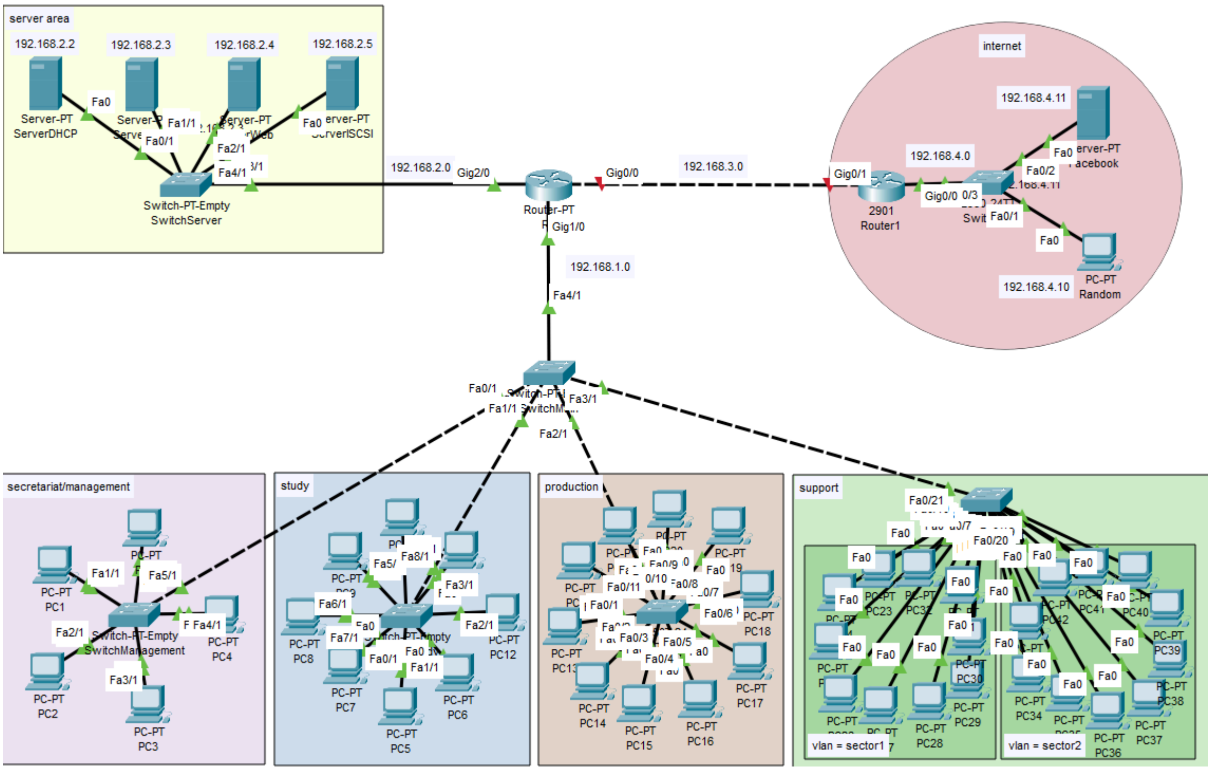


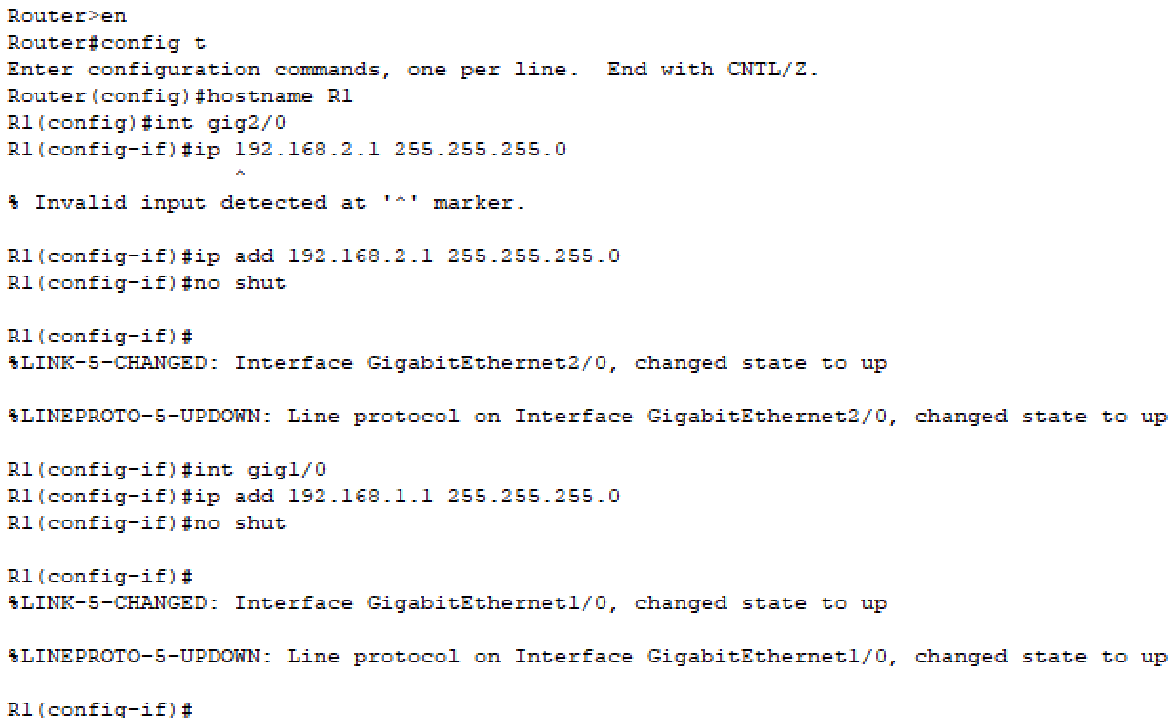
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPoolHosts	192.168....	192.168....	192.168....	255.255....	43	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168....	255.255....	512	0.0.0.0	0.0.0.0

8) Now each PC on the network of area servers (192.168.2.0) is able to use DHCP.

9) Our hosts are on different network, 192.168.1.0, we need to allow DHCP for this network

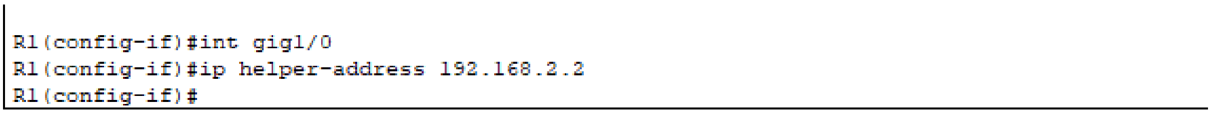
10)Go to the CLI of your router, in our case R1, and set up interfaces IP





```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int gig2/0
R1(config-if)#ip 192.168.2.1 255.255.255.0
                  ^
% Invalid input detected at '^' marker.

R1(config-if)#ip add 192.168.2.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up

R1(config-if)#int gig1/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up

R1(config-if)#
```

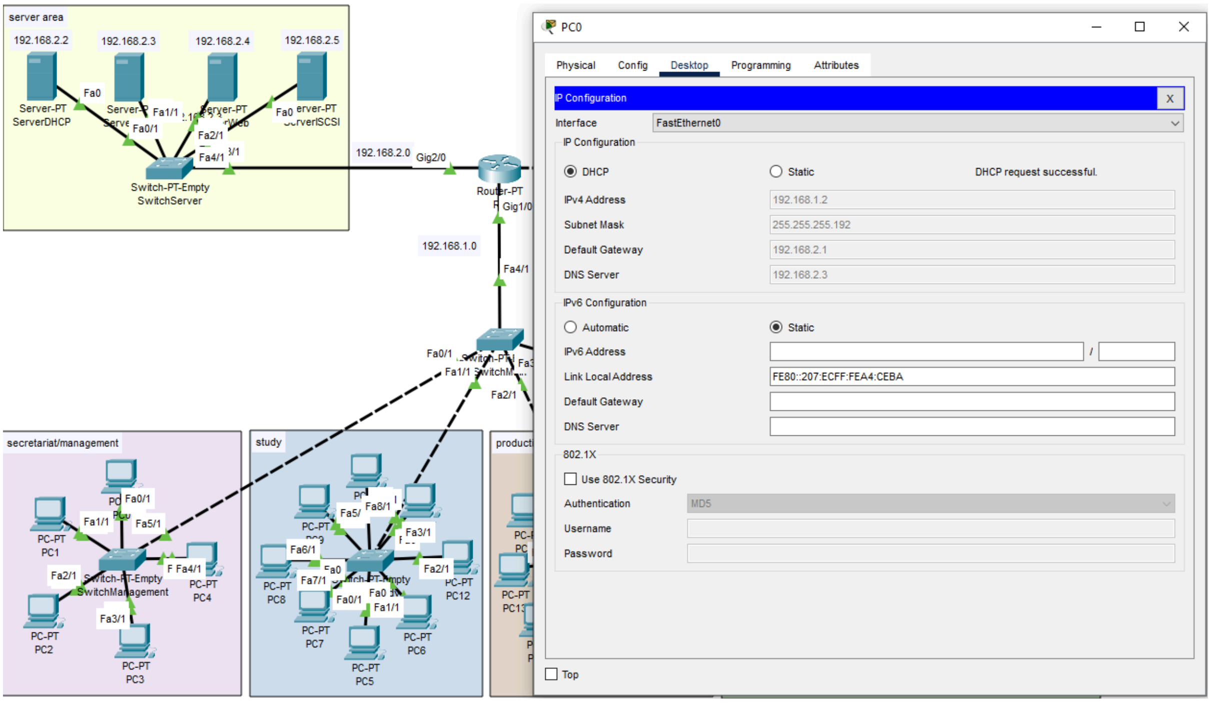
11) Still in R1 CLI, set up an address helper so the network 192.168.1.0 can access the DHCP server.



```
R1(config-if)#int gig1/0
R1(config-if)#ip helper-address 192.168.2.2
R1(config-if)#
```

12) Now our hosts outside the network of our DHCP server can have their IP assigned

through DHCP



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.192

Default Gateway: 192.168.2.1

DNS Server: 192.168.2.3

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::207:ECFF:FEA4:CEBA

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

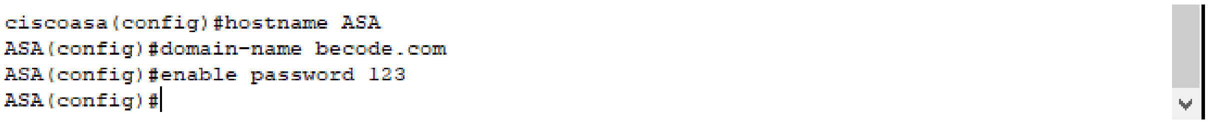
□ Top

Security Measures

To ensure the security of the network, the following measures are implemented:

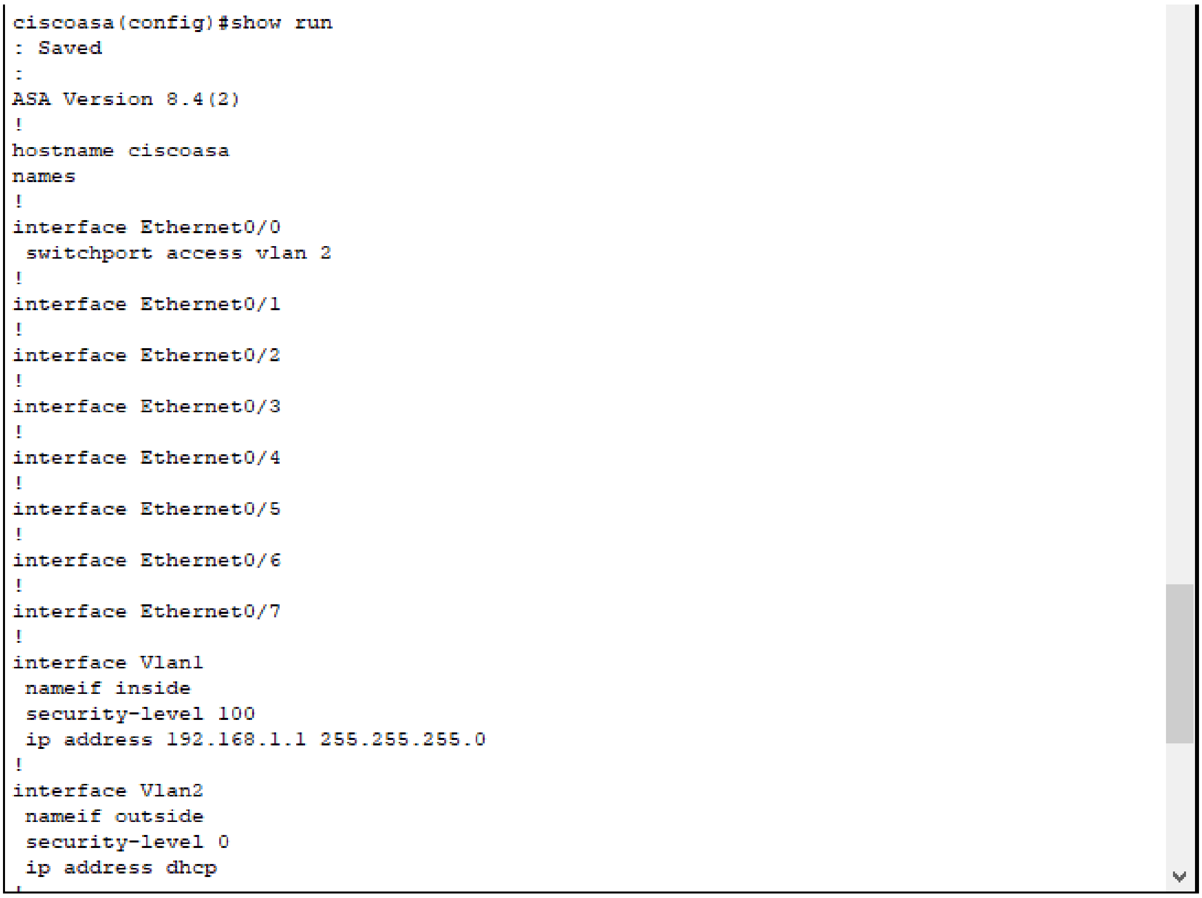
- **Firewalls :**

  1) Create your hostname



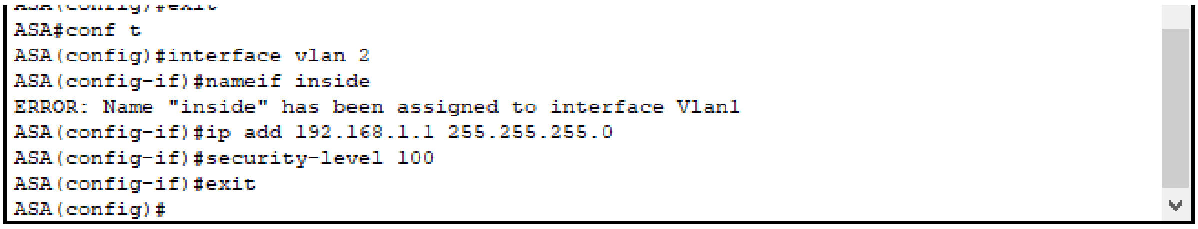
```
ciscoasa(config)#hostname ASA
ASA(config)#domain-name becode.com
ASA(config)#enable password 123
ASA(config)#
```

- 2) Check your vlan with : show run



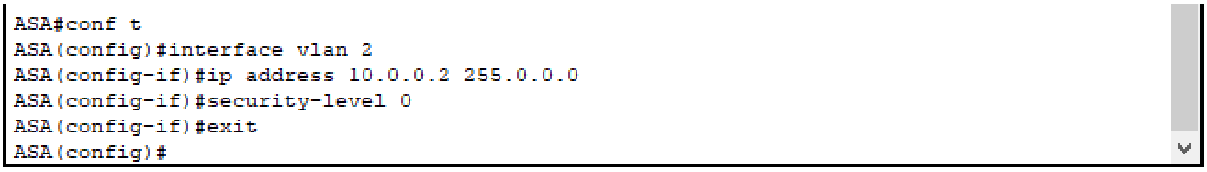
```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
```

- 3) You can rename your vlan, usually vlan1 is your network and vlan2 outside your network. In our case vlan2 was our network so we'll rename it to " inside " with a security level of 100. Meaning this vlan can access outside his network (internet) without restriction.



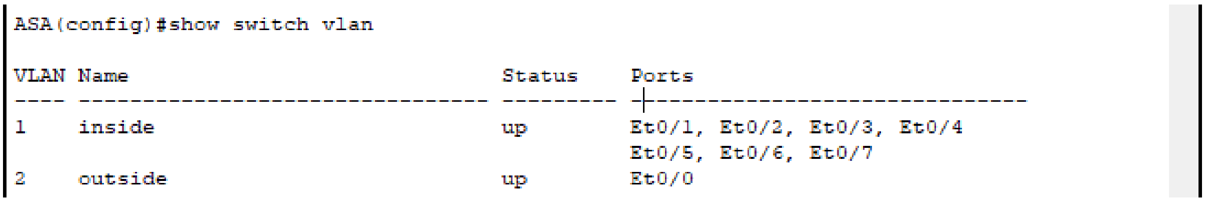
```
ASA(config)#exit
ASA#conf t
ASA(config)#interface vlan 2
ASA(config-if)#nameif inside
ERROR: Name "inside" has been assigned to interface Vlan1
ASA(config-if)#ip add 192.168.1.1 255.255.255.0
ASA(config-if)#security-level 100
ASA(config-if)#exit
ASA(config)#
```

4) Do the same for outside vlan with a security-level 0.



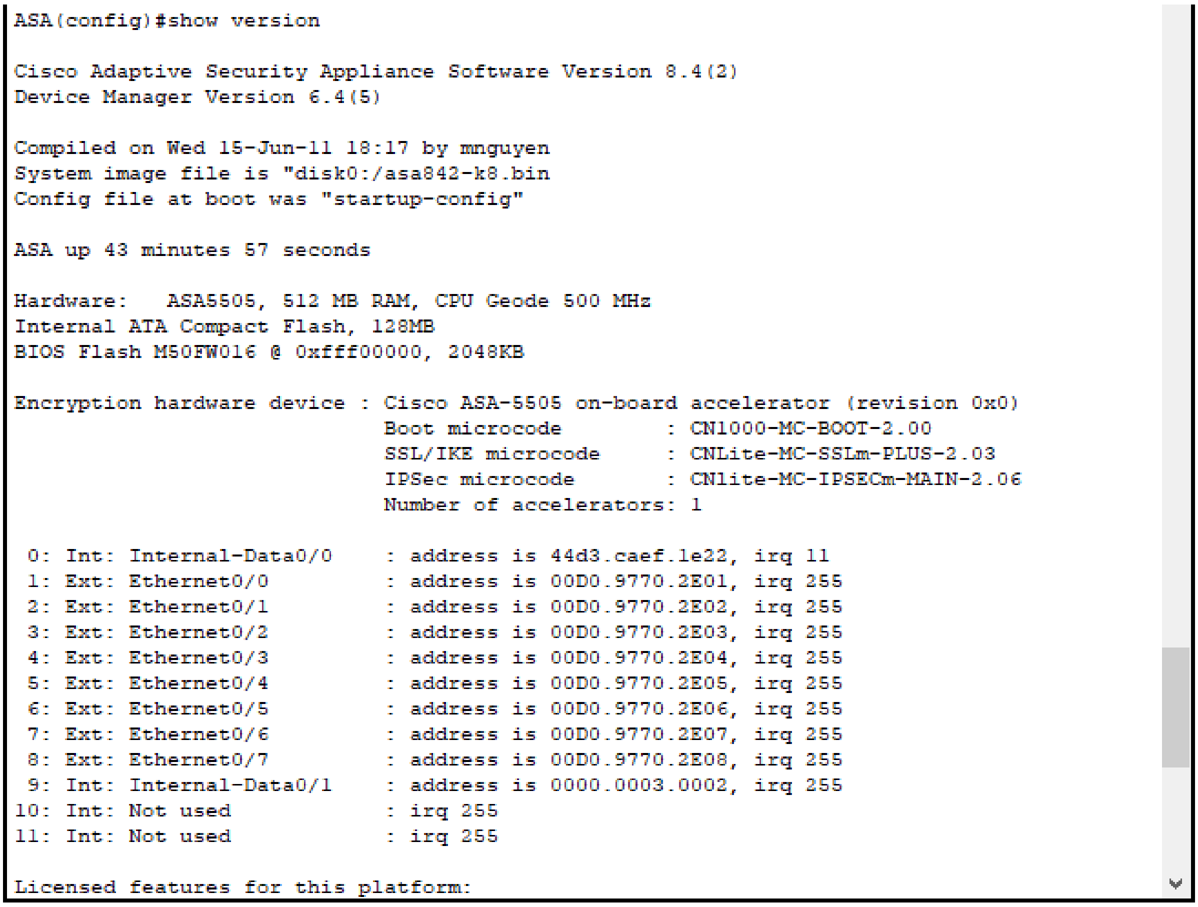
```
ASA#conf t
ASA(config)#interface vlan 2
ASA(config-if)#ip address 10.0.0.2 255.0.0.0
ASA(config-if)#security-level 0
ASA(config-if)#exit
ASA(config)#
```

- 5) To see vlan switch port : show switch vlan



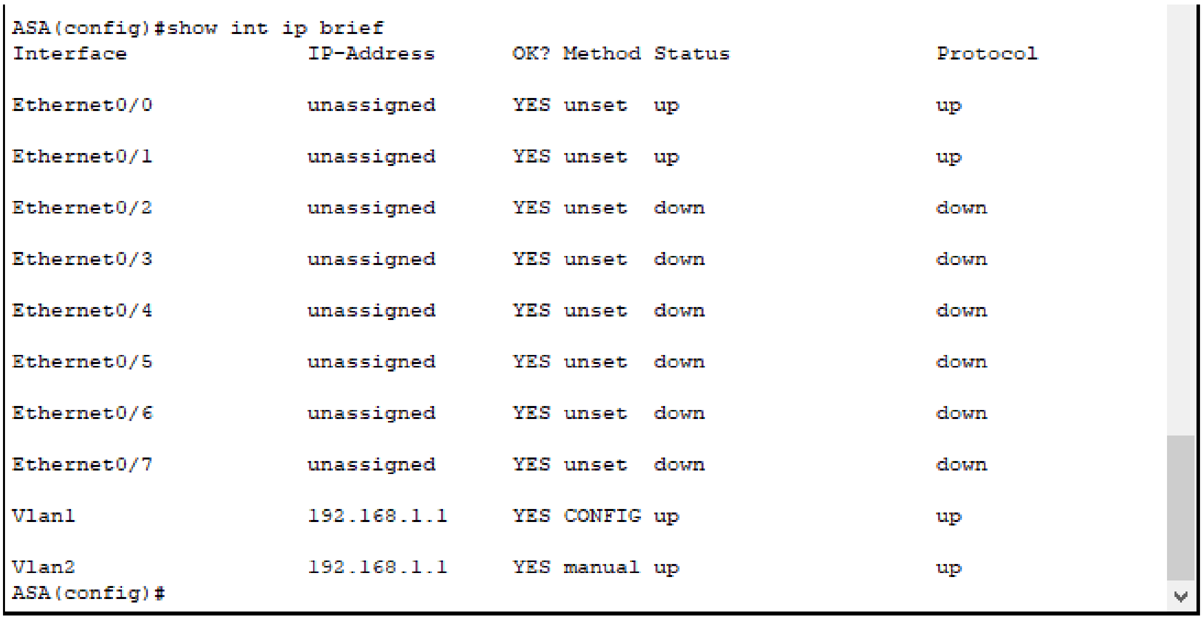
```
ASA(config)#show switch vlan

VLAN Name                             Status     Ports
---- -------------------------------- ---------- ------------------------------
1    inside                           up         Et0/1, Et0/2, Et0/3, Et0/4
                                                 Et0/5, Et0/6, Et0/7
2    outside                          up         Et0/0
```

- 6) Too see overall information : show version



```
ASA(config)#show version

Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Wed 15-Jun-11 18:17 by mnguyen
System image file is "disk0:/asa842-k8.bin
Config file at boot was "startup-config"

ASA up 43 minutes 57 seconds

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode        : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode     : CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode       : CNlite-MC-IPSECm-MAIN-2.06
                             Number of accelerators: 1

 0: Int: Internal-Data0/0    : address is 44d3.caef.1e22, irq 11
 1: Ext: Ethernet0/0         : address is 00D0.9770.2E01, irq 255
 2: Ext: Ethernet0/1         : address is 00D0.9770.2E02, irq 255
 3: Ext: Ethernet0/2         : address is 00D0.9770.2E03, irq 255
 4: Ext: Ethernet0/3         : address is 00D0.9770.2E04, irq 255
 5: Ext: Ethernet0/4         : address is 00D0.9770.2E05, irq 255
 6: Ext: Ethernet0/5         : address is 00D0.9770.2E06, irq 255
 7: Ext: Ethernet0/6         : address is 00D0.9770.2E07, irq 255
 8: Ext: Ethernet0/7         : address is 00D0.9770.2E08, irq 255
 9: Int: Internal-Data0/1    : address is 0000.0003.0002, irq 255
10: Int: Not used            : irq 255
11: Int: Not used            : irq 255

Licensed features for this platform:
```

- 7) To see ip : show int ip brief

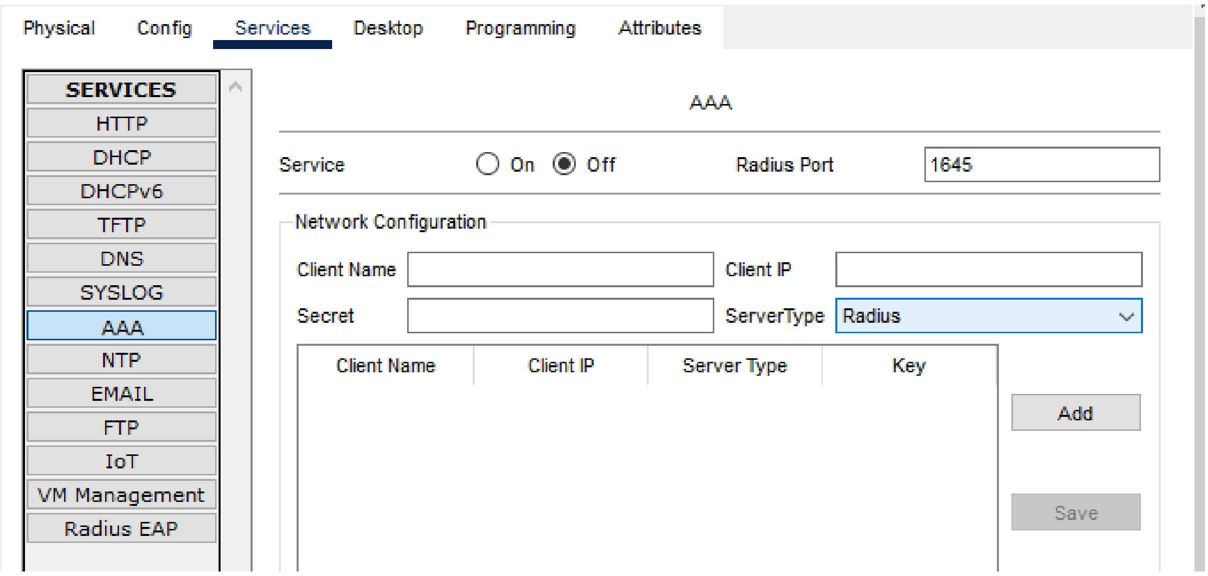


```
ASA(config)#show int ip brief
Interface              IP-Address       OK? Method Status                Protocol

Ethernet0/0            unassigned       YES unset  up                    up

Ethernet0/1            unassigned       YES unset  up                    up

Ethernet0/2            unassigned       YES unset  down                  down

Ethernet0/3            unassigned       YES unset  down                  down

Ethernet0/4            unassigned       YES unset  down                  down

Ethernet0/5            unassigned       YES unset  down                  down

Ethernet0/6            unassigned       YES unset  down                  down

Ethernet0/7            unassigned       YES unset  down                  down

Vlan1                  192.168.1.1      YES CONFIG up                    up

Vlan2                  192.168.1.1      YES manual up                    up
ASA(config)#
```

- **Access Control**:

  Radius is an AAA protocol that manage network access (Authentication, Authorization, Accounting)

  Let's add Radius on our ISCSI server, double click on it and go to tab services of AAA.



AAA

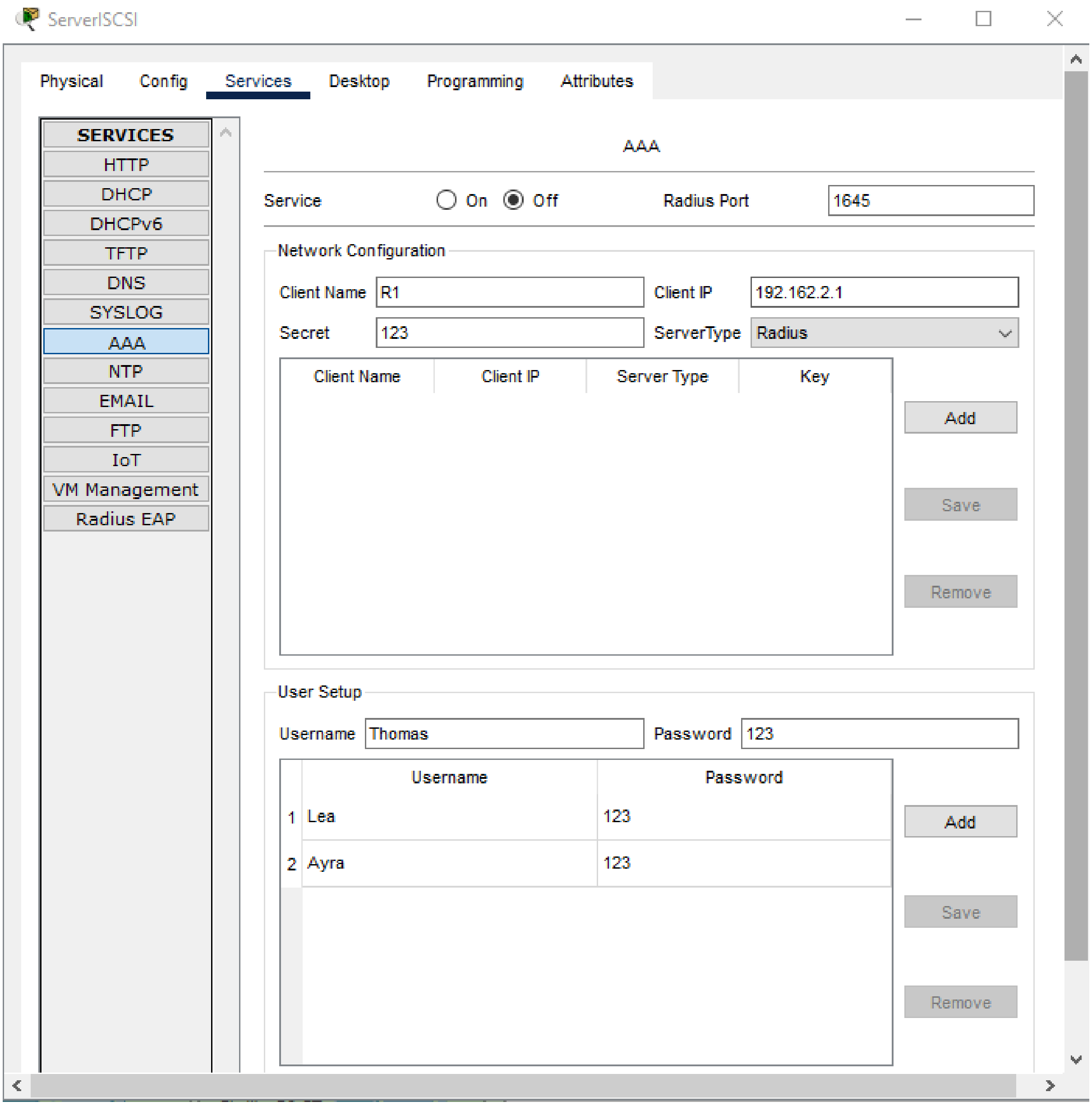
Service ○ On ● Off   Radius Port 1645

Network Configuration

Client Name   Client IP

Secret   ServerType Radius

Set up network configuration and users



AAA

Service ○ On ● Off Radius Port 1645

Network Configuration

Client Name R1 Client IP 192.162.2.1

Secret 123 ServerType Radius

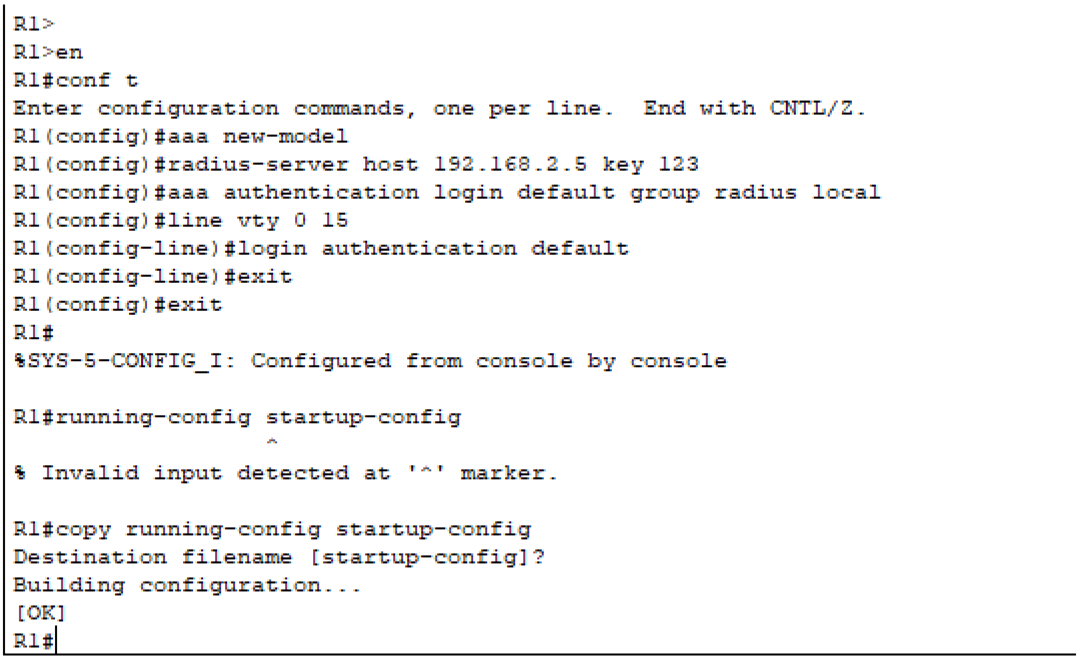
Client Name	Client IP	Server Type	Key

User Setup

Username Thomas Password 123

	Username	Password
1	Lea	123
2	Ayra	123

Go to the main router (R1) and set up AAA through CLI.



```
R1>
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#radius-server host 192.168.2.5 key 123
R1(config)#aaa authentication login default group radius local
R1(config)#line vty 0 15
R1(config-line)#login authentication default
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#running-config startup-config
                  ^
% Invalid input detected at '^' marker.

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

)

Now we've created 3 users on our ISCSI server, meaning that any remote user attempting to access the device through Telnet or SSH will be subject to the AAA settings we configured.

Cost breakdown

- **Servers**:
  - 4 Cisco PT-server : 4 x 2.000€ = 8.000$
- **Workstations**:
  - 43 Cisco PC-PT : 43 x 1.000€ = 43.000$
- **Routers**:
  - Router-PT (150$) with 3 * PT-ROUTER-NM-1CGE as the main router.
- **Switches:**
  - Switch PT-Empty (400$) with 6 * PT-SWITCH-NM-1CFE for secretariat/management with 5 hosts.
  - Switch PT-Empty (800$) with 9 * PT-SWITCH-NM-1CFE for study with 8 hosts.
  - Switch 2950T-24 (550$)for production with 10 hosts.
  - Switch 2950T-24 (550$) for support with 20 hosts.
  - Switch PT-Empty (600$) with 5 * PT-SWITCH-NM-1CFE for server area with 4 servers.
  - Switch PT-Empty (600$) with 5 * PT-SWITCH-NM-1CFE for 3 switch and the main router.

- **Firewall:**
  - 1 Cisco “5505” ASA firewall : 600$
- **TOTAL COST :**
  - 54650$

Conclusion

The network infrastructure outlined in this document is designed to provide a secure, scalable, and efficient platform to support the operations of the company that owns it. By adopting a str-based topology, deploying strategic hosts and connectivity solutions, and implementing robust security measures, the network ensures optimal performance, reliability, and protection against external threats. Efforts will continue to enhance the network's functionality, scalability and resilience in the face of evolving challenges and technological advancements.