# SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

GERMAN EDUARDO CASTRO ESTRADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
MARIQUITA, TOLIMA
2021

# SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

GERMAN EDUARDO CASTRO ESTRADA

Diplomado de opción de grado presentado para optar el título de INGENIERO DE SISTEMAS

DIRECTOR:
MSc. RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE SISTEMAS
MARIQUITA, TOLIMA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

MARIQUITA, 27 DE NOVIEMBRE DEL 2021

## AGRADECIMIENTOS

Agradezco a dios primeramente y a mi familia por el apoyo incondicional durante este largo proceso de aprendizaje, el cual estoy próximo al culminar, con muchos sinsabores, esfuerzos y lucha en todos los aspectos tanto académicos como personales

**CONTENIDO**

## LISTA DE TABLAS

## LISTA DE FIGURAS

## GLOSARIO

Router: Dispositivo de internetworking que conecta hosts en diferentes redes

Switch: Dispositivo de la capa 2 que conecta hosts en la misma red.

Consola: Terminal para ejecutar comandos en los dispositivos

Vty: Línea de terminal virtual de telnet para acceso remoto al dispositivo

Ssh: Secure Shell es un protocolo que proporciona acceso remoto seguro a los dispositivos de red, encriptando los mensajes

Motd banner: comando para configurar el mensaje del día

Cifrado rsa: Cifrado de encriptamiento propuesto por la compañía rsa y cisco

Svi: interfaz virtual del Switch para acceso remoto del dispositivo

Gateway: Puerta de salida de red, así se le llama al router

Dns: sistema de nombre mde dominio

Telnet: protocolo de red para acceder de forma remota a un dispositivo

Loopback: La interfaz loopback es una interfaz lógica interna del router. Se la considera una interfaz de software que se coloca automáticamente en estado UP (activo), siempre que el router esté en funcionamiento.

Enlace Troncal: enlace punto a punto entre dos dispositivos que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

Vlan: virtual lan, es un método para crear redes lógicas independientes dentro de una misma red física.

Ospf: primero la ruta libre mas corta, autenticación de origen de la ruta, convergencia rápida, funciona dividiendo una intranet en unidades jerárquicas de menor tamaño enlazándose con un área de backbone mediante un border router.

Nat: permite acceder a internet traduciendo las direcciones privadas en direcciones ip registradas

Dhcp: permite a los dispositivos de redes obtener una dirección ip, mascara y puerta de enlace, cuando se conectan a la red

Ntp: protocolo de tiempo de red, permite a los routers sincronizar sus configuracines de tiempo con un servidor para tener  desempeños más confiables.

Acl: sirven para filtrar el tráfico por parte de los routers, para una mejor administración y control de flujo por sus interfaces.

## RESUMEN

Se desarrollan dos escenarios en los cuales hay redes para configurarlas bajo diferentes parámetros y comprobar varios aspectos, como la conectividad el funcionamiento de varios dispositivos de internetworking, el uso de diferentes protocolos de red, Se conforma estas redes LAN con dispositivos de internetworking como router, switch, servidores, hosts.

Se asignan direcciones ip a las interfaces de los dispositivos haciendo el subneting propuesto en la guia, se cifran el acceso a los mismos mediante protocolo ssh.

También se activan las diferentes interfaces mediante el comando no shutdown.

Se da seguridad alas diferentes consolas mediante contraseñas, se establece una clave segura con un minimos de 10 caracteres

Se trabaja con las líneas vty para usarlas en la base de datos local, también se configura para que solo acepten protocolo ssh en el caso del router

Se establece un nombre de un dominio y un acceso a una base de datos local mediante usuario, también se configura las líneas virtuales telnet en el caso del Switch.

También se configura un mensaje de aviso en el router y switch y se cifran también con claves rsa.

Se configuran los computadores y se hacen pruebas de conectividad entre los dieferentes dispositivos de la red.

En general se dan todos los parámetros de configuración a los dispositivos de dos redes LAN para una comunicación eficaz y segura, obteniendo como resultado una red óptima para intercambio de información.

En el segundo escenario se configuran los dispositivos con sus parámetros básicos, se configurarn las interfaces y posteriormente se activan, se establece una loopback a un servidor web simulado en el router 2.

En el router 3 se establecen unas loopbacks.

Se configura un enlace troncal entre el switch 1 y 3 y entre el switch 1 y router 1

Se asignan diferentes subinterfaces a las vlan en el router 1

Se abordan temáticas de seguridad en los Switch, en los routers propuestos, configuracion de las VLAN, establecimiento del protocolo OSPF, configuración al router 1, como servidor DHCP, traducción de redes estáticas y dinámicas NAT y asignación de un rango, listas de control de acceso ACL como permitir el acceso de una red en este caso líneas vty del router 2 y denegar otras redes,el protocolo

de tiempo de red NTP como configurar un router master y uno cliente ajustándole la hora.

Se registran los diferentes comandos en la CLI respectiva de los dispositivos para comparar y verificar las configuraciones respectivas.

Obteniendo unas redes LAN seguras, optimas en su desempeño, capaces de brindar la mayor capacidad de servicio a las empresas que las diseñan y las implantan.

Palabras clave: switch, vlan, ospf, dhcp,cisco

## ABSTRACT

Two scenarios are developed in which there are networks to configure them under different parameters and check various aspects, such as connectivity, the operation of various internetworking devices, the use of different network protocols, these LAN networks are formed with internetworking devices such as a router, switch, servers, hosts.

IP addresses are assigned to the interfaces of the devices by doing the subnetting proposed in the guide, access to them is encrypted using the ssh protocol.

The different interfaces are also activated using the no shutdown command.

The different consoles are given security by means of passwords, a secure key is established with a minimum of 10 characters

It works with the vty lines to use them in the local database, it is also configured so that they only accept ssh protocol in the case of the router

A domain name and access to a local database by user is established, virtual telnet lines are also configured in the case of the Switch.

A warning message is also configured on the router and switch and they are also encrypted with rsa keys.

Computers are configured and connectivity tests are made between the different devices on the network.

In general, all the configuration parameters are given to the devices of two LAN networks for an efficient and secure communication, obtaining as a result an optimal network for information exchange.

In the second scenario, the devices are configured with their basic parameters, the interfaces are configured and later activated, a loopback is established to a simulated web server on router 2.

Loopbacks are established on router 3.

A trunk link is configured between switch 1 and 3 and between switch 1 and router 1

Different subinterfaces are assigned to vlan's on router 1

Security issues are addressed in the Switches, in the proposed routers, VLAN configuration, establishment of the OSPF protocol, configuration to router 1, such as DHCP server, translation of static and dynamic NAT networks and assignment of a range, control lists of ACL access such as allowing access to a network in this case vty lines from router 2 and denying other networks, the NTP network time protocol such as configuring a master router and a client router setting the time.

The different commands are registered in the respective CLI of the devices to compare and verify the respective configurations.

Obtaining secure LAN networks, optimal in their performance, capable of providing the highest service capacity to the companies that design and implement them.

Keywords: switch, vlan, ospf, dhcp, cisco

## INTRODUCCION

El planteamiento de este proyecto es tener las habilidades para configurar los dispositivos de internetworking.

Conocer los comandos de consola necesarios para establecer contraseñas, cifrar las mismas, establecer nombres de dominio, acceso a una DB local mediante usuario, configurar la vlan del switch y utilizar claves seguras rsa.

El proyecto tiene como objetivos adquirir las competencias para configurar una red LAN haciendo subnetting, dando nombre de dominio, asignando direcciones ip a los diferentes dispositivos de internetworking como lo son el router, switch, y los hosts.

Cifrando líneas seguras con protocolo ssh, y dando uso de claves cifradas rsa, entre otros.

En el segundo escenario se abordan temas de configuración de los switch, routers, servidores, configuración de las Vlan en el switchpara su uso en dispositivos de capa 3, uso de protocolos OSPF, DHCP, traducción de redes estáticas y dinámicas NAT, las listas de control de acceso. El protocolo de tiempo de red, NAT.

Todas estas configuraciones se hicieron en los diferentes CLI de los equipos de internetworking.

El objetivo de esta temática es adentrarnos en el mundo del routing y tener las capacidades de poder configuar estos dispositivos y crear redes seguras, modulares, flexibles para un alto desempecho en la transmisión de datos en las empresas donde estén diseñadas y montadas.

## DESARROLLO

1. Escenario 1

Figura 1 Escenario propuesto


Fuente: Autor

**Objetivos**
Parte 1: Construir en el simulador la Red
Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1
Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

**Aspectos básicos/situación**
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

**Parte 1: Construya la Red**
En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.
**Parte 2: Desarrolle el esquema de direccionamiento IP**
Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.
Cada estudiante tomará el direccionamiento 192.168.**X**.0 donde X corresponde a los últimos dos dígitos de su cédula.

## Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Dirección de Red:

Tabla 1.subneting

| SUBRED | DESCRIPCION | MASK | #HOSTS | 1º IP VALIDA | ULTIMA IP VALIDA | BROADCAST | #Magico |
|---|---|---|---|---|---|---|---|
| 1 | 192.168.58.0 | /25 | 127 | 192.16858.1 | 192.168.58.126 | 192.168.58.127 | 128 |
| 2 | 192.168.58.128 | /26 | 64 | 192.168.58.129 | 192.168.58.190 | 192.168.58.191 | 64 |
| | 192.168.58.192 | | | | | | |

Fuente: Autor

**Desactivar la búsqueda DNS**

R1(config)#no ip domain-lookup En modo global,desactivo búsqueda dns

R1(config)#

**Nombre del router**

Router(config)#hostname R1 En modo global, doy nombre al router

**Contraseña de acceso a la consola**

R1(config-line)#line console 0 ingreso a línea de consola

R1(config-line)#password ciscoconpass asigno contraseña

R1(config-line)#login habilito la contraseña

**Contraseña cifrada para el modo EXEC privilegiado**

R1(config)#enable secret ciscoenpass asigno contraseña en modo privilegiado

**Nombre de dominio**

R1(config)#ip domain-name ccna-lab.com se asigna nombre al dominio

**Establecer la longitud mínima para las contraseñas**

R1(config)#security passwords min-length 10 En modo global, asigno contraseña
Con 10 bits de seguridad

**Crear un usuario administrativo en la base de datos local**

R1(config)#username admin password admin1pass En modo gobal, creo usuario
admin base de datos local

**Configurar el inicio de sesión en las líneas VTY para que use la base de datos local**

R1(config-line)#line vty 0 4 configuro inicio de sesión líneas vty

R1(config-line)#password ciscocisco se asigna contraseña en base local

R1(config-line)#login local se confirma la contraseña

**Configurar VTY solo aceptando SSH**

R1(config-line)#transport input ssh se asigna modo seguro ssh

**Cifrar las contraseñas de texto no cifrado**

R1(config)#service password-encryption se cifran las contraseñas sin cifrar

**Configure un MOTD Banner**

R1(config)#banner motd #se prohibe el acceso no autorizado# se pone un Banner

**Configurar interfaz G0/0/0**

R1(config)#interfac g0/0/0 se llama a la interface

R1(config-if)#ip address 192.168.58.129 255.255.255.192 se asigna ip

R1(config-if)#no shutdow se sube la interfaz

**Configurar interfaz G0/0/1**

R1(config)#interfac g0/0/1 se llama a la interfaz

R1(config-if)#ip address 192.168.58.1 255.255.255.128 se asigna una ip

R1(config-if)#no shutdown se sube la interfaz

**Generar una clave de cifrado RSA**

R1(config)#ip domain-name ccna-lab.com llamo al dominio

R1(config)#crypto key generate rsa activo clave rsa

How many bits in the modulus [512]: 1024 le confirmo de 1024 bits

**Paso 2. Configurar los equipos**

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**

**Desactivar la búsqueda DNS**.

Switch(config)#no ip domain-lookup se desactiva búsqueda dns

**Nombre del switch**

Switch(config)#hostname S1 en modo global se da nombre al switch

**Nombre de dominio**

Switch(config)# ip domain-name ccna-lab.com se da nombre al dominio

**Contraseña cifrada para el modo EXEC privilegiado**

S1(config)#enable secret ciscoenpass se da contraseña en modo privilegiado

**Contraseña de acceso a la consola**

S1(config)#line console 0 en modo global configuramos acceso a consola

S1(config-line)#password ciscoconpass asignamos contraseña

S1(config-line)#login confirmamos la contraseña

.**Crear un usuario administrativo en la base de datos local**

S1(config)# username admin password admin1pass En modo gobal, creo usuario admin base de datos local

**Configurar el inicio de sesión en las líneas VTY para que use la base de datos local**

L S1(config-line)#line vty 0 15 se configuran líneas vty

S1(config-line)#password ciscocisco se asina contraseña

S1(config-line)#login local se confirma la contraseña

S1(config-line)#

**Configurar las líneas VTY para que acepten únicamente las conexiones SSH**

S1(config-line)#transport input ssh se configura solo protocolo de seguridad

**Cifrar las contraseñas de texto no cifrado**

S1(config)#service password-encryption se cifran las contraseñas

**Configurar un MOTD Banner**

S1(config)#banner motd $Se Prohibe El Acceso No Autorizado$ se configura

S1(config)# banner

**Generar una clave de cifrado RSA**

R1(config)#ip domain-name ccna-lab.com llamanos al dominio

R1(config)#crypto key generate rsa activamos clave rsa

How many bits in the modulus [512]: 1024 le confirmamos clave 1024 bits

**Configurar la interfaz de administración (SVI)**

S1(config-if)#interface vlan 1 configuro interface administracion

S1(config-if)#ip add 192.168.58.2 255.255.255.128 se asina ip

S1(config-if)# no shutdown se sube la interfaz

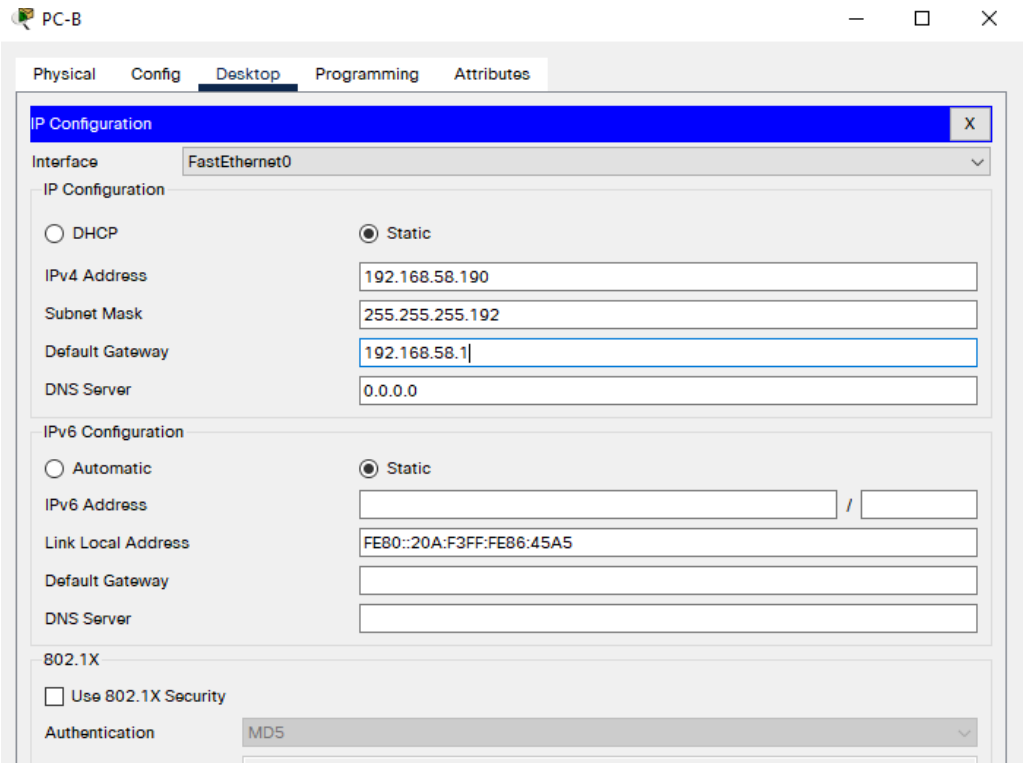
**Configuración del gateway predeterminado**

S1(config)#ip default-gateway 192.168.58.1 se asigna el Gateway

**PC-B Network Configuration**

Configuramos la ip, mascara de subred, y gateway predeterminado en la terminal B

Figura 2.Configurar host B

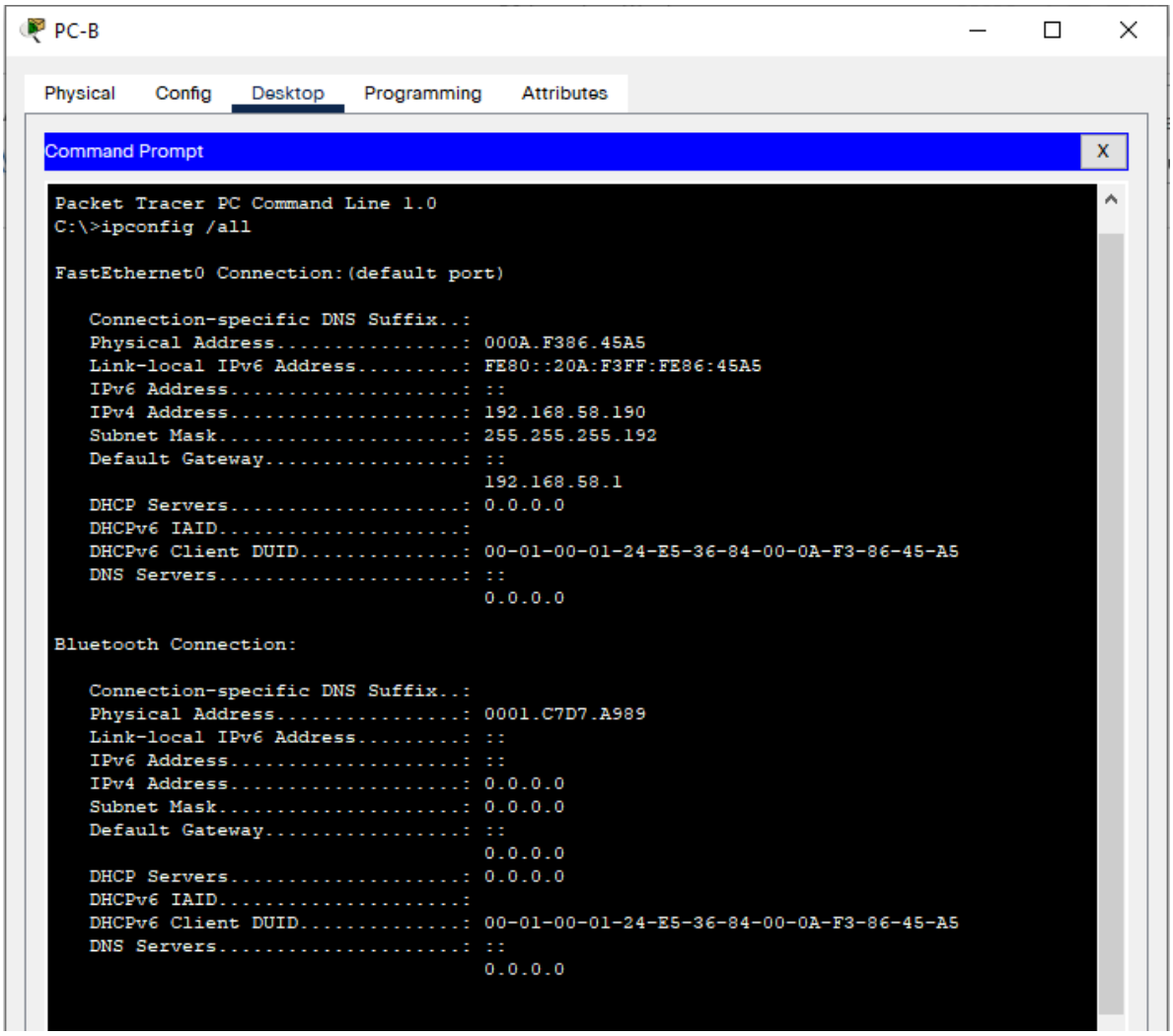



Fuente: Autor

Ipconfig /all.

Vamos a la consola del command prompt y digitamos ipconfig /all

Figura 3.Ipconfig



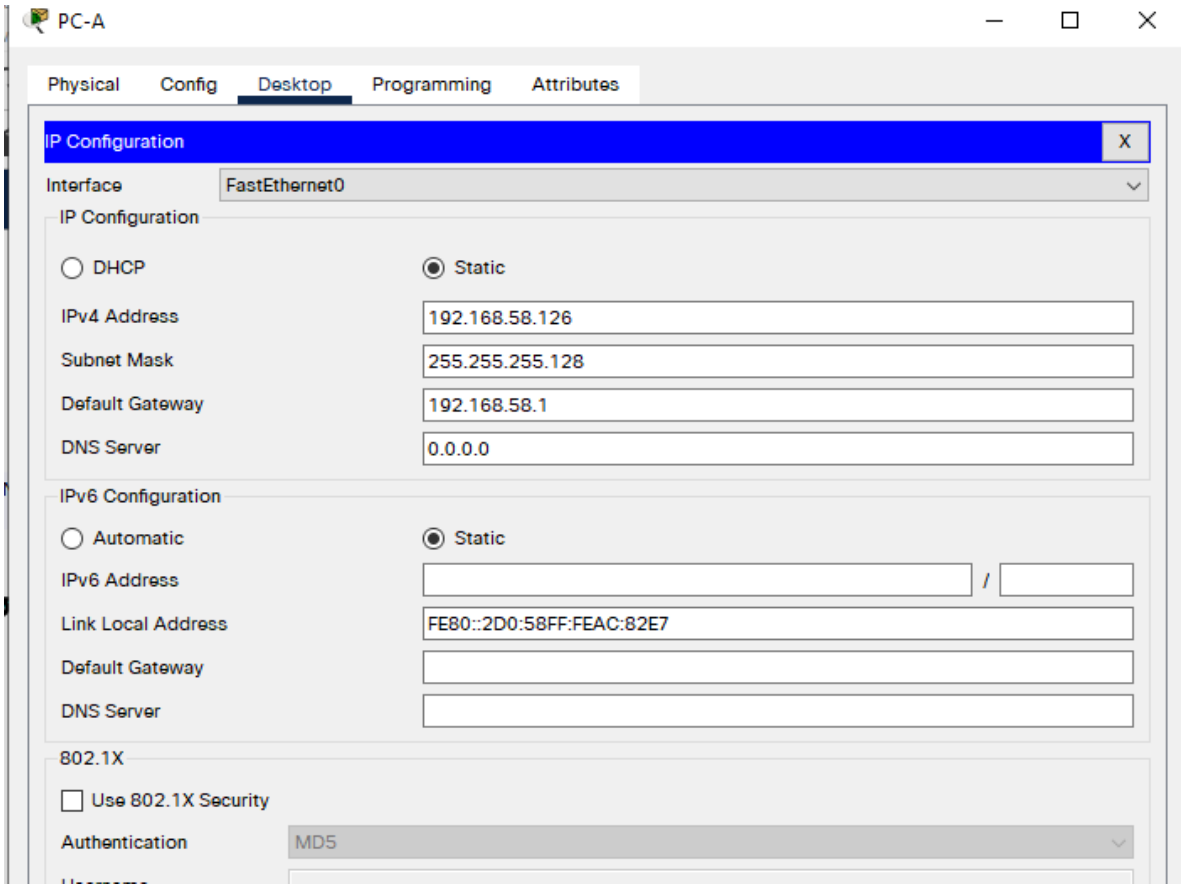

Fuente: Autor

**PC-A Network Configuration**

Configuramos la ip, mascara de subred, y gateway predeterminado en la terminal

A

Figura 4.Configurar host B

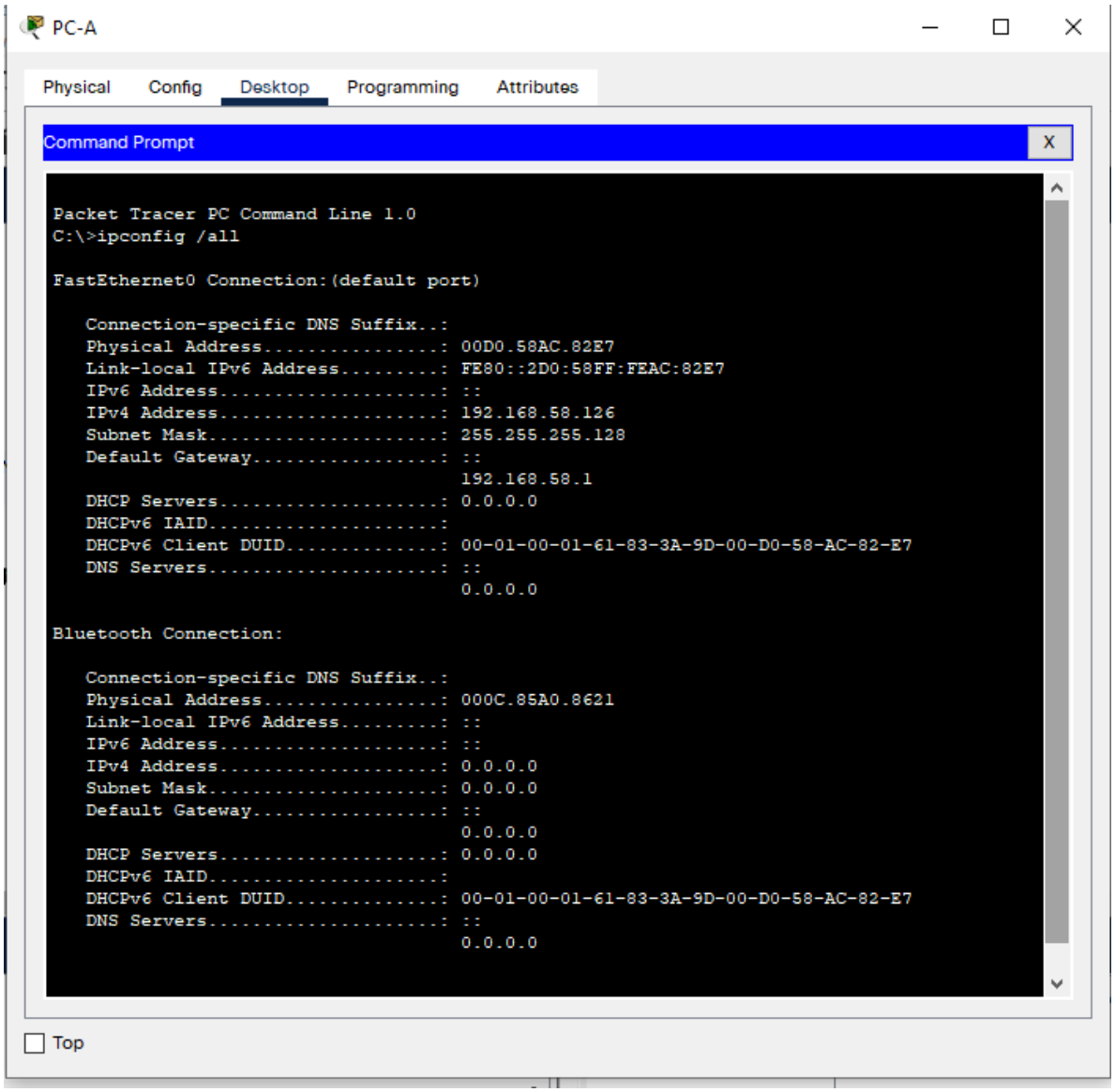



Fuente: Autor

Ipconfig /all.

Vamos a la consola del command prompt y digitamos ipconfig /all

Figura 5.Ipconfig

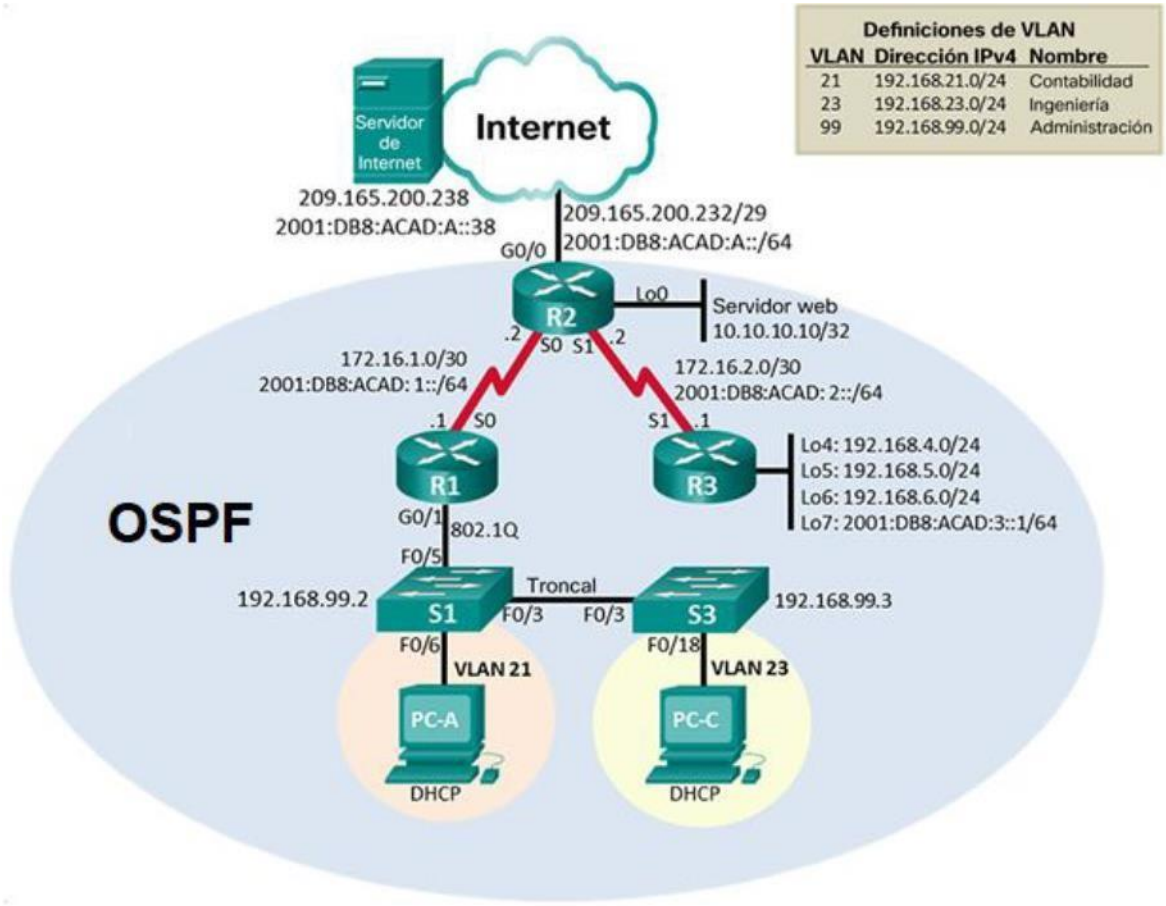



Fuente: Autor

**2.** Escenario 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 6.Escenario propuesto




Fuente: Autor

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

**Para el R11**

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm]

Initializing Hardware ...

Checking for PCIe device presence...done

System integrity status: 0x610

Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE

Copyright (c) 1994-2018 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR4331/K9 platform with 4194304 Kbytes of main memory

no valid BOOT image found

Final autoboot attempt from default boot device...

Located isr4300-universalk9.16.06.04.SPA.bin

############################################################################
############################################################

Package header rev 1 structure detected

**Para el R2**

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm]

Initializing Hardware ...

Checking for PCIe device presence...done

System integrity status: 0x610

Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE

Copyright (c) 1994-2018 by cisco Systems, Inc.

**Para el R1**

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm]

Initializing Hardware ...

Checking for PCIe device presence...done

System integrity status: 0x610

Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE

**Para el R3**

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm]

Initializing Hardware ...

Checking for PCIe device presence...done

System integrity status: 0x610

Rom image verified correctly

System Bootstrap, Version 16.7(3r), RELEASE SOFTWARE

Copyright (c) 1994-2018 by cisco Systems, Inc.

**Para el S1**

Switch#show flash

Directory of flash:/

1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#reload

Proceed with reload? [confirm]

C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

2960-24TT starting...

Base ethernet MAC Address: 00E0.F961.51DA

Xmodem file system is available.

Initializing Flash...

flashfs[0]: 1 files, 0 directories

flashfs[0]: 0 orphaned files, 0 orphaned directories

flashfs[0]: Total bytes: 64016384

flashfs[0]: Bytes used: 4670455

flashfs[0]: Bytes available: 59345929

flashfs[0]: flashfs fsck took 1 seconds.

...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3

Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...

############################################################################ [OK]

Smart Init is enabled

**Para el S2**

Switch#show flash

Directory of flash:/

1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#reload

Proceed with reload? [confirm]

C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

2960-24TT starting...

Base ethernet MAC Address: 00E0.F961.51DA

Xmodem file system is available.

Initializing Flash...

flashfs[0]: 1 files, 0 directories

flashfs[0]: 0 orphaned files, 0 orphaned directories

flashfs[0]: Total bytes: 64016384

flashfs[0]: Bytes used: 4670455

flashfs[0]: Bytes available: 59345929

flashfs[0]: flashfs fsck took 1 seconds.

...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3

Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...

################################################################################ [OK]

Smart Init is enabled

**Para el S3**

Switch#show flash

Directory of flash:/

1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#reload

Proceed with reload? [confirm]

C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

2960-24TT starting...

Base ethernet MAC Address: 00E0.F961.51DA

Xmodem file system is available.

Initializing Flash...

flashfs[0]: 1 files, 0 directories

flashfs[0]: 0 orphaned files, 0 orphaned directories

flashfs[0]: Total bytes: 64016384

flashfs[0]: Bytes used: 4670455

flashfs[0]: Bytes available: 59345929

flashfs[0]: flashfs fsck took 1 seconds.

...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3

Parameter Block Filesystem (pb:) installed, fsid: 4

Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"...

################################################################################ [OK]

Smart Init is enabled

**Configurar R11:**

R11(config)#int G0/0/1 en modo golbal asignamos la interfaz

R11(config-if)#ip address 209.165.200.234 255.255.255.248 asignamos ip

R11(config-if)#no shutdow subimos la interfaz

**Configurar R1**

Nombre del router

Router(config)#hostname R1 en modo global asignamos nombre al R

**Desactivar la búsqueda DNS**

R1(config)#no ip domain-lookup desactivo búsquedas DNS

**Contraseña de exec privilegiado cifrada**

R1(config)#enable secret class habilito contraseña en modo privilegiado

**Contraseña de acceso a la consola**

R1(config-line)#line console 0 accedo a la consola principal

R1(config-line)#password cisco asigno contraseña

R1(config-line)#login confirmo contraseña

**Contraseña de acceso Telnet**

R1(config-line)#line vty 0 4 accedo a la consola telnet

R1(config-line)#password cisco asigno contraseña

R1(config-line)#login confirmo la contraseña

**Cifrar las contraseñas de texto no cifrado**

R1(config)#service password-encryption encripto contraseñas sin encriptar

**Mensaje MOTD**

R1(config)#banner motd #se prohibe el acceso no autorizado# asigo un banner

**Interfaz S0/2/0**

Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección dis ponible en la subred.

R1(config)#interf s0/2/0 accedo a la interfaz

R1(config-if)#ip address 172.16.1.1 255.255.255.252 asigno una ip

R1(config-if)#no shutdow subo la interfaz

**Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz**

R1(config)#ipv6 unicast-routing en modo global, habilito usar ipv6

R1(config)#interfac s0/2/0 accedo a la interfaz

R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 asigno una ip

R1(config-if)#clock rate 128000 asigno frecuencia de reloj

R1(config-if)#no shutdow subo la interfaz

R1(config-if)#

Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

R1(config)#ip route 0.0.0.0 0.0.0.0 S0/2/0 asigno ruta pred. En ipv4

%Default route without gateway, if not a point-to-point interface, may impact performance

R1(config)#

R1(config)#ipv6 route ::/0 S0/2/0 asigno ruta pred.en ipv6

**Configurar R2**

**Desactivar la búsqueda DNS**

Router(config)#no ip domain-lookup en modo global se deactiva búsqueda DNS

**Nombre del router**

Router(config)#hostname R2 se da nombre al R

**Contraseña de exec privilegiado cifrada**

R2(config)#enable secret class se da contraseña en modo privilegiado

**Contraseña de consola principal**

CR2(config)#line console 0 se accede a la consola principal

R2(config-line)#password cisco se asigna contraseña

R2(config-line)#login se confirma contraseña

**Contraseña de acceso Telnet**

R2(config-line)#line vty 0 4 se accede a la consola telnet

R2(config-line)#password cisco se asigna contraseña

R2(config-line)#login se confirma contraseña

R2(config-line)#exit se sale

**Cifrar las contraseñas de texto no cifrado**

R2(config)#service password-encryption se encriptan contraseñas no cifradas

**HR2(config)#ip http server** comando invalido en el IOS

% Invalid input detected at '^' marker.

R2(config)#ip http secure-server

% Invalid input detected at '^' marker.

habilitar el servidor HTTP

Este comando no es soportado en packet-tracer

**Mensaje MOTD**

R2(config)#banner motd $se prohibe el acceso no autorizado$ se pone un banner

**Interfaz S0/2/0**

**Establezca la descripción**

**Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred**.

R2(config)#ipv6 unicast-routing se activa protocolo ipv6

R2(config)#interfac s0/2/0 se accede a la interfaz

R2(config-if)#ip address 172.16.1.2 255.255.255.252 se asigna una ip

R2(config-if)#description esta interfaz va hacia el R1 se da una descripcion

**Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz**

R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 se asigna una ipv6

R2(config-if)#no shutdow se sube la interfaz

R2(config-if)#

%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

**Interfaz S0/2/1**

**Establecer la descripción**

**Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.**

R2(config)#interfac s0/2/1 se accede a la interfaz

R2(config-if)#description esta interfaz va hacia el R3 se da una descripcion

R2(config-if)#ip address 172.16.2.1 255.255.255.252 se asigna una ip

**Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000.**

Activar la interfaz

R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 se asigna una ipv6

R2(config-if)#clock rate 128000 se asigna una frecuencia de reloj

R2(config-if)#no shutdown se sube la interfaz

%LINK-5-CHANGED: Interface Serial0/2/1, changed state to down

**Interfaz G0/0/0 (simulación de Internet)**

**Establecer la descripción.**

**Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.**

R2(config)#interfac g0/0/0 se accede a la interfaz

R2(config-if)#description interface hacia internetse da una descripcion

R2(config-if)#exit se sale

R2(config)#ipv6 unicast-routing se activa protocolo ipv6

R2(config)#interfac g0/0/0 se accede a la interfaz

R2(config-if)#ip address 209.165.200.233 255.255.255.248 se asigna una ip

**Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.**

**Activar la interfaz**

R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64 se asigna una ipv6

R2(config-if)#no shutdown se sube la interfaz

R2(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

**Interfaz loopback 0 (servidor web simulado)**

**Establecer la descripción. Establezca la dirección IPv4.**

R2(config)#interfac loopback 0 se asigna una interfaz loopback

R2(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#description servidor web se da una descripcion

R2(config-if)#ip address 10.10.10.10 255.255.255.255 se asigna una ip

R2(config-if)#

**Ruta predeterminada**

Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0/0 se da una ruta pred.ipv4

%Default route without gateway, if not a point-to-point interface, may impact performance

R2(config)#ipv6 route ::/0 G0/0/0 se asigna ruta pred.ipv6

R2(config)#

**Configurar R3**

**Desactivar la búsqueda DNS**

Router>en se accede al modo privilegiado

Router#config termi se accede al modo de configuración global

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#no ip domain-lookup se desactivan búsquedas DNS

**Nombre del router**

Router(config)#hostname R3 se asigna un nombre al R

**Contraseña de exec privilegiado cifrada**

R3(config)#enable secret class se da contraseña al modo privilegiado

**Contraseña de acceso a la consola**

R3(config)#line console 0 se accede a la consola principal

R3(config-line)#password cisco se asigna contraseña

R3(config-line)#login se confirma contraseña

**Contraseña de acceso Telnet**

R3(config-line)#line vty 0 4 se accede a la consola de telnet

R3(config-line)#password cisco se asigna contraseña

R3(config-line)#login se confirma contraseña

**Cifrar las contraseñas de texto no cifrado**

R3(config-line)#exit se sale

R3(config)#service password-encryption se encripta contraseñas sin encriptar

**Mensaje MOTD**

R3(config)#banner motd $Se Prohibe El Acceso No Autorizado$ se da un banner

R3(config)#

**Interfaz S0/2/1**

**Establecer la descripción**

R3(config-if)#description esta es la interfaz hacia el R2 se da una descripcion

**Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.**

R3(config)#ipv6 unicast-routing se activa el protocolo ipv6

R3(config)#interfac s0/2/1 se accede a la interfaz

R3(config-if)#ip address 172.16.2.2 255.255.255.252 se da una ip

**Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz**

R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 se da una ipv6

R3(config-if)#no shutdown se sube la interfaz

R3(config-if)#

%LINK-5-CHANGED: Interface Serial0/2/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up

Interfaz loopback 4

R3(config)#interfac loopback 4 se crea la loopback

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up

R3(config-if)#ip add 192.168.4.1 255.255.255.0 se da una ip

R3(config-if)#exit se sale

Interfaz loopback 5

R3(config)#interfa loopback 5 se crea la interfaz

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up

R3(config-if)#ip address 192.168.5.1 255.255.255.0 se le da una ip

R3(config-if)#exit se sale

In R3(config)#interfac loopback 6 se crea la interfaz

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0 se le da una ip

R3(config-if)#exit se sale

Interfaz loopback 7

R3(config)#interfac loopback 7 se crea la interfaz

R3(config-if)#

%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

R3(config-if)#

**Rutas predeterminadas**

R3(config-if)#ip route 0.0.0.0 0.0.0.0 S0/2/1 se crea ruta pred.ipv4

%Default route without gateway, if not a point-to-point interface, may impact performance

R3(config)#ipv6 route ::/0 S0/2/1 se crea ruta pred. Ipv6

R3(config)#

**Configurar S1**

**Desactivar la búsqueda DNS**

Switch(config)#no ip domain-lookup se desactivan búsquedas DNS

**Nombre del switch**

Switch(config)#hostname S1 se da un nombre al R

**Contraseña de exec privilegiado cifrada**

S1(config)#enable secret class se asigna contraseña en modo privilegiado

**Contraseña de acceso a la consola**

S1(config)#line console 0 se accede a la consola 0

S1(config-line)#password cisco se asigna una contraseña

S1(config-line)#login se confirma contraseña

**Contraseña de acceso Telnet**

S1(config-line)#line vty 0 15 se accede a la consola telnet

S1(config-line)#password cisco se asigna contraseña

S1(config-line)#login se confirma contraseña

S1(config-line)#exit se sale

**Cifrar las contraseñas de texto no cifrado**

S1(config)#service password-encryption se cifran contraseñas sin cifrar

**Mensaje MOTD**

S1(config)#banner motd $Se Prohibe El Acceso No Autorizado$ se da un banner

S1(config)#

**Configurar el S3**

**Desactivar la búsqueda DNS**

Switch(config)#no ip domain-lookup se dasactivan búsquedas DNS

Nombre del switch

Switch(config)#hostname S3 se da un nombre al Switch

**Contraseña de exec privilegiado cifrada**

S3(config)#enable secret class se da contraseña al modo privilegiado

**Contraseña de acceso a la consola**

S3(config)#line console 0 se accede a la consola 0

S3(config-line)#password cisco se asigna contraseña

S3(config-line)#login se confirma contraseña

**Contraseña de acceso Telnet**

S3(config)#line vty 0 15 se accede a la consola telnet

S3(config-line)#password cisco se asigna contraseña

S3(config-line)#login se confirma contraseña

**Cifrar las contraseñas de texto no cifrado**

S3(config)#service password-encryption se cifran contraseñas sin cifrar

S3(config)#

**Mensaje MOTD**

S3(config-line)#banner motd $Se prohibe El Acceso No Autirizado$se da un banner

S3(config)#exit

**Verificar la conectividad de la red**

Figura 7.ping de R1 a R2

```
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Fuente: Autor

Figura 8.ping de R2 a R3

```
R2#ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
```

Fuente: Autor

**Configurar la seguridad del switch, las VLAN y el routing entre VLAN**

**Configurar S1**

**Crear la base de datos de VLAN**

S1(config)#vlan 21 se crea la interfaz

S1(config-vlan)#name contabilidad se asigna un nombre

S1(config-vlan)#vlan 23 se crea la interfaz

S1(config-vlan)#name ingeniería se asigna un nombre

S1(config-vlan)#vlan 99 se crea la interfaz

S1(config-vlan)#name administración se asigna un nombre

Asignar la dirección IP de administración.

S1(config-vlan)#interfac vlan 99 se crea la interfaz

S1(config-if)#ip address 192.168.99.2 255.255.255.0

S1(config-if)#no shutdown se sube la interfaz

S1(config-if)#exit se sale

S1(config)#

**Asignar el gateway predeterminado**

S1(config)#ip default-gateway 192.168.99.1 se asigna un Gateway pred.

S1(config)#

**Forzar el enlace troncal en la interfaz F0/3**

S1(config)#interfac f0/3 se accede ala interfaz

S1(config-if)#switchport mode trunk se asigna modo troncal en el S

S1(config-if)#switchport trunk native vlan 1 se asigna vlan nativa en troncal

**Forzar el enlace troncal en la interfaz F0/5**

S1(config)#interface f0/5 se accede ala interfaz

S1(config-if)#switchport trunk native vlan 1 se asigna vlan nativa en troncal

S1(config-if)#switchport mode trunk se asigna modo troncal en el S

S1(config-if)#

**Configurar el resto de los puertos como puertos de acceso**

S1(config)#interf range f0/1-f0/2 se accede ala interfaz

S1(config-if-range)#switchport mode access se asigna mode de acceso en S

S1(config-if-range)#interfa f0/4 se accede ala interfaz

S1(config-if)#switchport mode access se asigna modo de acceso en S

S1(config-if)#interf range f0/7-f0/24 se asigna un rango en la interfaz

S1(config-if-range)#switchport mode access se asignan modo de acceso

**Asignar F0/6 a la VLAN 21**

S1(config-if-range)#interface f0/6 se accede ala interfaz

S1(config-if)#switchport mode access se asigna modo de acceso al S

S1(config-if)#switchport access vlan 21 se da modo de acceso a la vlan

S1(config-if)#

**Apagar todos los puertos sin usar**

S1(config-if)#interfa range f0/7-f0/24 se asigna un rango en la interfaz

S1(config-if-range)#shutdown se desactivan las interfaces

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

**Configurar el S3**

**Crear la base de datos de VLAN**

S3(config)#vlan 21 se crea la interfaz

S3(config-vlan)#name contabilidad se asigna un nombre

S3(config-vlan)#vlan 23 se crea la interfaz

S3(config-vlan)#name ingeniería se asigna un nombre

S3(config-vlan)#vlan 99 se crea la interfaz

S3(config-vlan)#name administración se asigna un nombre

**Asignar la dirección IP de administración**

S3(config-vlan)#interfac vlan 99 se crea la interfaz

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0 se da una ip

S3(config-if)#no shutdown se sube la interfaz

S3(config-if)#exit se sale

**Asignar el gateway predeterminado.**

ip default-gateway 192.168.99.1 se asigna un Gateway pred.

**Forzar el enlace troncal en la interfaz F0/3**

S3(config)#interfac f0/3 se accede a la interfaz

S3(config-if)#switchport mode trunk se configura modo troncal

S3(config-if)#switchport trunk native vlan 1 se asigna vlan1 nativa en troncal

S3(config-if)#

**Configurar el resto de los puertos como puertos de acceso**

S3(config)#interfac range f0/1-f0/2 se asigna un rango en la interface

S3(config-if-range)#switchport mode access se asigna mode de acceso

S3(config-if-range)#interf range f0/4-f0/24 se asigna un rango en la interface

S3(config-if-range)#switchport mode Access se asigna modo de acceso

S3(config-if-range)#exit se sale

**Asignar F0/18 a la VLAN 21**

S3(config)#interf f0/18 se accede a la interfaz

S3(config-if)#switchport access vlan 21 se configura modo de acceso a la vlan

S3(config-if)#exit se sale

**Apagar todos los puertos sin usar**

S3(config)#interface range f0/4-f0/17 se configura un rango en el interface

S3(config-if-range)#shutdown se desactivan las interfaces

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

**Configurar R1**

R1(config)#interface g 0/0/1 se accede a la interfaz

R1(config-if)#no shutdown se sube la interfaz

**Configurar la subinterfaz 802.1Q .21 en G0/0/1**

R1(config)#interface g 0/0/1.21 se accede a la interfaz vlan

R1(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.21, changed state to up

R1(config-subif)#description LAN de Contabilidad se describe la interfaz

R1(config-subif)#encapsulation dot1q 21 se da un comando de encapsulacion

R1(config-subif)#ip address 192.168.21.1 255.255.255.0 se asigna una ip

R1(config-subif)#exit se sale

**Configurar la subinterfaz 802.1Q .23 en G0/0/1**

R1(config)#interface g 0/0/1.23 se crea la subinterfaz

R1(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23, changed state to up

R1(config-subif)#description Lan de Ingenieria se da descripción de la interfaz

R1(config-subif)#encapsulation dot1q 23 se asigna modo de encapsulacion

R1(config-subif)#ip address 192.168.23.1 255.255.255.0 se da una ip

R1(config-subif)#exit

**Configurar la subinterfaz 802.1Q .99 en G0/0/1**

R1(config)#interface g 0/0/1.99 se crea la subinterfaz

R1(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up

R1(config-subif)#description LAN de Administracion se da una descripcion

R1(config-subif)#encapsulation dot1q 99 se da modo de encapsulacion

R1(config-subif)#ip add 192.168.99.1 255.255.255.0 se da una ip

R1(config-subif)#exit

**Activar la interfaz G0/0/1**

R1(config)#interface g 0/0/1 se accede a la interfaz

R1(config-if)#no shutdown se sube la interfaz

R1(config-if)#

**Verificar la conectividad de la red**

Figura 9.ping de S1 a subinterfaz 802.1Q .99

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: Autor

Figura 10.ping de S3 a a subinterfaz 802.1Q .99

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/15 ms
```

Fuente: Autor

Figura 11.ping de S1 a la subinterfaz 802.1Q .21 en G0/0/1

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: Autor

Figura 12.ping de S3 a la la subinterfaz 802.1Q .23 en G0/0/1

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Fuente: Autor

**Configurar el protocolo de routing dinámico OSPF**

**Configurar OSPF en el R1**

**Configurar OSPF área 0**

Anunciar las redes conectadas directamente

R1(config)#router ospf 58 se configura el router al protocolo ospf

R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 se declaran la red

R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 se declaran la red

R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 se declaran la red

R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 se declaran la red

Establecer todas las interfaces LAN como pasivas

R1(config-router)#passive-interface g0/0/1 se declara la interfaz pasiva

R1(config-router)#passive-interface g0/0/1.21 se declara la interfaz pasiva

R1(config-router)#passive-interface g0/0/1.23 se declara la interfaz pasiva

R1(config-router)#passive-interface g0/0/1.99 se declara la interfaz pasiva

**Desactive la sumarización automática**

OSPF no realiza la sumarización automática

**Configurar OSPF en el R2**

**Configurar OSPF área 0**

**Anunciar las redes conectadas directamente**

Nota: Omitir la red G0/0.

R2(config)#router ospf 58 se declara protocolo ospf

R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 se declara la red

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 se declara la red

R2(config-router)#

11:19:47: %OSPF-5-ADJCHG: Process 58, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to FULL, Loading Done

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 se declara la red

**Establecer la interfaz LAN (loopback) como pasiva**

R2(config-router)#passive-interface loopback 0 se declara pasiva esta interfaz

R2(config-router)#exit se sale

**Desactive la sumarización automática**

OSPF no realiza la sumarización automática

**Configurar OSPFv3 en el R2**

**Configurar OSPF área 0**

R2(config)#interface s 0/2/0 se accede a la interfaz

R2(config-if)#ipv6 ospf 59 area 0 se activa protocolo ospf ipv6

R2(config-if)#exit se sale

| | |
|---|---|
| R2(config)#interfece s 0/2/1 | se accede ala interfaz |
| R2(config-if)#ipv6 ospf 59 area 0 | se activa protocolo ospf ipv6 |
| R2(config-if)#exit | se sale |
| R2(config)#interface g 0/0/0 | se accede a la interfaz |
| R2(config-if)#ipv6 ospf 59 area 0 | se activa protocolo ospf ipv6 |
| R2(config-if)#exit | se sale |

**Anunciar redes IPv4 conectadas directamente**

El protocolo OSPF V3. No maneja redes IPV4

**Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas**

la loopback no tiene direcciones bajo IPV6.

en este protocolo eso no se hace para eso se coloca la wildcard y en IPV6 no se hace.

**Desactive la sumarización automática**.

OSPF no realiza la sumarización automática

**Verificar la información de OSPF**

**Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:**

**¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?**

**La ID del router, interfaces pasivas, las redes de routing:**

Figura 13.Show ip protocols

```
R2#show ip protocols

Routing Protocol is "ospf 58"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10           110      00:23:52
    192.168.99.1          110      00:23:52
  Distance: (default is 110)
```

Fuente: Autor

**¿Qué comando muestra solo las rutas OSPF?**

Figura 14.Show ip route ospf

```
R2#show ip route ospf
O    192.168.21.0 [110/65] via 172.16.1.1, 02:25:55, Serial0/2/0
O    192.168.23.0 [110/65] via 172.16.1.1, 02:25:55, Serial0/2/0
O    192.168.99.0 [110/65] via 172.16.1.1, 02:25:55, Serial0/2/0
```

Fuente: Autor

**¿Qué comando muestra la sección de OSPF de la configuración en ejecución?**

show ip ospf database

Figura 15.Show ip ospf database

```
R2#show ip ospf database
            OSPF Router with ID (10.10.10.10) (Process ID 58)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.10.10.10     10.10.10.10     1058        0x80000009 0x004799 4
192.168.99.1    192.168.99.1    1057        0x8000000b 0x00c7b8 5
R2#
```

Fuente: Autor

**Implementar DHCP y NAT para IPv4**

**Configurar el R1 como servidor de DHCP para las VLAN 21 y 23**

**Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas**

ip dhcp excluded-address 192.168.21.1 192.168.21.20 se excluyen estas redes

ip dhcp excluded-address 192.168.23.1 192.168.23.20 se excluyen estas redes

**Crear un pool de DHCP para la VLAN 21.**

R1(config)#ip dhcp pool ACCT se crea el nombre del pool de direcciones

R1(dhcp-config)#network 192.168.21.0 255.255.255.0 se declara la red

R1(dhcp-config)#domain-name ccna-sa.com se crea al dominio

R1(dhcp-config)#dns-server 10.10.10.10 se declara servidor de DNS

R1(dhcp-config)#default-router 192.168.21.1 se declara el gateway

**Crear un pool de DHCP para la VLAN 23**

R1(config)#ip dhcp pool ENGNR se crea el nombre del pool de direcciones

R1(dhcp-config)#network 192.168.23.0 255.255.255.0 se declara la red

R1(dhcp-config)#dns-server 10.10.10.10 se declara el servidor DNS

R1(dhcp-config)#domain-name ccna-sa.com se accede al dominio

R1(dhcp-config)#default-router 192.168.23.1 se declara el gateway

R1(dhcp-config)#

**Configurar la NAT estática y dinámica en el R2**

**Crear una base de datos local con una cuenta de usuario**

R2(config)#username webuser privilege 15 password cisco12345 se asigna usuario y clave

**HR2(config)#ip http server** comando no funciona en el IOS

% Invalid input detected at '^' marker.

habilitar el servicio del servidor HTTP

packet tracer no recibe este comando

**Configurar el servidor HTTP para utilizar la base de datos local para la autenticación**

R2(config)#ip http authentication local comando no funciona en el IOS

% Invalid input detected at '^' marker.

packet tracer no recibe este comando

**Crear una NAT estática al servidor web.**

ip nat inside source static 10.10.10.10 209.165.200.233 se crea ip NAT estatica

**Asignar la interfaz interna y externa para la NAT estática**

R2(config)#interface g0/0/0 se accede a la interfaz

R2(config-if)#ip nat outside se declara interfaz de salida

R2(config-if)#interface S0/2/0 se accede a la interfaz

R2(config-if)#ip nat inside se declara interfaz de entrada

R2(config-if)#interface S0/2/1 se accede a la interfaz

R2(config-if)#ip nat inside se declara interfaz de entrada

R2(config-if)#interface loopback 0 se accede a la interfaz

R2(config-if)#ip nat inside se declara de entrada

R2(config-if)#

**Configurar la NAT dinámica dentro de una ACL privada**

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 red q se traduce

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 red q se traduce

R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255 red q se traduce

R2(config)#

**Defina el pool de direcciones IP públicas utilizables**.

R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 pool de direcciones q se van a usar

R2(config)# ip nat inside source list 1 pool INTERNET se declaran como entrada

**Definir la traducción de NAT dinámica**

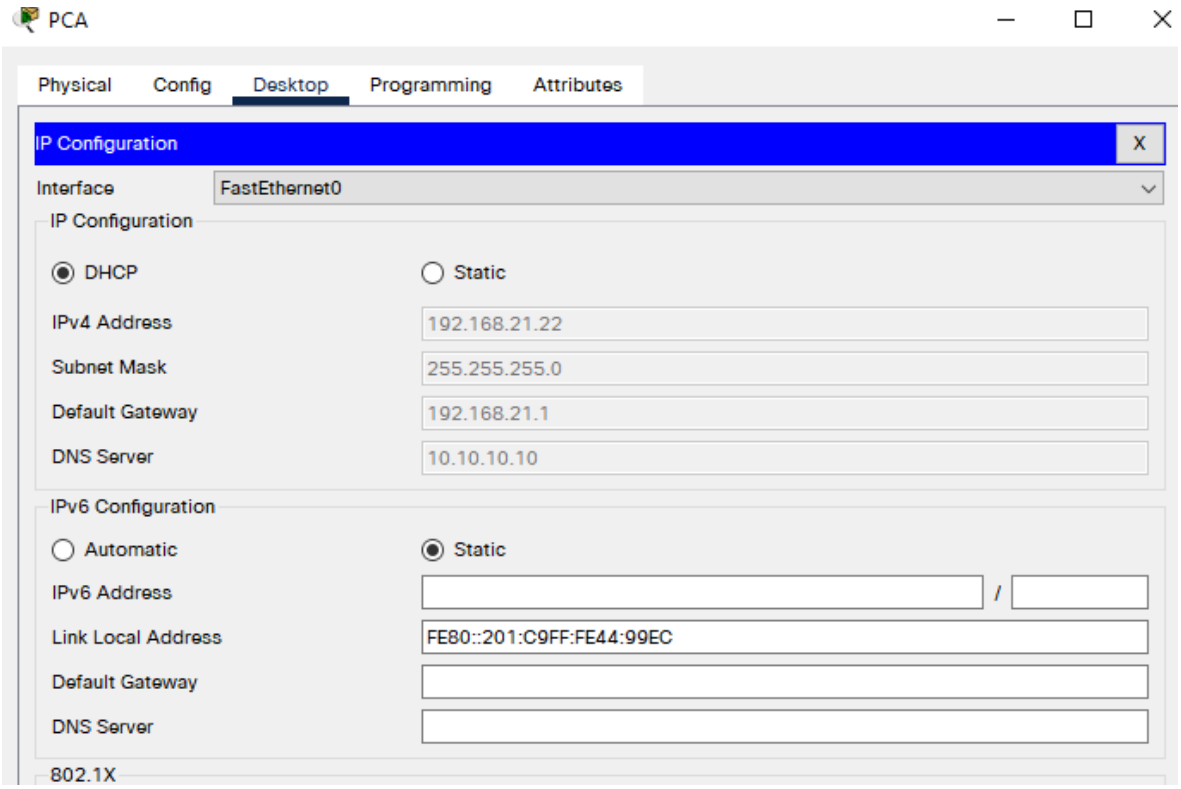
NAT (Network Address Traslation), permite acceder a internet traduciendo las direccones privadas en direcciones ip publicas.

Incrementando la seguridad y la privacidad de la red local al traducir el direccionamiento interno a uno externo.

**Verificar el protocolo DHCP y la NAT estática**

**Verificar que la PC-A haya adquirido información de IP del servidor de DHCP**

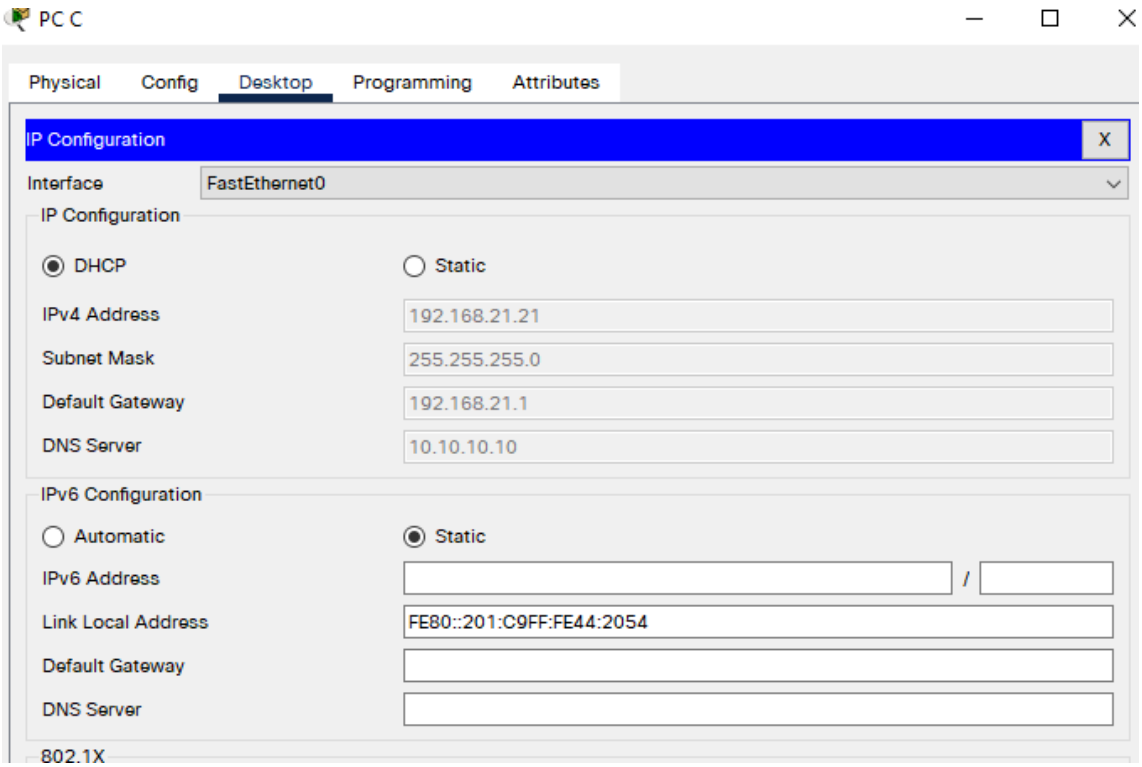
Figura 16.DHCP en PC-A




Fuente: Autor

**Verificar que la PC-C haya adquirido información de IP del servidor de DHCP**

Figura 17. PC-C.Direccion DHCP




Fuente: Autor

**Verificar que la PC-A pueda hacer ping a la PC-C**

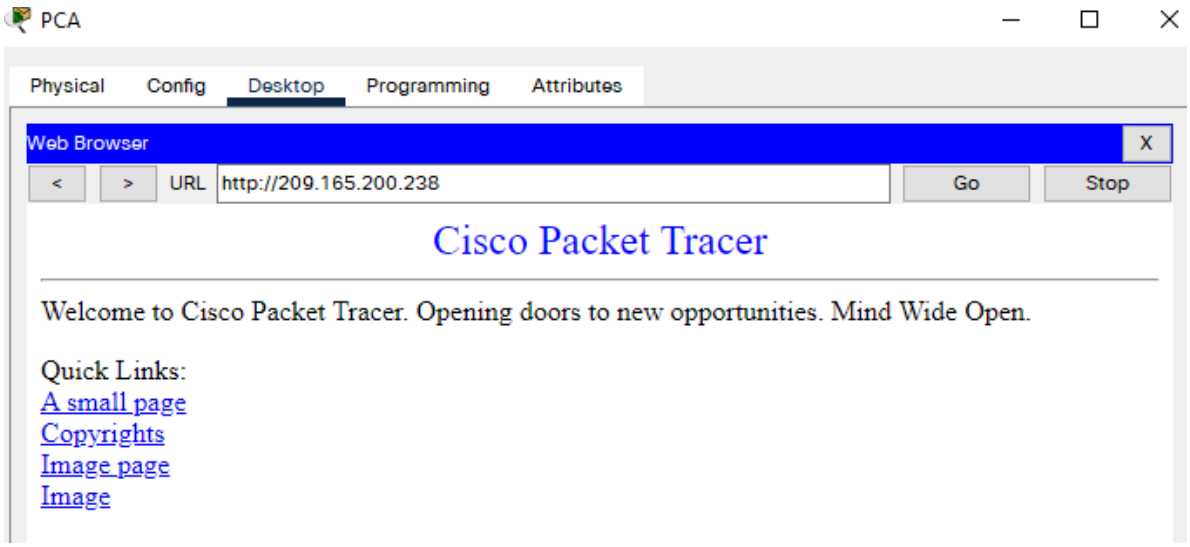
Figura 18.ping PC-A a la PC-C

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.21.22

Pinging 192.168.21.22 with 32 bytes of data:

Reply from 192.168.21.22: bytes=32 time=1ms TTL=128
Reply from 192.168.21.22: bytes=32 time<1ms TTL=128
Reply from 192.168.21.22: bytes=32 time=11ms TTL=128
Reply from 192.168.21.22: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.21.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Fuente: Autor

**Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345**

Figura 19.Acceso Servidor Web




Fuente: Autor

**Configurar NTP**

**Ajuste la fecha y hora en R2.**

R2#clock set 09:00:00 05 march 2016 se configura el set clock

R2#show clock se muestra el set clock

9:6:11.735 UTC Sat Mar 5 2016

**Configure R2 como un maestro NTP.**

R2#confi termi se accede al modo global

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#ntp master 5 se configura R2 como maestro

**Configurar R1 como un cliente NTP.**

R1#show clock se muestra el set clock

*6:11:32.929 UTC Mon Mar 1 1993

R1#config termi se accede al modo global

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ntp server 172.16.1.2 se configura R1 como cliente

**Configure R1 para actualizaciones de calendario periódicas con hora NTP.**

R1(config)#ntp update-calendar se actualiza el calendario

R1(config)#exit se sale

**Verifique la configuración de NTP en R1.**

R1#show clock muestra el set clock

9:22:20.404 UTC Sat Mar 5 2016

**Restringir el acceso a las líneas VTY en el R2**

**Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2**

R2(config)#ip access-list standard ADMIN-MGT crea una lista de acceso standar

R2(config-std-nacl)#permit host 172.16.1.1 se permite esta red

R2(config-std-nacl)#deny any se deniega el resto

R2(config-std-nacl)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to down

10:19:05: %OSPF-5-ADJCHG: Process 58, Nbr 192.168.99.1 on Serial0/2/0 from FULL to DOWN, Neighbor Down: Interface down or detached

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

10:19:15: %OSPF-5-ADJCHG: Process 58, Nbr 192.168.99.1 on Serial0/2/0 from LOADING to FULL, Loading Done

**Aplicar la ACL con nombre a las líneas VTY**

R2(config-std-nacl)#exit se sale

R2(config)#line vty 0 4 se accede ala consola de telnet

R2(config-line)#ip access-class ADMIN-MGT in  permite que esta red acceda a vty

**Permitir acceso por Telnet a las líneas de VTY**

transport input telnet  accede mediante protocolo telnet

**Verificar que la ACL funcione como se espera**

R1#telnet 172.16.1.2  telnet a esa ip

Trying 172.16.1.2 ...Opense prohibe el acceso no autorizado

User Access Verification

Password:

R2>en

Password:

Password:

**Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente**

**Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció**

R2#show access-lists

Figura 20.Show Access-lists

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255 (2 match(es))
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.0.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
    20 deny any
```

Fuente: Autor

**Restablecer los contadores de una lista de acceso**

clear access-list counters

R2#clear access-list counters

R2#show access-list

Figura 21.Ejecutando clear en R2

```
R2#clear  access-list counters
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.0.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
    20 deny any
```

Fuente: Autor

**¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?**

Show ip interface

R2#show ip interface

Figura 22.Show ip interface en R2

```
R2#show ip interface
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
```

Fuente: Autor

¿Con qué comando se muestran las traducciones NAT?

**Show ip nat translations**

R2#Show ip nat translations

Figura 23.Show ip translations

```
R2#Show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.233   10.10.10.10        ---                ---
tcp 209.165.200.225:1025192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
```

Fuente: Autor

**show ip nat statistics**

Figura 24.Show ip nat stadistics en R2

```
R2#show ip nat statistics
Total translations: 2 (1 static, 1 dynamic, 1 extended)
Outside Interfaces: GigabitEthernet0/0/0
Inside Interfaces: Serial0/2/0 , Serial0/2/1 , Loopback0
Hits: 8  Misses: 3
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 1 pool INTERNET refCount 1
 pool INTERNET: netmask 255.255.255.248
       start 209.165.200.225 end 209.165.200.228
       type generic, total addresses 4 , allocated 1 (25%), misses 0
```

Fuente: Autor

**¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?**

**Clear ip nat translation ***

R2#clear ip nat translation *

R2#show ip nat translations

Figura 25.ejecutando clear en ip nat translations

```
R2#Clear ip nat translation *
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.233   10.10.10.10        ---                ---
```

Fuente: Autor

## CONCLUSIONES

Se obtuvo las habilidades para configurar los dispositivos de internetworking.

Se conoció los comandos de consola necesarios para establecer contraseñas, cifrar las mismas, establecer nombres de dominio, acceso a una DB local mediante usuario, configurar la vlan del switch y utilizar claves seguras rsa.

Se adquirió las competencias para configurar una red LAN haciendo subnetting, dando nombre de dominio, asignando direcciones ip a los diferentes dispositivos de internetworking como lo son el router, switch, y los hosts.

Se cifro líneas seguras con protocolo ssh, y dando uso de claves cifradas rsa, entre otros.

En el segundo escenario, ponemos a punto los equipos para iniciar configuraciones haciéndoles un borrado y y recargado de las configuraciones iniciales.

Se configuro los equipos de red dándoles unos direcciones, contraseñas de seguridad, se configuraron unas loopback en el router 3, se crearon unas Vlan en el router 1, se verifico mediante el comando ping la conectividad entre las diferentes interfaces Vlan

Se configura el protocolo OSPF en sus diferentes versiones en los routers propuestos.

Se configura el router 1 como servidor DHCP de las Vlans 21 y 23.

Se configura la NAT dinámica y estatica en el router 2, creando una base de datos local y no pudiéndose habilitar el servicio http porque packet tracer no toma ese comando.

Se definio el pool de direcciones publicas utilizables.

Se verifico el protoloco DHCP en las computadoras.

Se configuro el protocolo de tiempo de red NTP en el router 2.

Se configuro y verifico las listas de control ACL en el router 2 aplicadas a las lineas vty.

Por linea de comandos se buscan las concidencias en la lista de control de acceso y también se borran

Por comandos también se muestran las traducciones NAT y también se eliminan

## BIBLIOGRAFIA


[1] GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. Inge Cuc, 12(1), 86-93.

[2] GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. Revista de Tecnología, 14(1), 127-138.

[3] BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In International Conference on Knowledge Management in Organizations (pp. 331-344). Springer, Cham.

[4] BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. Revista UIS Ingenierías, 16(1), 75-84.

[5] BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

[6] BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In 2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI) (pp. 1-5). IEEE.

[7] MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In 2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI) (pp. 1-6). IEEE.

[8] ARIGANELLO. Ernesto. Redes Cisco: Guía de estudio para certificación CCNA Security.Madrid: RA-MA, 2014. 77-58p

[9] ARIGANELLO. Ernesto. Redes Cisco. Guía de estudio para la certificación CCNA Routing And Switching. Madrid: RA-MA, 2014. 220-198p.

[10] ARIGANELLO. Ernesto y BARRIENTOS SEVILLA.Enrique.Redes Cisco: Estudio para la certificacion CCNP.2 Edicion. Madrid: RA-MA, 2014. 69-92p

[11] ARIGANELLO. Ernesto.Tecnicas de configuración de routers cisco.Madrid: RA-MA, 2014. 73-84p

[12] MOLINA ROBLES.Francisco.Panificacion y administración de redes. Madrid: RA-MA, 2014. 73-84p

[13] PEREZ TORRES.Daniel.Redes Cisco.Curso practico de formación para la certificación CCNA.Madrid: RC libros, 2018.361-371p

[14] LUCA DE TENA.Juan.Enrutadores Cisco.Madrid: ANAYA, 2009.175p

[15] WENDELL. Odom. CCNA Rout&Switch 200-101: Guía examen certificación (Cisco Press).Madrid: PEARSON, 2014.231p