<https://www.firewall.cx/cisco/cisco-routers/cisco-router-site-to-site-ipsec-vpn.html>

<https://www.firewall.cx/cisco/cisco-services-technologies/cisco-comparing-vpn-technologies.html>

<https://www.firewall.cx/cisco/cisco-firewalls/cisco-asa5500-startup.html>

<https://www.speaknetworks.com/basic-cisco-asa-5506-x-configuration-example/>

<https://www.linkedin.com/pulse/my-ise-lab-initial-setup-jonas-resende/>

<https://www.geeksforgeeks.org/basic-configuration-of-adaptive-security-appliance-asa/>

<https://www.ccri.edu/faculty_staff/comp/jmowry/Security/ASA5506%209-3-1-2%20Lab%20-%20Configure%20ASA%20Basic%20Settings%20and%20Firewall%20Using%20CLI.pdf>

<http://www.networkset.net/2012/06/17/cisco-asa-basic/>

ipsec

<https://www.youtube.com/watch?v=oWb1OptFBpk>

show crypto isakmp sa

dhcp

<https://www.youtube.com/watch?v=CYYhusR6Mh4>

<https://www.youtube.com/watch?v=oUmR31WjouU>

vpc>ip dhcp

dns

<https://www.youtube.com/watch?v=E6b1bCIpi20>

<https://www.youtube.com/watch?v=RYrnRZtjAxo>

L3 switch

<https://www.youtube.com/watch?v=NZwDldhtqxA>

R1# **configure terminal**  
R1(config)# **ip dns server**R1(config)# **ip domain-lookup**

R1(config)# **ip name-server 4.2.2.5**  
R1(config)# **ip name-server 4.2.2.6**

R1(config)# **ip host alan 192.168.1.10**  
R1(config)# **ip host john 192.168.1.11**  
R1(config)# **ip host wayne 192.168.1.12**

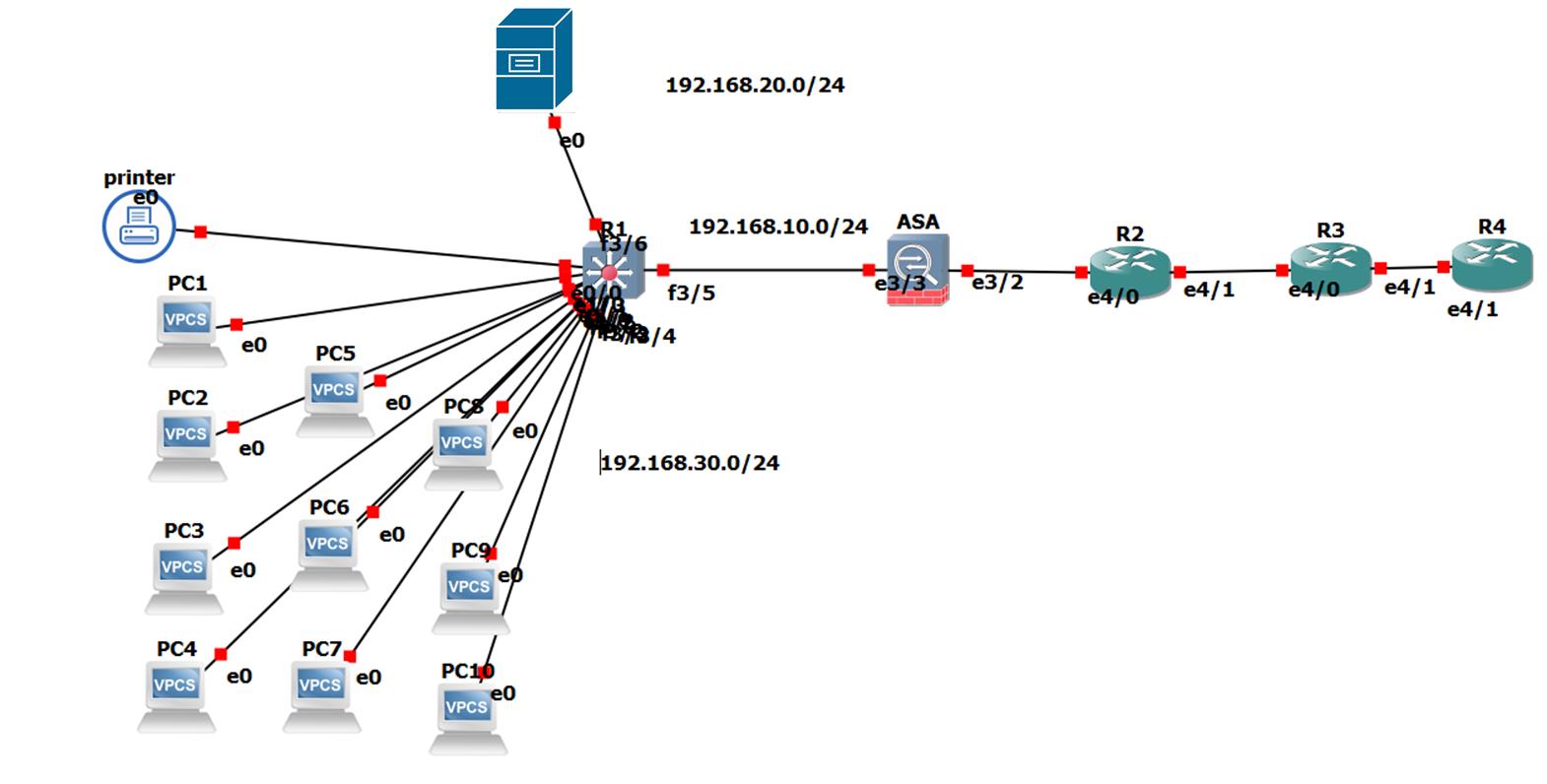
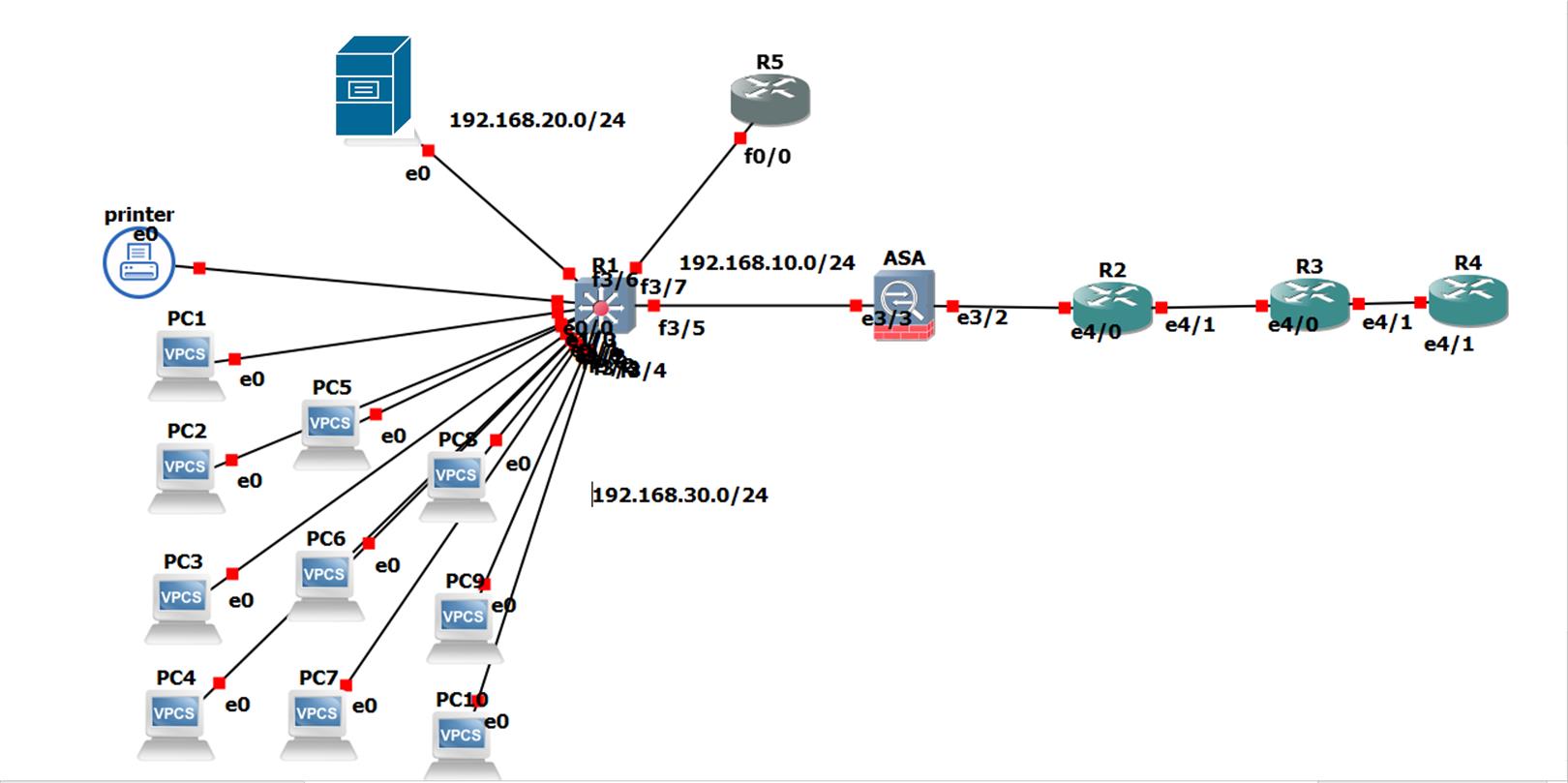
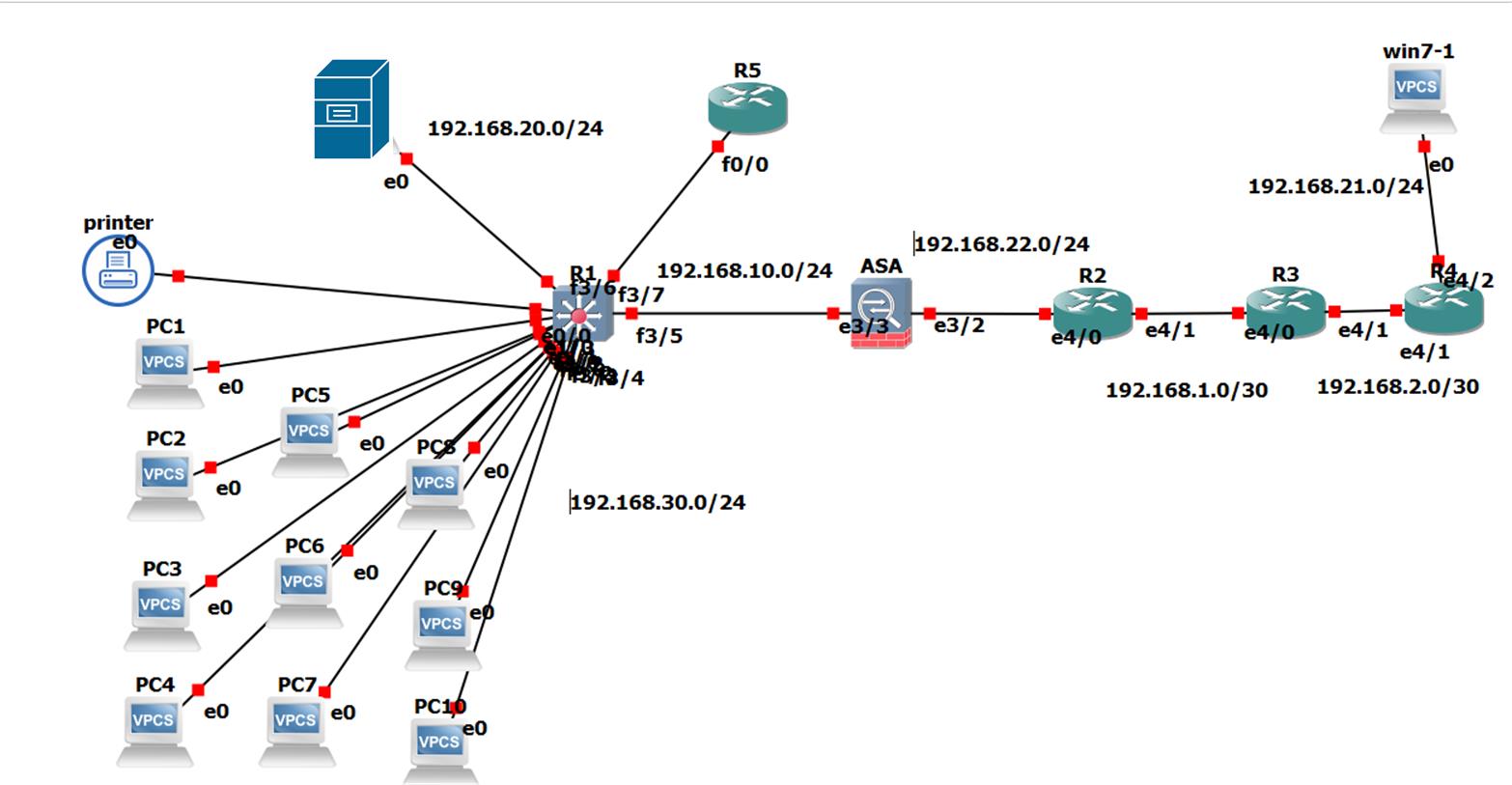
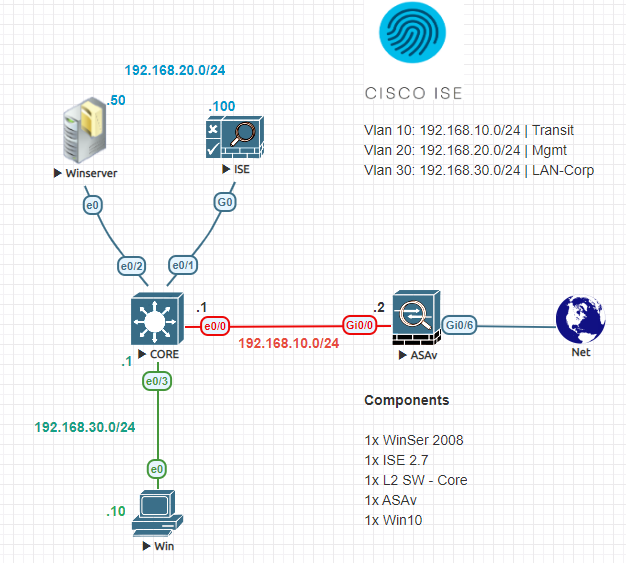
**محاكاة شبكة حاسوبية لمكتب صغير:**

**قم بتصميم شبكة حاسوبية لمكتب صغير يتضمن 10 أجهزة كمبيوتر، طابعة، خادم، راوتر، و سويتش.**

**قم بتكوين عناوين IP، DHCP، DNS، و VPN.**

**قم بتأمين الشبكة باستخدام جدار الحماية، قواعد التصفية، و VPN.**

**قم باختبار الشبكة للتأكد من عملها بشكل صحيح**



**VLANs**

Three VLANs have been separated for this.

**VLAN 10**

* Subnet: 192.168.10.0/24
* Name: transit

**VLAN 20**

* subnet: 192.168.20.0/24
* name: mgmt (management)

**VLAN 30**

* subnet: 192.168.30.0/24
* name: lan-corp

Let’s go to the device’s configuration.

**CORE Switch**

*config t*

*!*

*hostname CORE*

*!*

*vlan 10*

*name transit*

*!*

*vlan 20*

*name mgmt*

*!*

*vlan 30*

*name lan-corp*

*!*

*interface vlan 10*

*description transit*

*ip address 192.168.10.1 255.255.255.0*

*no shut*

!

You can repeat the same process for interfaces VLAN 20 and 30, changing the third octet based on the VLAN number and always using the first available IP address for each interface.

For interface vlan 30 there is an additional command to include, that is *ip helper-address 192.168.20.50*. This command is to forward all DHCP request to DHCP server coming from devices connected to the interfaces with VLAN 30 configured.

At this moment, all the physical interfaces will be in host mode, that is access mode, and with VLAN configured as per indicated in the topology.

!

*interface ethernet0/0*

*switchport host*

*switchport access vlan 10*

*!*

*interface ethernet0/1*

*switchport host*

*switchport access vlan 20*

*!*

*interface ethernet0/2*

*switchport host*

*switchport access vlan 20*

*!*

*interface ethernet0/3*

*switchport host*

*switchport access vlan 30*

!

At last, but not least, a username with password, and enable password.

!

*enable password Cisco123*

*username Admin password Cisco123*

*!*

The default route below is using as default gateway/next-hop the Firewall interface IP address and this is to allow the communication to Internet.

!

*ip route 0.0.0.0 0.0.0.0 192.168.10.2*

!

***note: all the commands above are issued in global configuration mode.***

Do not forget to save the configuration with *copy running-config startup-config* or only *write.*

**FIREWALL**

The first configuration of firewall are the two interfaces, inside and outside.

The inside one will be configured in transit subnet and outside it’s configured with DHCP address, due to my lab, but it can also be configured with an IP address for the default gateway.

!

*conf t*

!

*interface GigabitEthernet0/0*

*nameif inside*

*security-level 100*

*ip address 192.168.10.2 255.255.255.0*

!

*interface GigabitEthernet0/6*

*nameif outside*

*security-level 0*

*ip address dhcp*

!

After configuring the interfaces, it’s time to setup the object network.

These network objects are essential for the communication from the internal network to external world, Internet, and in order to stablish this flow, it's also need apply the NAT configuration (in this case we are using dynamic NAT).

!

object network lan-corp

subnet 192.168.30.0 255.255.255.0

nat (inside,outside) dynamic interface

object network mgmt

subnet 192.168.20.0 255.255.255.0

nat (inside,outside) dynamic interface

!

Also, apply the default route (route to Internet) and static routes (to internal subnets).

!

*route outside 0.0.0.0 0.0.0.0 172.29.129.254*

*route inside 192.168.20.0 255.255.255.0 192.168.10.1*

*route inside 192.168.30.0 255.255.255.0 192.168.10.1*

!

Just note, that after applying all these configurations, let’s enable icmp inspect in the firewall, because in case this protocol is not being inspected in the policy-map global\_policy, no icmp packets will be allowed in the network.

!

*policy-map global\_policy*

*class inspection\_default*

*inspect icmp*

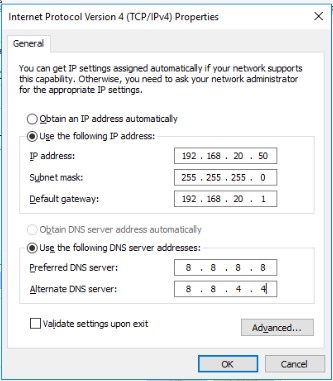
!

Then, firewall-ASA configuration Is ready.

***Note: All the configurations above are applied in global configuration mode.***

**WINDOWS SERVER - AD, DNS, DHCP and NTP**

The first configuration for Windows Server, of course is the IP address.

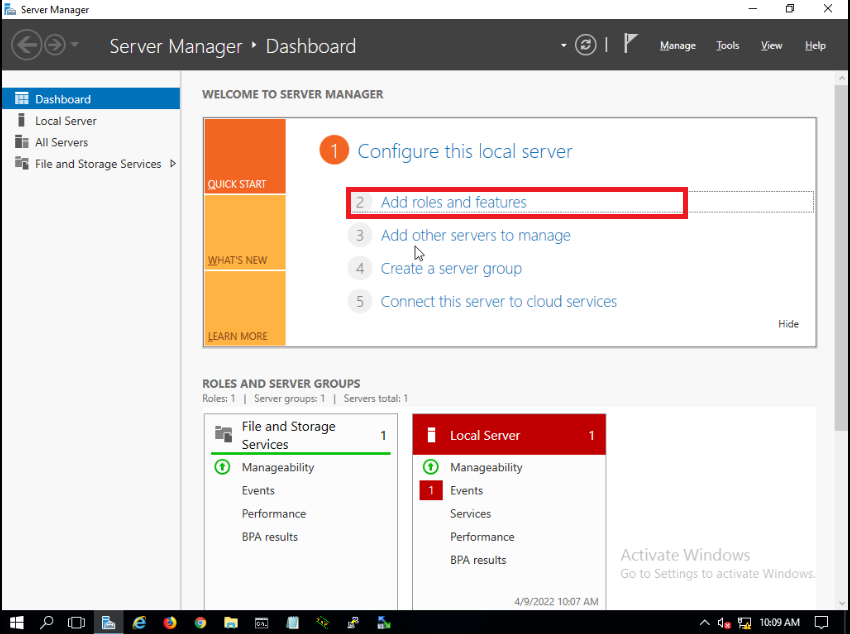


After the IP address configuration is completed, let's jump to configure the features that will be used in this lab.

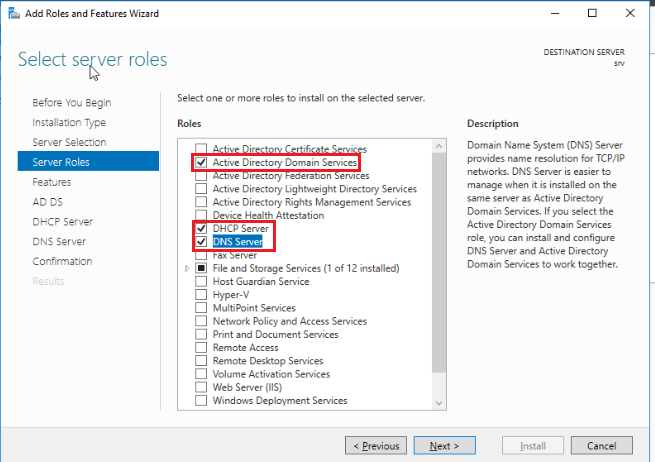
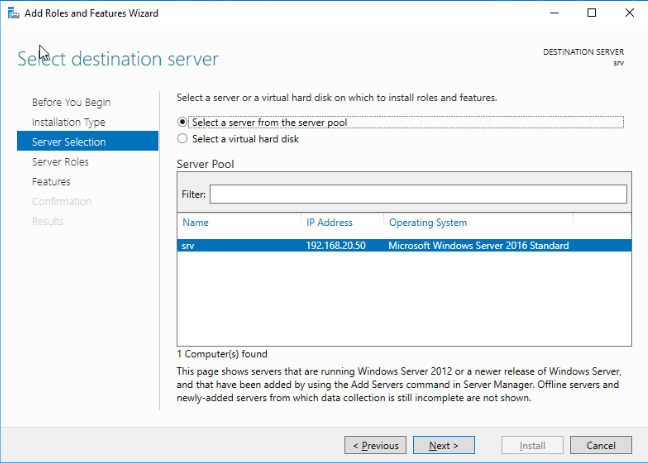
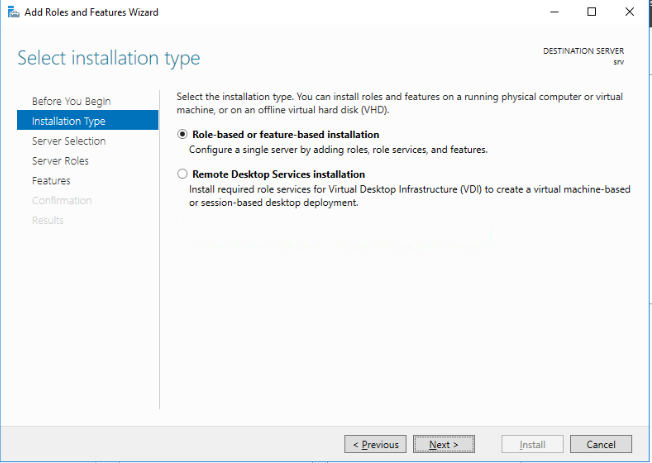
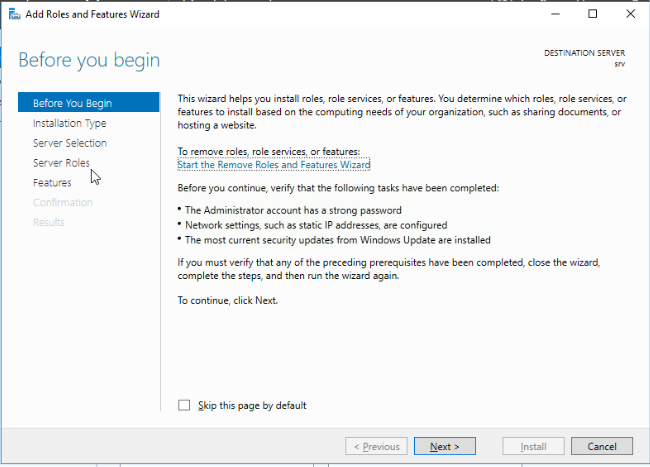
**AD, DNS and DHCP**

To configure these three services, let’s follow the setup below.

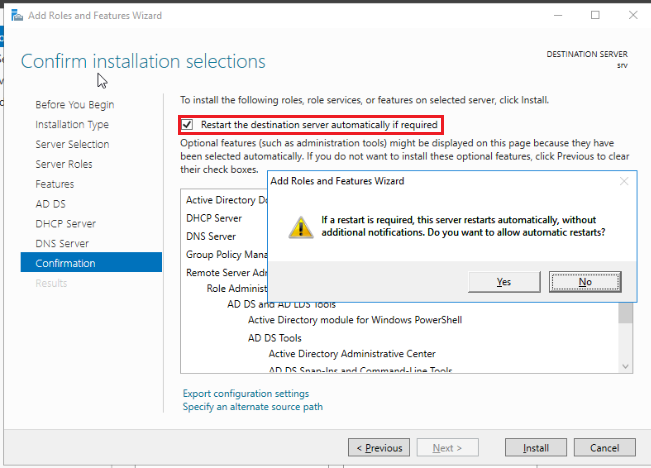
On the Windows menu open **Server Manager** and click on Add roles and features.**Add roles and features.**



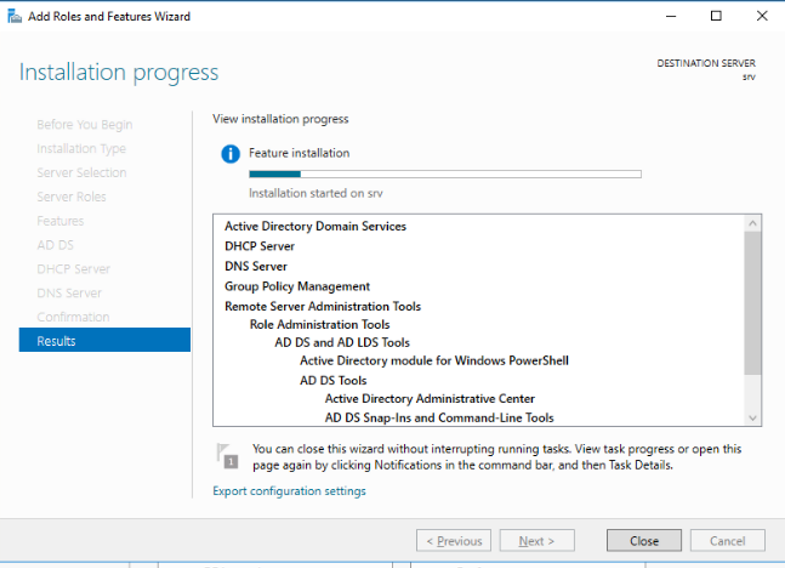
After that click on **Add Roles and Features**, click on Next>Next>Next in the next three windows.



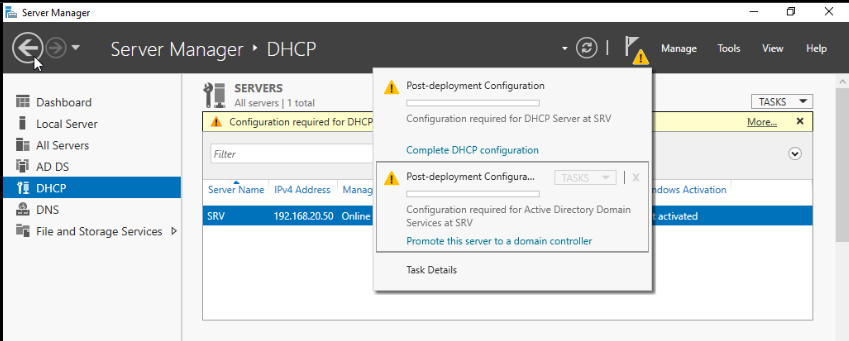
Then click, Next until the Confirm installation selections window, then click install. After that, the installation process will start. If want, you can mark the check box **Restart the destination...** or leave unchecked and later restart the device.



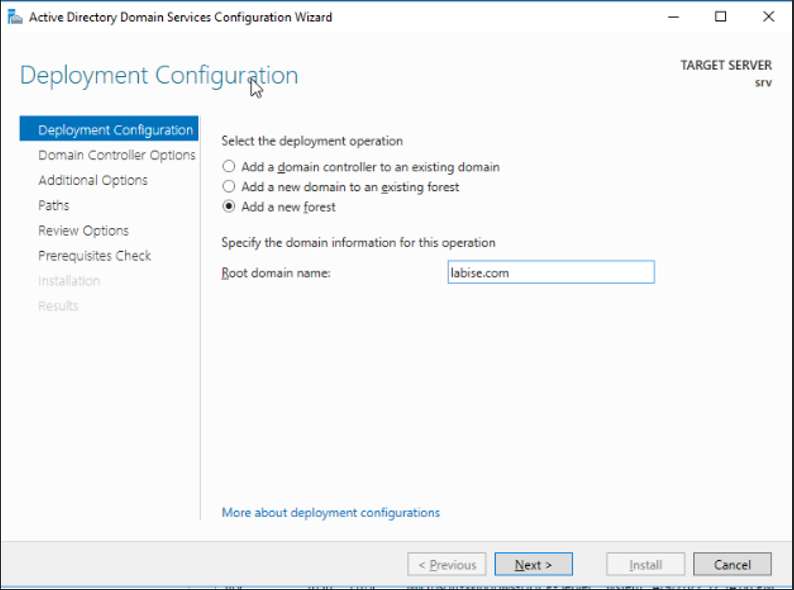
After the message Installation succeeded on the server, click on the close button and restart the server.



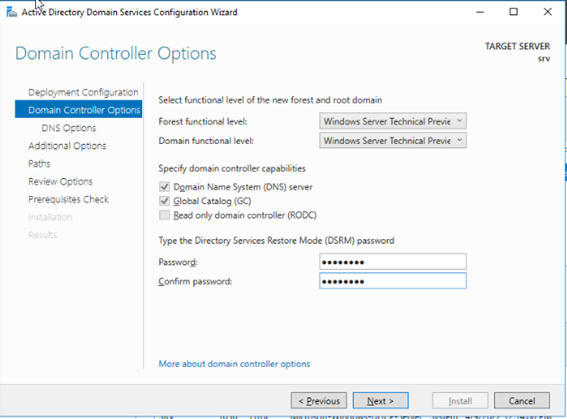
After this configuration is completed, two Post-deployment Configuration alarm will pop up, that is to complete DHCP setup and to promote the server as domain-controller. So, let’s go to apply those.



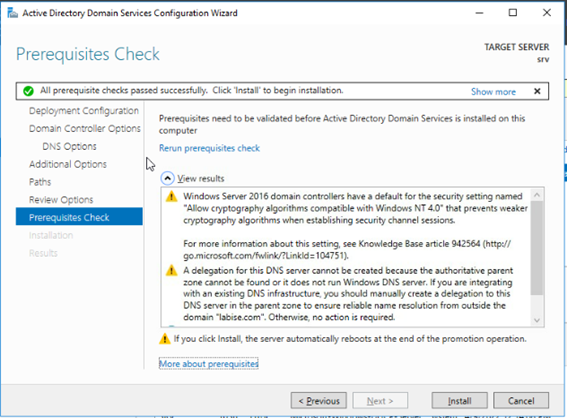
First, let’s promote the server to a domain controller, selecting Add a new forest, and root domain name as labise.com, the click on Next.



Insert a new password, as your preference.

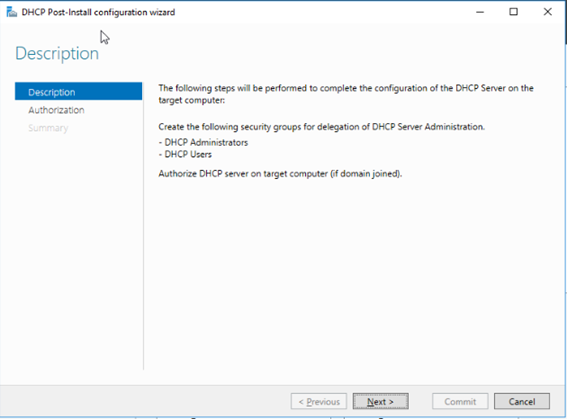


Click on Next button until you get Prerequisites Check completed, then click on install. It will be a little time consuming, time to do a break and get a cup of coffee. Have in mind that the server will automatically restart to during the configuration deployment.



After the installation, login again in the server and complete the DHCP configuration.

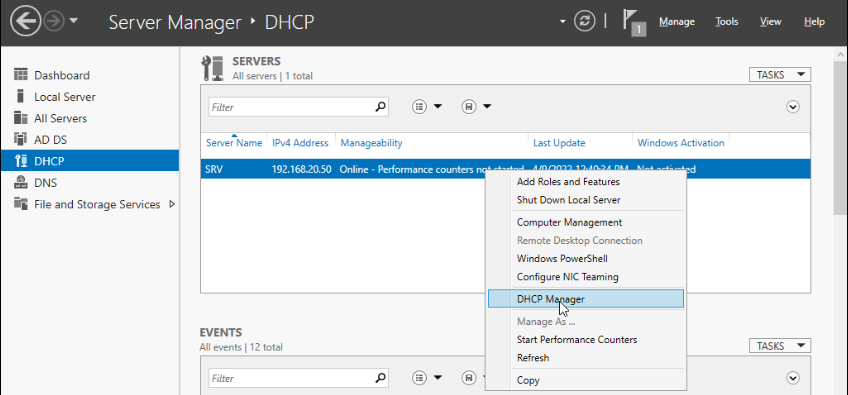
On the top right side, click on Complete DHCP Configuration, as you did to Promote the server in domain controller.



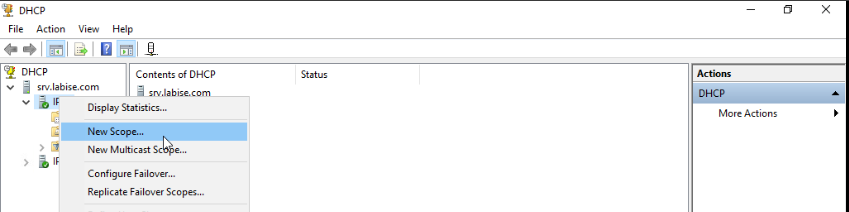
Click on next, then commit and after close.

Now that DHCP configuration is completed, let’s create a DHCP scope for lan-corp.

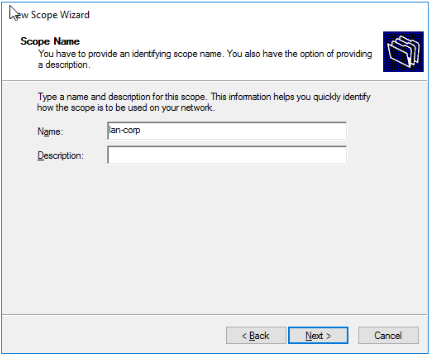
Click on DHCP at the right corner, then right mouse button on DHCP IP address and click on DHCP Manager.



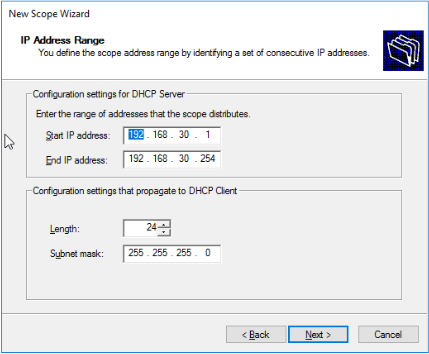
In the new window, click with the right button on IPv4 and New Scope, then click on next.



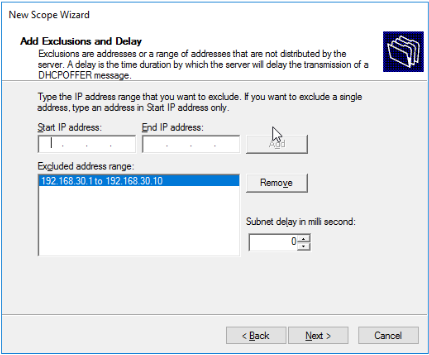
Insert the name of scope, on this case lan-corp, click next.



Type the first and last IP address from range, click next.

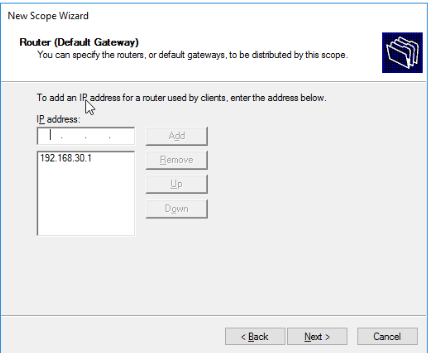


Create an exclusion. This is to avoid the DHCP server leasing there range of IP addresses that is static configured in the subnet, as the address for interface VLAN 30 in the CORE switch. Click next until the window Configure DHCP Options, and select Yes, I want to configure this option now.

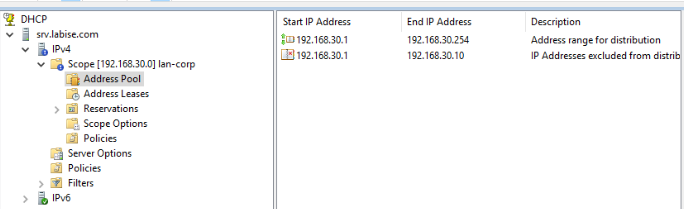


DNS configuration will come automatically, as DNS server is the same then DHCP. WINS server, there is no need to be configured on this lab.

Configure the **Router (Default Gateway)** that is the IP address in the interface VLAN 30 in CORE switch, then click Next and finish button. Also, select Yes to activate the scope now.



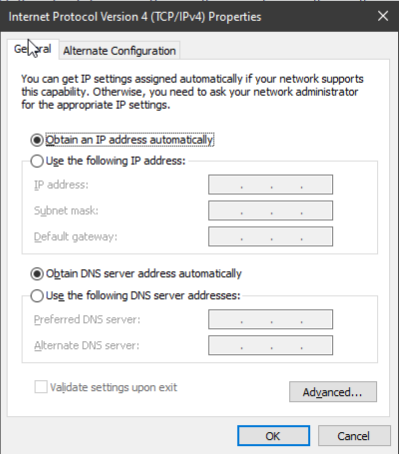
After this configuration, you can see on the right side that there is a new scope created.



That way, windows server is also configured and ready for the lab.

## **WINDOWS-PC**

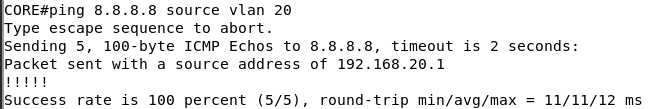
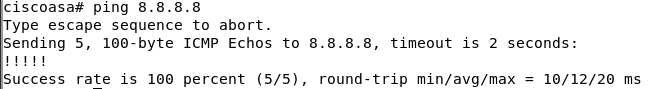
For the Windows PC, the only configuration that needs to be confirmed is the DHCP configuration in the NIC. It needs to be as automatically/DHCP.



## **Tests and validation**

After the configuration is completed, is the time to test our lab.

### Internet connectivity from ASA and CORE

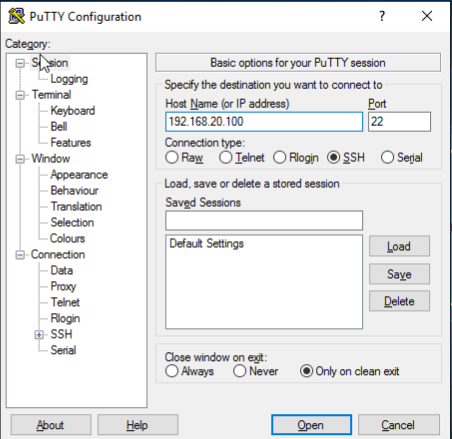
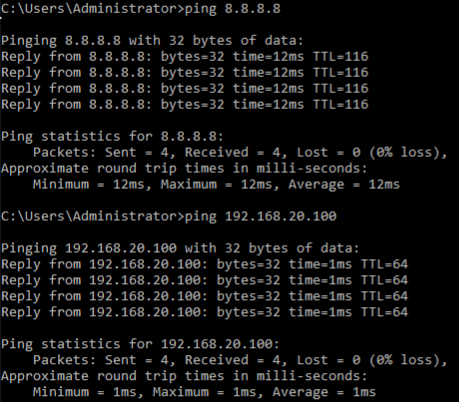


From CORE switch I have used as source VLAN 20, because is one of the VLANs which has a return route configured in the firewall. If we use only ping without source interface, the traffic will get out by default over Interface VLAN 10, and in the firewall there is no static route configured for VLAN 10 subnet.

### Tests from AD-Server

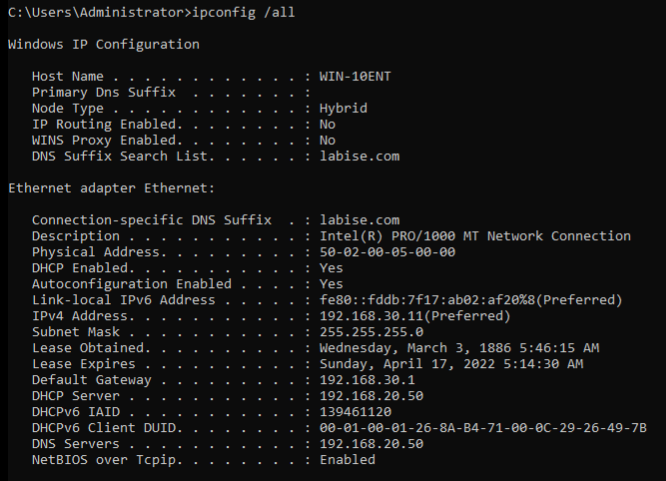
From AD server, will be test:

* Internet connectivity
* ISE connectivity, over HTTPS, ICMP and SSH



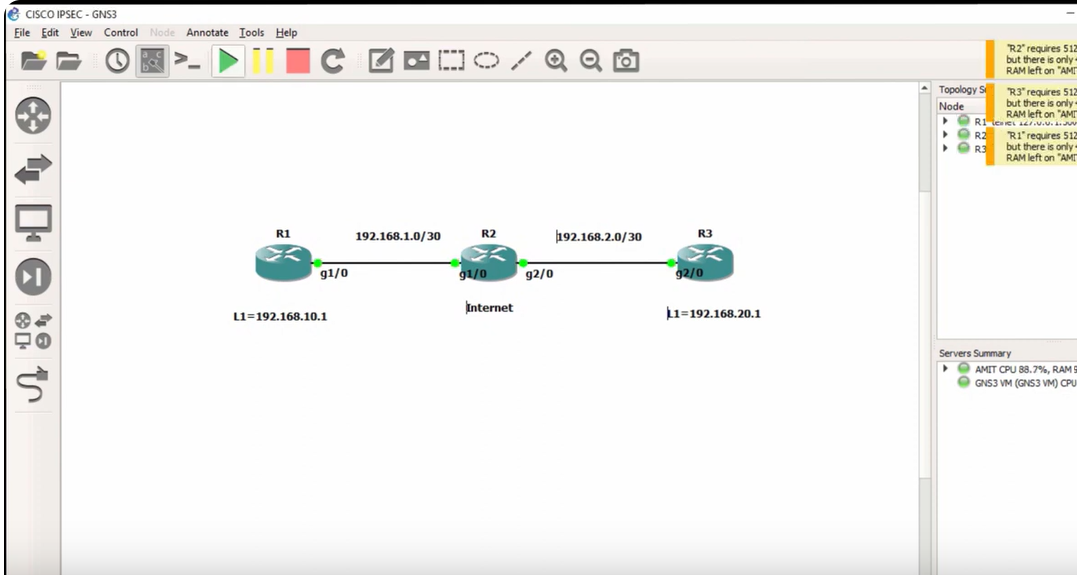
## Windows PC

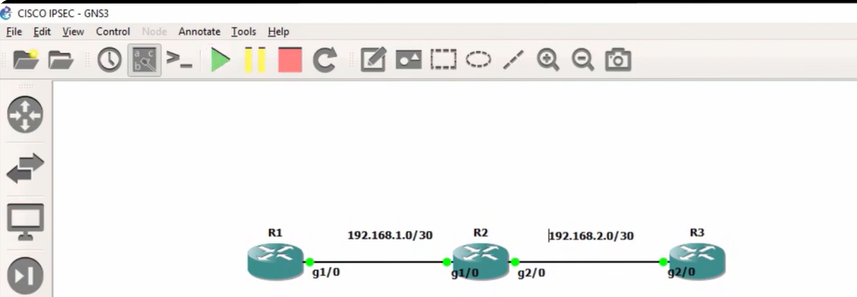
For Windows PC, just validate that it has received an IP address from DHCP server, with the command ipconfig /all from cmd prompt.

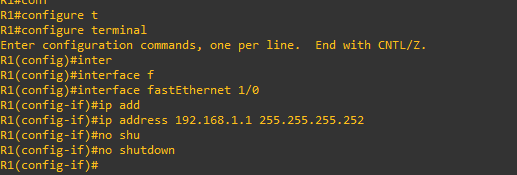


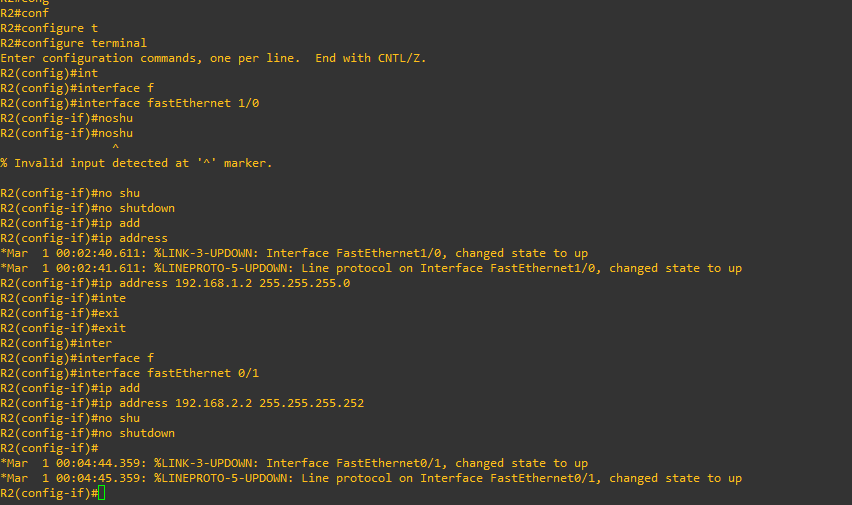
The results above show that the computer is right receiving the correct DNS server, Default Gateway, IP address, Mask, etc.

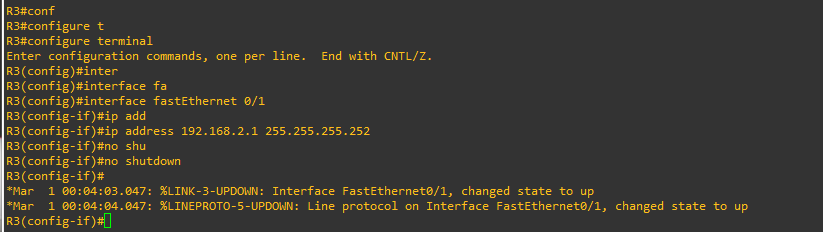
VPN configuration





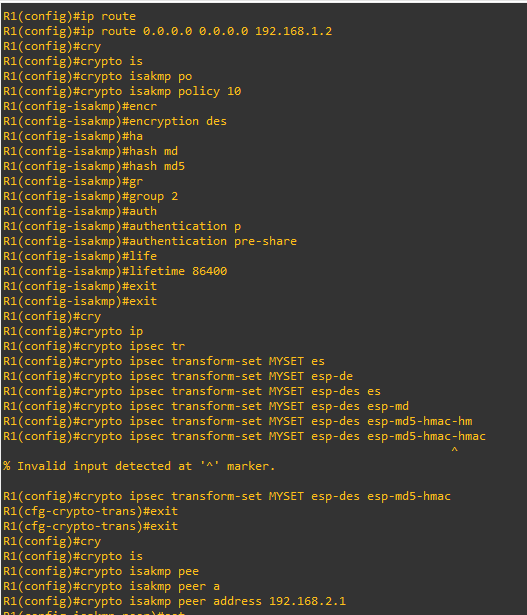


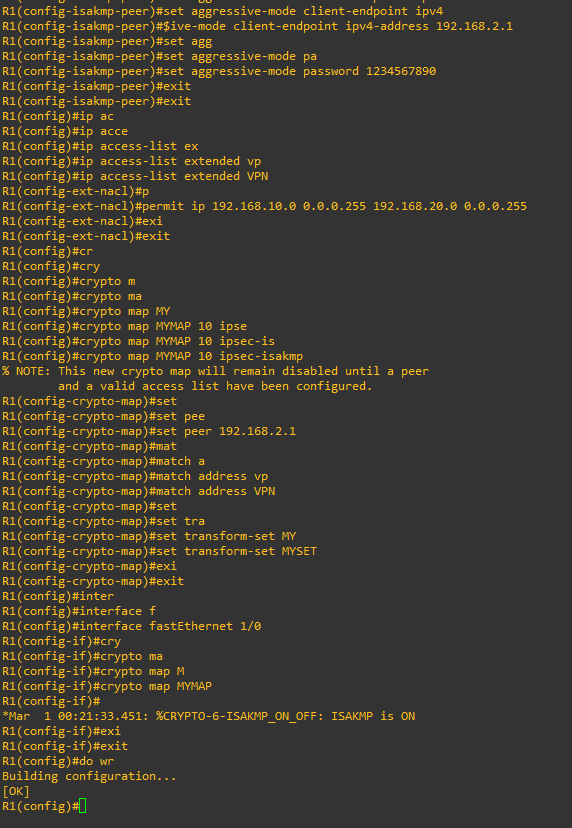




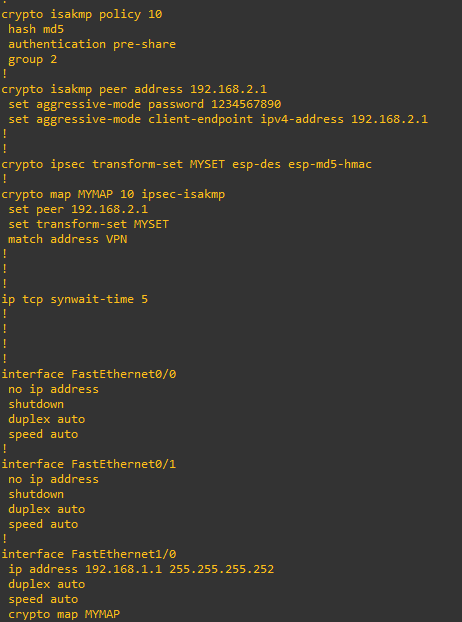


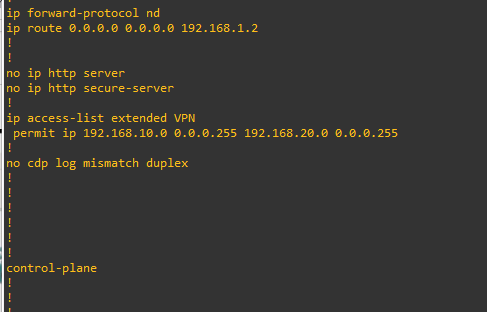




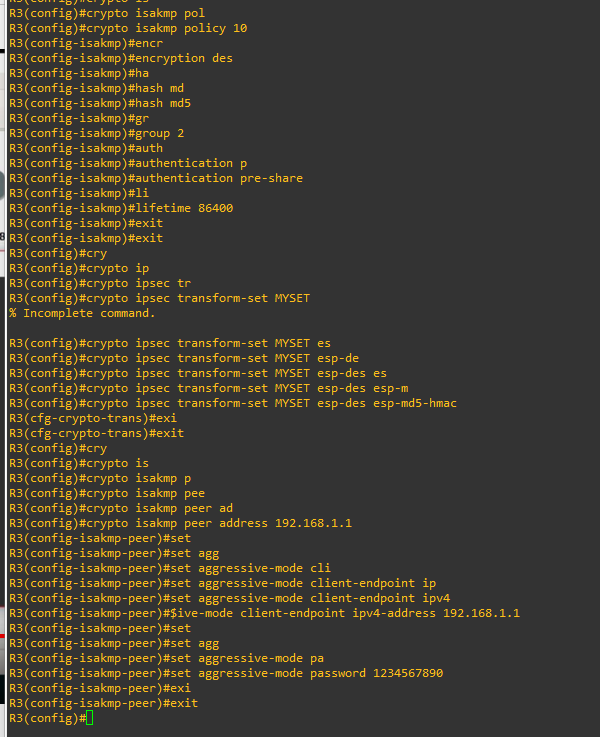


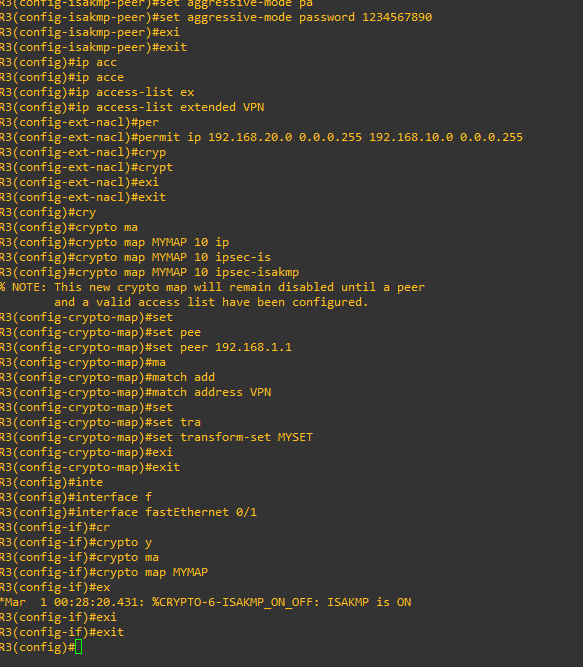
R1# show running config



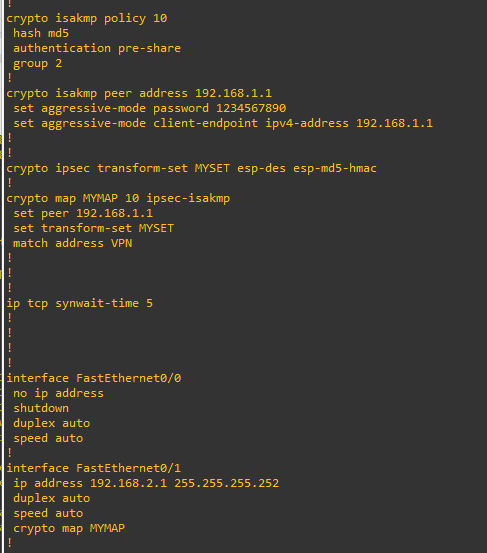


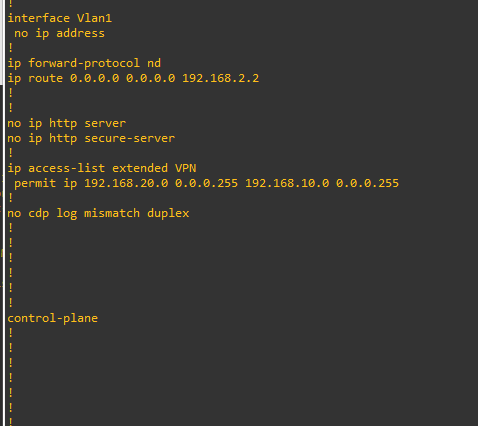
R3 configuration





R3# show running config

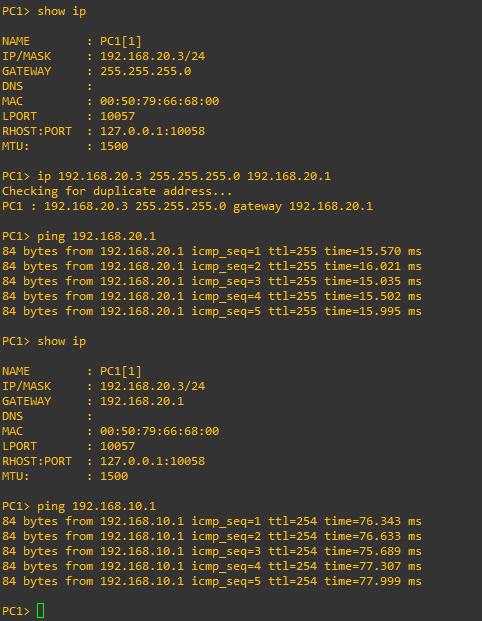


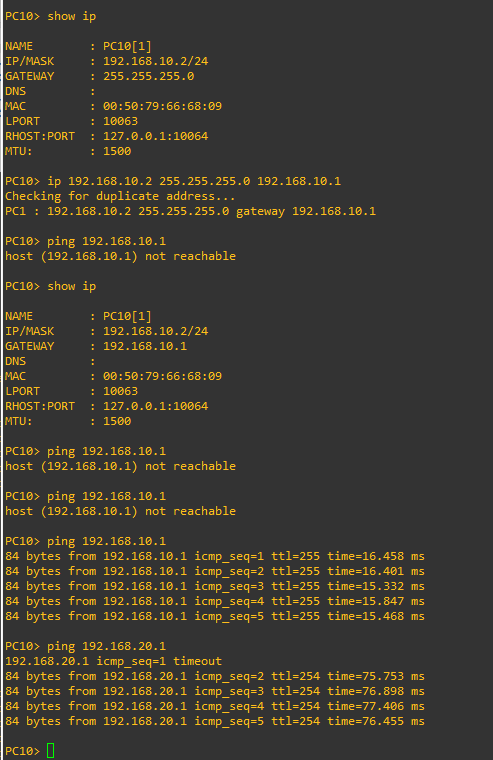


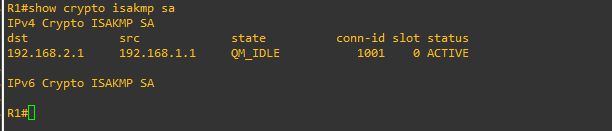
L3 switch

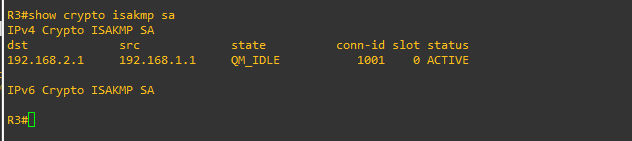
<https://drive.google.com/file/d/1blbUEewxrx1sr6prANgOYuvXbzAAHjg7/view?usp=drive_link>

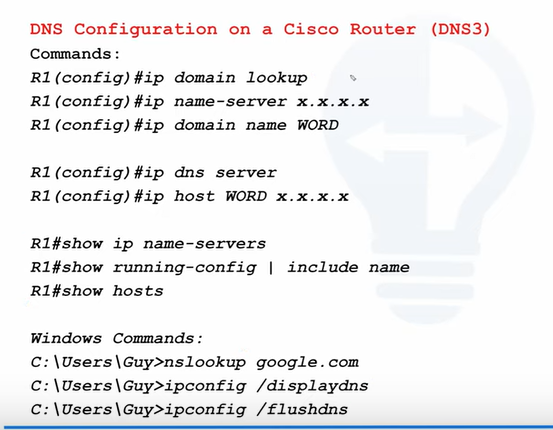
3725











 تأكد من إمكانية وصول الموجه إلى خادم DNS. يؤز خادم DNS من الموجه باستخدام عنوان IP الخاص به، وتأكد من إستخدام الأمر **ip name-server** لتكوين عنوان IP الخاص بخادم DNS على الموجه.

 أستخدم هذه الخطوات لضمان أن الموجه يقوم بإعادة توجيه طلبات البحث:

### . ما هو81.192.17.61؟

81.192.17.61 هو عنوان IP لخادم DNS المجاني والعامة لـ Office National des Postes et Telecommunications ONPT (Maroc Telecom) / IAM.

يمكن لخادم DNS تحويل أسماء النطاقات إلى عناوين IP يمكن التعرف عليها بسهولة بواسطة الشبكة ، بحيث يحتاج المستخدمون فقط إلى إدخال اسم المجال للوصول إلى موقع الويب الهدف عند تصفح الإنترنت ، بدلاً من إدخال عناوين IP رقمية طويلة.

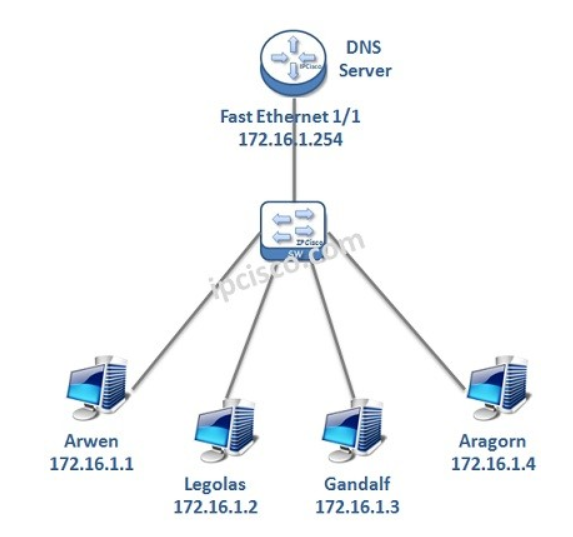
بعد تعيين عنوان خادم DNS على 81.192.17.61 ، يمكن لجهاز المستخدم الاتصال بخادم DNS الخاص بـ Office National des Postes et Telecommunications ONPT (Maroc Telecom) / IAM.

**DNS Configuration on Cisco Routers**

## How to Configure DNS on Cisco Routers?

To use **DNS**, firstly, we must configure a **DNS Server**. In a network, we can confgiure a router as a [**Domain Name System**](https://ipcisco.com/lesson/domain-name-system-overview/) **Server**. In this lesson, we will talk about Cisco DNS Server Configuration, we will see how to configure a Cisco Router as a **DNS Server** in a network.

For our **DNS Server Configuration Example**, we will use the below topology:



To configure a Cisco Router as a **DNS Server**, we need to follow some basic configuration steps. These **Cisco DNS Server configuration** steps are below:

**1. Enable DNS Server  
2. Enable Domian Lookup  
3. Public Name Server Configuration  
4. Host / IP Address Mappings  
5. Router Interface IP Configuration  
6. Hosts IP Configuration  
7. Configuration Verification**

Now, let’s configure our **Cisco Router** as a **DNS Server** with the above steps

### Enable DNS Server

To enable **DNS Server** on the router, we will use “**ip dns server**” command. With this command, our router is becoming a DNS Server.

|  |
| --- |
| RouterA # **configure terminal** RouterA (config)# **ip dns server** |

### Enable Domain Lookup

We will define hostname-ip matchings manually. But what if there is a query different than them? At this time, router will **query to an upper DNS Server** that we will configure in the next step. To enable this query, we will use “**ip domain lookup**” command.  With this command, router can query to the configured public DNS Servers if the record does not exist in it.

|  |
| --- |
| RouterA (config)# **ip domain lookup** |

### Public Name Servers Configuration

In this step, we will configure **Public Name Servers**. If the requested record is not in the host table, then router will query to these Public DNS Servers.  Here, we can use one or more, any **Public DNS Server** addresses. To use these DNS Servers for queries, this feature must be enabled with “**ip domain lookup**” command.

|  |
| --- |
| RouterA (config)# **ip name-server 1.1.1.1** RouterA (config)# **ip name-server 2.2.2.2** |

### Host / IP Address Mappings

In this step, we will give the **Hostnames** and their **IP addresses** to the DNS Server **manually**. With these records, **DNS Server** can answer to the requests.

|  |
| --- |
| RouterA (config)# **ip host Arwen 172.16.1.1**  RouterA (config)# **ip host Legolas 172.16.1.2**  RouterA (config)# **ip host Gandalf 172.16.1.3**  RouterA (config)# **ip host Aragorn 172.16.1.4** |

We can check hosts on the router with “**show hosts**” command. This command will show manually configured hosts as permanent and dynamically learned hosts via Public DNS Server as temporary. Now, we have only manual permanent configurations. If there is an ip addresses learned via public DNS, it will be listed as temporary in this list.

|  |
| --- |
| Router# **show hosts** Default domain is not set Name/address lookup uses domain service Name servers are 8.8.8.8  Codes: UN – unknown, EX – expired, OK – OK, ?? – revalidate temp – temporary, perm – permanent NA – Not Applicable None – Not defined  Host Port Flags Age Type Address(es) Arwen None (perm, OK) 0 IP 172.16.1.1 Legolas None (perm, OK) 0 IP 172.16.1.2 Gandalf None (perm, OK) 0 IP 172.16.1.3 Aragorn None (perm, OK) 0 IP 172.16.1.4 |

### Router Interface IP Configuration

Router’s Interface towards our network will be configured with an IP address in the same network with the hosts. Here, our router’s interface ip address is **172.16.1.254**. This will be used as **Default Gateway Address** and **DNS Server Address** by hosts.

|  |
| --- |
| RouterA (config)# **interface fastethernet 1/1** RouterA (config-if)# **ip address 172.16.1.254 255.255.255.0** RouterA (config-if)# **end** |

After this configuration, do not forget to save our configuration.

|  |
| --- |
| RouterA # **copy running-config startup-config** |

# Configuring Site to Site IPSec VPN Tunnel Between Cisco Routers

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

to setup and configure two Cisco routers to create a permanent secure site-to-site VPN tunnel over the Internet, using the [IP Security (IPSec) protocol](https://www.firewall.cx/networking/network-protocols/ip-security-protocol.html). In this article we assume both Cisco routers have a **static public IP address**.  Readers interested in configuring support for **dynamic public IP address endpoint routers** can refer to our [Configuring Site to Site IPSec VPN with Dynamic IP Endpoint Cisco Routers](https://www.firewall.cx/cisco/cisco-routers/cisco-router-vpn-dynamic-endpoint.html) article.

IPSec VPN tunnels can also be configured using GRE (Generic Routing Encapsulation) Tunnels with IPsec. GRE tunnels greatly simply the configuration and administration of VPN tunnels and are covered in our [Configuring Point-to-Point GRE VPN Tunnels](https://www.firewall.cx/cisco/cisco-routers/cisco-router-gre-ipsec.html) article.  Lastly, DMVPNs – a new VPN trend that provide major flexibility and almost no administration overhead can also be examined by reading our [Understanding Cisco Dynamic Multipoint VPN (DMVPN)](https://www.firewall.cx/cisco/cisco-services-technologies/cisco-dmvpn-intro.html),  [Dynamic Multipoint VPN (DMVPN) Deployment Models & Architectures](https://www.firewall.cx/cisco/cisco-services-technologies/cisco-dmvpn-models.html) and [Configuring Cisco Dynamic Multipoint VPN (DMVPN) - Hub, Spokes , mGRE Protection and Routing - DMVPN Configuration](https://www.firewall.cx/cisco/cisco-routers/cisco-router-dmvpn-configuration.html) articles.

**ISAKMP** (**Internet Security Association and Key Management Protocol**) and **IPSec** are essential to building and encrypting the VPN tunnel. **ISAKMP**, also called **IKE** (**Internet Key Exchange**), is the negotiation protocol that allows two hosts to agree on how to build an IPsec security association. **ISAKMP** negotiation consists of **two phases**: **Phase 1** and **Phase 2**.

**Phase 1** creates the first tunnel, which protects later **ISAKMP negotiation messages**. **Phase 2** creates the tunnel that protects data.  **IPSec** then comes into play to **encrypt the data using encryption algorithms** and provides **authentication**, **encryption** and **anti-replay services**.

## IPSec VPN Requirements

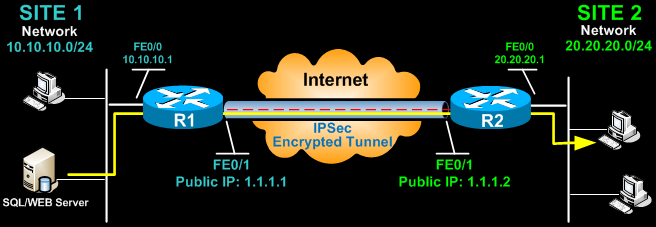
To help make this an easy-to-follow exercise, we have split it into two steps that are required to get the Site-to-Site IPSec VPN Tunnel to work.

These steps are:

(1)  Configure **ISAKMP** (ISAKMP Phase 1)

(2)  Configure **IPSec** (ISAKMP Phase 2, ACLs, Crypto MAP)

Our example setup is between two branches of a small company, these are **Site 1** and **Site 2**. Both the branch routers connect to the Internet and have a static IP Address assigned by their ISP as shown on the diagram:



**Site 1** is configured with an internal network of **10.10.10.0/24**, while **Site 2** is configured with network **20.20.20.0/24**. The goal is to securely connect both LAN networks and allow full communication between them, without any restrictions.

## Configure ISAKMP (IKE) - (ISAKMP Phase 1)

**IKE** exists only to establish **SAs** (**Security Association**) for **IPsec**. Before it can do this, **IKE** must **negotiate** an **SA** (an ISAKMP SA) relationship with the peer.

To begin, we’ll start working on the **Site 1 router (R1)**.

First step is to configure an **ISAKMP Phase 1 policy**:

|  |
| --- |
| R1(config)# **crypto isakmp policy 1**  R1(config-isakmp)# **encr 3des**  R1(config-isakmp)# **hash md5**  R1(config-isakmp)# **authentication pre-share**  R1(config-isakmp)# **group 2**  R1(config-isakmp)# **lifetime 86400** |

The above commands define the following (in listed order):

**3DES** - The encryption method to be used for Phase 1.

**MD5** - The hashing algorithm

**Pre-share** - Use Pre-shared key as the authentication method

**Group 2** - Diffie-Hellman group to be used

**86400** – Session key lifetime. Expressed in either kilobytes (after x-amount of traffic, change the key) or seconds. Value set is the default value.

We should note that **ISAKMP Phase 1** policy is defined globally. This means that if we have five different remote sites and configured five different ISAKMP Phase 1 policies (one for each remote router), when our router tries to negotiate a VPN tunnel with each site it will send all five policies and use the first match that is accepted by both ends.

Next we are going to define a pre shared key for authentication with our peer (R2 router) by using the following command

|  |
| --- |
| R1(config)# **crypto isakmp key firewallcx address 1.1.1.2** |

The peer’s pre shared key is set to **firewallcx** and its public **IP Address** is **1.1.1.2**. Every time **R1** tries to establish a **VPN tunnel** with **R2** (**1.1.1.2**), this pre shared key will be used.

**Configure IPSec - 4 Simple Steps**

To configure IPSec we need to setup the following in order:

* **Create extended ACL**
* **Create IPSec Transform**
* **Create Crypto Map**
* **Apply crypto map to the public interface**

Let us examine each of the above steps.

**Step 1: Creating Extended ACL**

Next step is to create an access-list and define the traffic we would like the router to pass through the VPN tunnel.  In this example, it would be traffic from one network to the other, 10.10.10.0/24 to 20.20.20.0/24.  Access-lists that define VPN traffic are sometimes called **crypto access-list** or **interesting traffic access-list**.

|  |
| --- |
| R1(config)# **ip access-list extended VPN-TRAFFIC** R1(config-ext-nacl)# **permit ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255** |

## Step 2: Create IPSec Transform (ISAKMP Phase 2 policy)

Next step is to create the transform set used to protect our data. We’ve named this **TS**:

|  |
| --- |
| R1(config)# **crypto ipsec transform-set TS esp-3des esp-md5-hmac** |

The above command defines the following:

- **ESP-3DES** - Encryption method

- **MD5** - Hashing algorithm

## Step 3: Create Crypto Map

The Crypto map is the last step of our setup and connects the previously defined ISAKMP and IPSec configuration together:

|  |
| --- |
| R1(config)# **crypto map CMAP 10 ipsec-isakmp**  R1(config-crypto-map)# **set peer 1.1.1.2**  R1(config-crypto-map)# **set transform-set TS**  R1(config-crypto-map)# **match address VPN-TRAFFIC** |

We’ve named our crypto map CMAP. The **ipsec-isakmp** tag tells the router that this crypto map is an IPsec crypto map. Although there is only one peer declared in this crypto map (1.1.1.2), it is possible to have multiple peers within a given crypto map.

**Step 4: Apply Crypto Map To The Public Interface**

The final step is to apply the crypto map to the outgoing interface of the router. Here, the outgoing interface is FastEthernet 0/1.

|  |
| --- |
| R1(config)# **interface FastEthernet0/1** R1(config- if)# **crypto map CMAP** |

Note that you can assign only one crypto map to an interface.

As soon as we apply crypto map on the interface, we receive a message from the router  that confirms isakmp is on: “**ISAKMP is ON**”.

At this point, we have completed the IPSec VPN configuration on the **Site 1 router**.

We now move to the **Site 2 router** to complete the VPN configuration. The settings for **Router 2** are identical, with the only difference being the **peer IP Addresses** and **access lists**

|  |
| --- |
| R2(config)# **crypto isakmp policy 1**  R2(config-isakmp)# **encr 3des**  R2(config-isakmp)# **hash md5**  R2(config-isakmp)# **authentication pre-share**  R2(config-isakmp)# **group 2**  R2(config-isakmp)# **lifetime 86400**  R2(config)# **crypto isakmp key firewallcx address 1.1.1.1**  R2(config)# **ip access-list extended VPN-TRAFFIC**  R2(config-ext-nacl)# **permit ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255**    R2(config)# **crypto ipsec transform-set TS esp-3des esp-md5-hmac**  R2(config)# **crypto map CMAP 10 ipsec-isakmp**  R2(config-crypto-map)# **set peer 1.1.1.1**  R2(config-crypto-map)# **set transform-set TS**  R2(config-crypto-map)# **match address VPN-TRAFFIC**  R2(config)# **interface FastEthernet0/1**  R2(config- if)# **crypto map CMAP** |

## Network Address Translation (NAT) and IPSec VPN Tunnels

[Network Address Translation (NAT)](https://www.firewall.cx/networking/network-address-translation.html) is most likely to be configured to provide Internet access to internal hosts. When configuring a **Site-to-Site VPN tunnel**, it is imperative to instruct the router **not to perform NAT** (deny NAT) on packets destined to the remote VPN network(s).

This is easily done by inserting a deny statement at the beginning of the **NAT access lists** as shown below:

For **Site 1’s router**:

|  |
| --- |
| R1(config)# **ip nat inside source list 100 interface fastethernet0/1 overload**  R1(config)# **access-list 100 remark -=[Define NAT Service]=-**  R1(config)# **access-list 100 deny ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255**  R1(config)# **access-list 100 permit ip 10.10.10.0 0.0.0.255 any**  R1(config)# **access-list 100 remark** |

And **Site 2’s router**:

|  |
| --- |
| R2(config)# **ip nat inside source list 100 interface fastethernet0/1 overload**  R2(config)# **access-list 100 remark -=[Define NAT Service]=-**  R2(config)# **access-list 100 deny ip 20.20.20.0 0.0.0.255 10.10.10.0  0.0.0.255**  R2(config)# **access-list 100 permit ip 20.20.20.0 0.0.0.255 any**  R2(config)# **access-list 100 remark** |

## Establishing and Verifying the IPSec VPN Tunnel

At this point, we’ve completed our configuration and the VPN Tunnel is ready to be brought up.  To initiate the VPN Tunnel, we need to force one packet to traverse the VPN and this can be achieved by pinging from one router to another:

|  |
| --- |
| R1# **ping 20.20.20.1 source fastethernet0/0**  Type escape sequence to abort.  Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:  Packet sent with a source address of 10.10.10.1  **.!!!!**  Success rate is 80 percent (4/5), round-trip min/avg/max = 44/47/48 ms |

The first [icmp echo (ping)](https://www.firewall.cx/networking/network-protocols/icmp-protocol/icmp-echo-ping.html) received a timeout, but the rest received a reply, as expected. The time required to bring up the VPN Tunnel is sometimes slightly more than 2 seconds, causing the first ping to timeout.

To verify the VPN Tunnel, use the **show crypto session** command:

|  |
| --- |
| R1# **show crypto session**  Crypto session current status  Interface: FastEthernet0/1  Session status: **UP-ACTIVE**  Peer: 1.1.1.2 port 500    IKE SA: local 1.1.1.1/500 remote 1.1.1.2/500 **Active**    IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 20.20.20.0/255.255.255.0  **Active SAs: 2, origin: crypto map** |

يعرّف IPsec في الأصل بروتوكولين لتأمين حزم IP: رأس المصادقة (AH) وتغليف حمولة الأمان (ESP). يوفر الأول سلامة البيانات وخدمات مكافحة إعادة التشغيل ، بينما يقوم الأخير بتشفير البيانات والمصادقة عليها.

فهرس المقال

* [ما هو IPSEC؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#___IPSEC_)
* [كيف يعمل IPsec؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#_____IPsec_)
* [لماذا تختار IPSEC VPN بدلاً من OpenSSL؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#______IPSEC_VPN_____OpenSSL_)
* [ما الذي يمثله IPSEC وماذا يفعل؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#_______IPSEC______)
* [ما هي المنافذ التي يعمل بها IPSEC؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#______________IPSEC_)
* [ما هو ISAKMP؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#___ISAKMP_)
* [ما المقصود بـ ESP و AH؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#_______ESP__AH_)
  + [تغليف بروتوكول الأمان](https://www.thra3.com/2021/11/what-is-IPSEC.html#___________)
  + [رأس المصادقة (Authentication Header)](https://www.thra3.com/2021/11/what-is-IPSEC.html#_______Authentication_Header_)
* [هل شبكة VPN IPSEC مناسبة لي؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#____VPN_IPSEC______)
* [ما الفرق بين وضع نفق IPsec ووضع النقل IPsec؟](https://www.thra3.com/2021/11/what-is-IPSEC.html#___________IPsec______IPsec_)

## ما هو IPSEC؟

في عالم [**الشبكات الافتراضية الخاصة VPN**](https://www.thra3.com/2021/11/what-is-vpn.html) ، يوجد عادةً نوعان يمكن للمؤسسة الاختيار من بينهما ... IPSEC أو OpenSSL. على الرغم من انتقال العديد من الأشخاص إلى وضع OpenSSL نظرًا لسهولة النشر النسبية الجديدة ، لا تزال هناك شركات تقوم بنشر الشبكات الظاهرية الخاصة القائمة على IPSEC بسبب طبقات الأمان الإضافية التي توفرها والتي لا تتوفر في شبكات VPN المستندة إلى OpenSSL.

إقرأ أيضا: [كل ماتحتاج معرفته عن التخزين السحابي Cloud Storage وأهميته للاعمال والشركات](https://www.thra3.com/2024/03/everything-about-cloud-storage.html).

IPsec عبارة عن مجموعة من البروتوكولات المستخدمة معًا لإعداد اتصالات مشفرة بين الأجهزة. يساعد في الحفاظ على البيانات المرسلة عبر الشبكات العامة آمنة. غالبًا ما يتم استخدام IPsec لإعداد شبكات VPN ، وهو يعمل عن طريق تشفير حزم IP ، جنبًا إلى جنب مع مصادقة المصدر الذي تأتي منه الحزم.

ضمن المصطلح "IPsec" ، تشير "IP" إلى "بروتوكول الإنترنت" و "ثانية" تعني "آمن". بروتوكول الإنترنت هو بروتوكول التوجيه الرئيسي المستخدم على الإنترنت ؛ يحدد أين ستذهب البيانات باستخدام عناوين IP. IPsec آمن لأنه يضيف التشفير \* والمصادقة إلى هذه العملية.

\* التشفير هو عملية إخفاء المعلومات عن طريق تعديل البيانات رياضيًا بحيث تظهر عشوائية. بعبارات أبسط ، التشفير هو استخدام "رمز سري" لا يمكن تفسيره إلا من قبل الأطراف المصرح لهم.

## كيف يعمل IPsec؟

تتضمن اتصالات IPsec الخطوات التالية:

**تبادل المفاتيح:** المفاتيح ضرورية للتشفير؛ المفتاح عبارة عن سلسلة من الأحرف العشوائية التي يمكن استخدامها "لقفل" (تشفير) و "إلغاء تأمين" (فك تشفير) الرسائل. يقوم IPsec بإعداد المفاتيح مع تبادل المفاتيح بين الأجهزة المتصلة ، بحيث يمكن لكل جهاز فك تشفير رسائل الجهاز الآخر.

**رؤوس الحزم والمقاطع الدعائية:** يتم تقسيم جميع البيانات التي يتم إرسالها عبر الشبكة إلى أجزاء أصغر تسمى الحزم. تحتوي الحزم على حمولة أو بيانات فعلية يتم إرسالها ورؤوس أو معلومات حول تلك البيانات حتى تعرف أجهزة الكمبيوتر التي تتلقى الحزم ما يجب فعله بها. يضيف IPsec عدة رؤوس إلى حزم البيانات التي تحتوي على معلومات المصادقة والتشفير. يضيف IPsec أيضًا مقطورات ، والتي تتبع حمولة كل حزمة بدلاً من قبل.

**المصادقة:** يوفر IPsec مصادقة لكل حزمة ، مثل ختم المصادقة على عنصر قابل للتحصيل. هذا يضمن أن الحزم من مصدر موثوق وليست مهاجمًا.

**التشفير:** تقوم IPsec بتشفير الحمولات داخل كل حزمة ورأس IP لكل حزمة (ما لم يتم استخدام وضع النقل بدلاً من وضع النفق - انظر أدناه). هذا يحافظ على البيانات المرسلة عبر IPsec آمنة وخاصة.

**الإرسال:** تنتقل حزم IPsec المشفرة عبر شبكة واحدة أو أكثر إلى وجهتها باستخدام بروتوكول النقل. في هذه المرحلة ، تختلف حركة مرور IPsec عن حركة مرور IP العادية من حيث أنها تستخدم UDP في أغلب الأحيان كبروتوكول نقل خاص بها ، بدلاً من TCP. يُنشئ بروتوكول التحكم في الإرسال TCP اتصالات مخصصة بين الأجهزة ويضمن وصول جميع الحزم. UDP ، بروتوكول مخطط بيانات المستخدم ، لا يقوم بإعداد هذه الاتصالات المخصصة. يستخدم IPsec بروتوكول UDP لأن هذا يسمح لحزم IPsec بالوصول عبر جدران الحماية.

**فك التشفير:** في الطرف الآخر من الاتصال ، يتم فك تشفير الحزم ، ويمكن للتطبيقات (مثل المتصفح) الآن استخدام البيانات التي تم تسليمها.

## لماذا تختار IPSEC VPN بدلاً من OpenSSL؟

في حين أن الشبكات الافتراضية الخاصة القائمة على SSL (**SSL-based VPNs**) لديها مجموعة خاصة بها من ميزات وضع الأمان ، فإن شبكات VPN من IPSEC تأخذها إلى المستوى التالي وتوفر وسائل قوية لضمان أمان البيانات التي يتم نقلها والتي لا تتوفر في شبكات VPN المستندة إلى SSL.

## ما الذي يمثله IPSEC وماذا يفعل؟

IPSEC لتقف على أمان IP. إنها مجموعة بروتوكولات قياسية لفريق هندسة الإنترنت (IETF) بين نقطتي اتصال عبر شبكة IP التي توفر مصادقة البيانات وسلامتها وسريتها. كما تحدد الحزم المشفرة والمفكوكة والمصادقة عليها. يتم تحديد بروتوكولات IPSEC اللازمة لتبادل المفاتيح الآمن وإدارة المفاتيح فيه.

## ما هي المنافذ التي يعمل بها IPSEC؟

يجب فتح منفذ UDP 500 كما يجب فتح بروتوكولي IP 50 و 51. يجب فتح منفذ UDP 500 للسماح بإعادة توجيه ISAKMP عبر جدار الحماية بينما يسمح البروتوكولين 50 و 51 بإعادة توجيه حركة مرور ESP و AH على التوالي.

## ما هو ISAKMP؟

ISAKMP تعني ارتباط أمان الإنترنت وبروتوكول إدارة المفاتيح. هذان مكونان رئيسيان لشبكة IPSEC VPN التي يجب أن تكون في مكانها حتى تعمل بشكل طبيعي وتحمي حركة المرور العامة التي يتم إعادة توجيهها بين العميل وخادم VPN أو خادم VPN إلى خادم VPN.

## ما المقصود بـ ESP و AH؟

لا ، ESP ليس تصورًا فوق حسي! يرمز ESP إلى Encapsulating Security Protocol و AH لتقف على رأس المصادقة.

### تغليف بروتوكول الأمان

يوفر ESP الحماية لبروتوكولات الطبقة العليا الجديدة ، مع منطقة موقعة تشير إلى مكان توقيع حزمة البيانات المحمية من أجل التكامل ، ومنطقة مشفرة تشير إلى المعلومات المحمية بسرية. ما لم تكن حزمة البيانات قيد الأنفاق ، فإن ESP يحمي فقط حمولة بيانات IP (ومن هنا جاء الاسم) ، وليس عنوان IP.

يمكن استخدام ESP لضمان السرية ، ومصادقة أصول البيانات ، والسلامة غير المتصلة ، ودرجة معينة من السرية على مستوى حركة المرور ، وخدمة منع إعادة التشغيل (شكل من أشكال تكامل التسلسل الجزئي الذي يحمي من استخدام الأوامر أو بيانات الاعتماد التي تم تم الاستيلاء عليها من خلال استنشاق كلمات المرور أو هجمات مماثلة) .3

### رأس المصادقة (Authentication Header)

رأس المصادقة (AH) هو بروتوكول جديد وجزء من مجموعة بروتوكولات أمان بروتوكول الإنترنت (IPsec) ، والتي تصادق على أصل حزم IP (مخططات البيانات) وتضمن سلامة البيانات. يؤكد AH المصدر الأصلي للحزمة ويضمن أن محتوياتها (كل من الرأس والحمولة) لم تتغير منذ الإرسال.

إذا تم إنشاء اقترانات أمنية ، يمكن تكوين AH اختياريًا للدفاع ضد هجمات إعادة التشغيل باستخدام تقنية النافذة المنزلقة.

كيف يعملون معًا؟

عند تكوينها بشكل صحيح ، توفر IPSEC VPN طبقات متعددة من الأمان تضمن وضع الأمان وسلامة البيانات التي يتم إرسالها عبر النفق المشفر. بهذه الطريقة يمكن للمؤسسة أن تشعر بالثقة من أنه لم يتم اعتراض البيانات وتعديلها أثناء النقل وأنه يمكنها الاعتماد على ما تشاهده.

**هل شبكة VPN IPSEC مناسبة لي؟**

يعتمد ذلك حقًا على ما تحاول تحقيقه بالإضافة إلى عناصر التحكم في الأمان والخصوصية الموجودة لديك داخل مؤسستك. بينما توفر شبكات VPN الخاصة بـ OpenSSL قدرًا كبيرًا من الأمان ، إلا أن هناك جوانب لا يمكن لشبكة IPSEC VPN توفيرها ببساطة.

**ما الفرق بين وضع نفق IPsec ووضع النقل IPsec؟**

يتم استخدام وضع نفق IPsec بين جهازي توجيه مخصصين ، حيث يعمل كل جهاز توجيه كنهاية واحدة لـ "نفق" افتراضي عبر شبكة عامة. في وضع نفق IPsec ، يتم تشفير عنوان IP الأصلي الذي يحتوي على الوجهة النهائية للحزمة ، بالإضافة إلى حمولة الحزمة. لإخبار أجهزة التوجيه الوسيطة بمكان إعادة توجيه الحزم ، يضيف IPsec رأس IP جديدًا. في كل نهاية النفق ، تقوم أجهزة التوجيه بفك تشفير رؤوس IP لتسليم الحزم إلى وجهاتها.

في وضع النقل ، يتم تشفير الحمولة لكل حزمة ، ولكن لا يتم تشفير عنوان IP الأصلي. وبالتالي ، فإن أجهزة التوجيه الوسيطة قادرة على عرض الوجهة النهائية لكل حزمة - ما لم يتم استخدام بروتوكول نفق منفصل (مثل GRE).

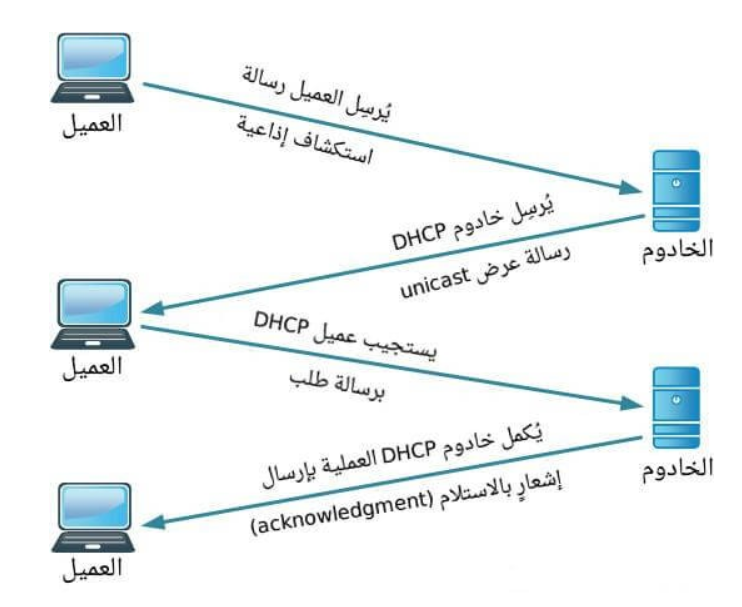
# استعمال موجه سيسكو (Cisco router) كخادوم DHCP عند بناء الشبكات

**فهم بروتوكول DHCP**

بروتوكول ضبط المضيف الديناميكي، أو ما يُعرَف اختصارًا بالاسم DHCP، هو برنامج من نمط عميل-خادوم يؤتمت عملية إسناد عنوان IP ومحلقاتها إلى أجهزة العملاء؛ أي أنَّ العملاء سيتصلون بالشبكة دون معلومات IP ثم سيطلبونها من خادوم DHCP.

المعلومات التي يوفرها خادوم DHCP تتراوح بين عنوان IP المطلوب والبوابة الافتراضية وقناع الشبكة الفرعية إلى خواديم DNS وخواديم أسماء NetBIOS وغيرها من المعلومات المخصصة مثل خواديم TFTP و SIP.

المعايير المُعرَّفة في RFC تتضمن مُعرِّفات الشبكات المحلية الوهمية (VLAN IDs) ومعاملات جودة الخدمة (QoS). يمكن أن يعمل البروتوكول بنمط «التأجير» (lease model) الذي تستأجر فيه الأجهزة المعاملات الخاصة بها التي يمكن أن تُستعمل من الأجهزة الأخرى إن لم يعد الجهاز الأصلي متوفرًا على الشبكة؛ تُستأجر تلك المعاملات بناءً على وقتٍ مُحدَّد، الذي يمكن أن يُعرَّف ويختلف لمجموعةٍ من عناوين IP أو لمجموعةٍ من الأجهزة؛ ويمكنك أيضًا إسناد عناوين ثابتة لأجهزة معيّنة. لنشرح الآن عمل DHCP بمزيدٍ من التفصيل.



في الشكل أعلاه، لدينا عميل يطلب عنوان IP من الخادوم (قد يبدو لك من الرسم أنَّ لدينا ثلاثة عملاء وخادومَين، لكن هذا لأغراضٍ توضيحيةٍ فقط، إذ نتحدث عن نفس العميل ونفس الخادوم هنا)، وأول ما علينا ملاحظته أنَّ تلك الرسائل هي رسائل إذاعيّة محليّة، لأن العملاء لا يعرفون الشبكة الفرعية، لأنهم لا يملكون عنوان IP وبالتالي لا يعرف الخادوم أين سيُرسِل البيانات.

سيُرسِل العملاء رسالة طلب (request massage)، وقد يرى الرسالة أكثر من خادوم، ولهذا السبب سنحتاج إلى أربع خطوات لإتمام هذه العملية. ستُجيب الخواديم برسالة عرض (offer massage)، وهي رسالة إذاعة محليّة لأن العميل لا يملك عنوان IP محلي؛ وهي رسالة إذاعية في الطبقة الثالثة، لكن عندما يُرسِل العميل رسالة الاستكشاف (discover massage)، فسيعلم عنوان MAC للعميل، ثم سيُرسِل رسالة unicast لاحقًا لأن الخادوم سيرسل المعلومات مباشرةً إلى عنوان MAC للعميل.

بعد رسالة الاستكشاف (discover)، قد يجيب أكثر من خادوم برسالة عرض (offer)، لذا على العميل اتخاذ القرار بأيّة معلومات عليه أخذها؛ لذلك سيُجيب برسالة طلب (request) مُقرِّرًا أي خادوم سيأخذ منه المعلومات. تُضمِّن رسائل العرض عناوين IP بجانب معاملات أخرى مثل البوابات الافتراضية، ووقت التأجير، ووقت انتهاء الصلاحية ...إلخ. في النهاية، سيقول الخادوم الذي تم اختياره: «حسنًا، لقد وصلني طلبك، وهذه هي المعلومات؛ وسنبدأ الآن وقت الإيجار، فأنت المالك المؤقت للعنوان»؛ وهذا هو إشعار الاستلام (acknowledgment message)، إذ سيراها العميل وسيبدأ عمله.

عليك الانتباه أنَّك إذا وضعت موجِّهًا بين الخادم والعميل، فلن تمر الرسائل الإذاعية المحلية؛ إذ أنَّ الموجِّهات لا تمررها؛ وعليك ضبط الموجِّه ليسمح بمرور تلك الرسائل، وإذا كنت ستضبط موجِّه سيسكو كخادوم DHCP، فعليه أولًا أن يدعم DHCP.

**إسناد العناوين في DHCP**

توفير عنوان IP للعميل هي أهم مهمة يُجريها بروتوكول ضبط المضيف؛ ومع ذاك العنوان، نحصل على معلومات حول القطع الشبكيّة، والبوابة الافتراضية، وخودايم DNS، واسم النطاق، وخواديم TFTP (المهمة في الاتصالات الهاتفية عبر IP) وهلم جرًا. ولكي يكون ضبط العناوين مرنًا لمختلف أنواع العملاء، فيُضمِّن معيار DHCP ثلاث آليات مختلفة لحجز العناوين.

* **الحجز اليدوي (Manual Allocation):** ويُعرَف أيضًا بالمصطلح «الحجز» (**reservation**). إذا يُحجَز عنوان IP معيّن مسبقًا إلى جهازٍ مُحدَّد من مدير الشبكة؛ ويُسنِد خادوم DHCP عنوان IP المعيّن إلى ذاك الجهاز فقط، إذ يُربَط عنوان IP إلى عنوان MAC للجهاز.
* **الحجز التلقائي (Automatic Allocation):** يُسنِد خادوم DHCP عنوان IP بشكلٍ دائمٍ إلى جهازٍ ما؛ ويختار الخادومُ العنوانَ من مجموعةٍ (تسمى بالمصطلح pool) من العناوين المتوفرة.
* **الحجز الديناميكي (Dynamic Allocation):** يُسنِد خادوم DHCP عنوان IP من مجموعة من العناوين لوقتٍ محدود ضُبِطَت قيمته في الخادوم، أو إلى أن يُخبِرَ العميلُ خادومَ DHCP أنَّ لم يعد بحاجةٍ إلى العنوان (كما لو نفذنا الأمر ipconfig /release في نظام ويندوز).

**استخدام الموجه كخادوم DHCP**

خدمة DHCP هي خدمة محورية ومهمة، ويمكن لنظام تشغيل سيسكو IOS للموجِّهات أن يكون خادوم DHCP بكامل الميزات. العديد من المعاملات والخيارات المُعرَّفة في RFC موجودة ومتوفرة في موجِّهات IOS. ومن المهم أن يستطيع الموجِّه توفير تلك الخدمة، لأنه موجود دائمًا في الشبكة، فيمكنه أن يوفِّر ذاك النوع من الخدمات دون الحاجة إلى ضبط خادوم كامل لذلك. إذ تستفيد المكاتب الفرعية والمكاتب الصغيرة من إمكانية تشغيل هذه الخدمة في عنصر من عناصر الشبكة.

هذه الخدمة هي خدمة برمجية، ويمكن أن تُضبَط ضبطًا كاملًا في موجِّهك لعدِّة بطاقات شبكيّة، ولعدة مجالات من العناوين، وتدعم هذه الخدمة أيضًا حجز العناوين يدويًا.

**الأوامر والضبط**

هذا مثال ضبطٍ عن كيفية إعداد مجموعة عناوين (pool) في خدمة DHCP في موجِّه سيسكو:

|  |
| --- |
| RouterX(config)#ip dhcp pool Marketing  RouterX(dhcp-config)#network 10.123.1.0 255.255.255.0  RouterX(dhcp-config)#default-router 10.123.1.1  RouterX(dhcp-config)#domain-name learncisco.net  RouterX(dhcp-config)#dns-server 172.16.4.10 172.16.4.12 |

هنالك أوامرٌ متوفرة لمساعدتك في مراقبة واستكشاف أخطاء تلك الخدمة.

|  |
| --- |
| RouterX#show ip dhcp pool Marketing  Pool Marketing :  Utilization mark (high/low) : 100 / 0  Subnet size (first/next) : 0 / 0  Total addresses : 254  Leased addresses : 0  Pending event : none  1 subnet is currently in the pool :  Current index IP address range Leased addresses  10.123.1.1 10.123.1.1 - 10.123.1.254 0  RouterX#  Router#sh ip dhcp conflict  IP address Detection method Detection time VRF  192.168.200.58 Gratuitous ARP May 28 2012 03:31 PM  192.168.200.59 Gratuitous ARP May 28 2012 03:31 PM  192.168.200.64 Gratuitous ARP May 28 2012 03:39 PM |

يُساعِدك آخر أمر (sh ip dhcp conflict) في التعرف على التضاربات في إسناد عناوين IP التي يتم العثور عليها من خواديم DHCP ومن العملاء. ويحدث التضارب في العناوين عندما يحاول خادوم أن يُسنِد عنوان IP، فيجد الخادوم أو العميل أنَّ هنالك أجهزة أخرى على الشبكة لها نفس العنوان. وستحاول الخواديم عميل ping لعناوين IP المُؤجَّرة قبل إسناد تلك العناوين لأجهزةٍ أخرى لتفادي حدوث تضاربات، وسيستعمل العملاء «gratuitous ARP» للعثور على جميع العملاء الذين يملكون نفس عنوان IP؛ إن حدث تضارب في العناوين، فسيُحذَف العنوان من مجموعة العناوين المتوفرة (pool)، ولن يُعاد إسناده حتى يحل مدير الشبكة التضارب. هذه الميزات تجعل من خادوم DHCP في موجِّهات سيسكو العاملة بنظام تشغيل IOS أداةً فعالةً جدًا.

DHCP Client

no ip dhcp use vrf connectedip dhcp excluded-address 10.1.10.252 10.1.10.254ip dhcp excluded-address 10.1.20.252 10.1.20.254ip dhcp excluded-address 10.1.30.252 10.1.30.254!ip dhcp pool

OFFICE   network 10.1.10.0 255.255.255.0   default-router 10.1.10.254!ip dhcp pool VOICE   network 10.1.20.0 255.255.255.0   default-router 10.1.20.254!ip dhcp pool GUEST   network 10.1.30.0 255.255.255.0   default-router 10.1.30.254

**DHCP Server Configuration**

|  |
| --- |
| R1(config)#no ip dhcp use vrf connected  R1(config)#ip dhcp excluded-address 10.1.10.252 10.1.10.254  R1(config)#ip dhcp excluded-address 10.1.20.252 10.1.20.254  R1(config)#ip dhcp excluded-address 10.1.30.252 10.1.30.254  !  R1(config)#ip dhcp pool OFFICE  R1(dhcp-config)# network 10.1.10.0 255.255.255.0  R1(dhcp-config)# default-router 10.1.10.254  !  R1(config)#ip dhcp pool VOICE  R1(dhcp-config)# network 10.1.20.0 255.255.255.0   R1(dhcp-config)#default-router 10.1.20.254  !  R1(config)#ip dhcp pool GUEST  R1(dhcp-config)# network 10.1.30.0 255.255.255.0  R1(dhcp-config)# default-router 10.1.30.254 |

**Host Config**

|  |
| --- |
| R1(config)# int fa0/0  R1(config- if) # ip dhcp clientclient-id fa0/0  R1(config- if) # ip dhcp client host R1  R1(config-if) # ip address dhcp |

**Steps to configure DHCP server through CLI.**

|  |
| --- |
| 1. Login to the device using SSH / TELNET and go to enable mode. 2. Go into the config mode. Router#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# 3. Exclude IP addresses from being assigned by DHCP by using the ip dhcp excluded-address FIRST\_IP LAST\_IP Router(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.50 Router(config)# 4. Create a new DHCP pool with the ip dhcp pool NAME command Router(config)#**ip dhcp pool Floor1DHCP** Router(dhcp-config)# 5. Define a subnet that will be used to assign IP addresses to hosts with the network SUBNET SUBNET\_MASK command. Router(dhcp-config)#**network 192.168.0.0 255.255.255.0** Router(dhcp-config)# 6. Define the default gateway with the default-router IP command Router(dhcp-config)#**default-router 192.168.0.1** Router(dhcp-config)# 7. Define the DNS server with the dns-server IP address command. Router(dhcp-config)#**dns-server 192.168.0.1** Router(dhcp-config)# 8. Return to privilege config mode Router(dhcp-config)#**exit** Router(config)# 9. Enable DHCP server on the interface using service dhcp interface-type number command Router(config)#**service dhcp vlan1** Router(config)# 10. Exit config mode Router(config)#**exit** Router# 11. To view information about the currently leased addresses, you can use the show ip dhcp binding command Router#**show ip dhcp binding** IP address Client-ID/ Lease expiration Type Hardware address 192.168.0.51 0060.5C2B.3DCC -- Automatic   In the output above you can see that there is a single DHCP client that was assigned the IP address of 192.168.0.51. Since we’ve excluded the IP addresses from the 192.168.0.1 – 192.168.0.50 range, the device got the first address available – 192.168.0.51.   1. To display information about the configured DHCP pools, you can use the show ip dhcp pool command Router#show ip dhcp pool Pool Floor1DHCP : Utilization mark (high/low) : 100 / 0 Subnet size (first/next) : 0 / 0 Total addresses : 254 Leased addresses : 1 Excluded addresses : 1 Pending event : none  1 subnet is currently in the pool Current index IP address range Leased/Excluded/Total 192.168.0.1 192.168.0.1 - 192.168.0.254 1 / 1 / 254   This command displays some important information about the DHCP pool(s) configured on the device – the pool name, total number of IP addresses, the number of leased and excluded addresses, subnet’s IP range, etc.   1. Copy the running configuration into startup configuration using below command Router#write memory Building configuration... [OK] Router# |

المراجع

<https://ipcisco.com/lesson/dns-configuration-on-cisco-routers/>

<https://www.firewall.cx/cisco/cisco-routers/cisco-router-site-to-site-ipsec-vpn.html>

<https://learningnetwork.cisco.com/s/question/0D53i00000Kt7TpCAJ/dhcp-client-in-gns3>

<https://www.manageengine.com/network-configuration-manager/configlets/configure-dhcp-server-cisco.html>

<https://www.thra3.com/2021/11/what-is-IPSEC.html>