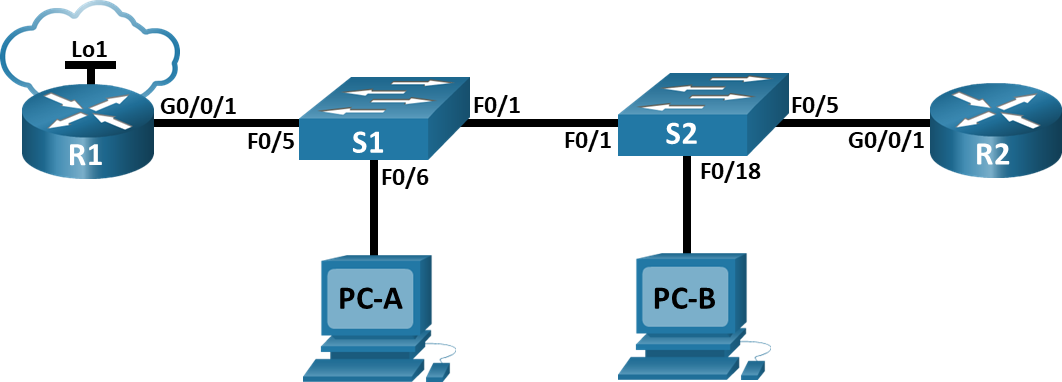
Laboratorio: configuración y verificación de IPv4 ACL extendidas (versión para el instructor)

**Nota para el instructor**: Los elementos con color de fuente rojo o resaltados en gris indican texto que aparece solo en la copia del instructor.

# Topología



# Tabla de asignación de direcciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| R1 | G0/0/1 | N/A | N/A | N/A |
| R1 | G0/0/1.20 | 10.20.0.1 | 255.255.255.0 | N/D |
| R1 | G0/0/1.30 | 10.30.0.1 | 255.255.255.0 | N/D |
| R1 | G0/0/1.40 | 10.40.0.1 | 255.255.255.0 | N/D |
| R1 | G0/0/1.1000 | N/A | N/A | No corresponde |
| R1 | Loopback1 | 172.16.1.1 | 255.255.255.0 | N/D |
| R2 | G0/0/1 | 10.20.0.4 | 255.255.255.0 | N/A |
| S1 | VLAN 20 | 10.20.0.2 | 255.255.255.0 | 10.20.0.1 |
| S2 | VLAN 20 | 10.20.0.3 | 255.255.255.0 | 10.20.0.1 |
| PC-A | NIC | 10.30.0.10 | 255.255.255.0 | 10.30.0.1 |
| PC-B | NIC | 10.40.0.10 | 255.255.255.0 | 10.40.0.1 |

# Tabla de VLAN

| VLAN | Nombre | Interfaz asignada |
| --- | --- | --- |
| 20 | Administración | S2: F0/5 |
| 30 | Operaciones | S1: F0/6 |
| 40 | Ventas | S2: F0/18 |
| 999 | ParkingLot | S1: F0/2-4, F0/7-24, G0/1-2  S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2 |
| 1000 | Nativo | N/A |

# Objetivos

Parte 1: Armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: Configurar y verificar listas de control de acceso extendido

# Antecedentes/Escenario

Se le ha encomendado la tarea de configurar listas de control de acceso en la red de la pequeña empresa. Las ACL son uno de los medios más simples y directos para controlar el tráfico de capa 3. R1 alojará una conexión a Internet (simulada por la interfaz Loopback 1) y compartirá la información de ruta predeterminada a R2. Una vez completada la configuración inicial, la empresa tiene algunos requisitos específicos de seguridad del tráfico que usted es responsable de implementar.

**Nota**: Los routers que se utilizan en los laboratorios prácticos de CCNA son Cisco 4221 con Cisco IOS XE versión 16.9.3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota**: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

**Nota para el instructor**: Consulte el Manual de Laboratorio del Instructor para conocer los procedimientos para inicializar y recargar dispositivos.

# Recursos necesarios

* 2 Router (Cisco 4221 con imagen universal Cisco IOS XE versión 16.9.3 o comparable)
* 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
* 2 PC (Windows con un programa de emulación de terminal, como Tera Term)
* Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
* Cables Ethernet, como se muestra en la topología

# Instrucciones

## Construir la red y configurar ajustes básicos de los dispositivos

### Realizar el cableado de red como se muestra en la topología

Conecte los dispositivos como se muestra en la topología y realizar el cableado necesario.

### Configure los parámetros básicos para cada router.

Abrir la ventana de configuración

* + - 1. Asigne un nombre de dispositivo al router.

router(config)# **hostname R1**

* + - 1. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

R1(config)# **no ip domain lookup**

* + - 1. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

R1(config)# **enable secret class**

* + - 1. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

R1(config)# **line console 0**

R1(config-line)# **password cisco**

R1(config-line)# **login**

* + - 1. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

* + - 1. Cifre las contraseñas de texto sin formato.

R1(config)# **service password-encryption**

* + - 1. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

R1(config)# **banner motd $ Authorized Users Only! $**

* + - 1. Guarde la configuración en ejecución en el archivo de configuración de inicio.

R1# **copy running-config startup-config**

Cerrar la ventana de configuración

### Configurar los parámetros básicos para cada switch

Abrir la ventana de configuración

* + - 1. Asigne un nombre de dispositivo al switch.

switch(config)# **hostname S1**

* + - 1. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

S1(config)# **no ip domain-lookup**

* + - 1. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

S1(config)# **enable secret class**

* + - 1. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

S1(config)# **line console 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

* + - 1. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

S1(config)# **line vty 0 15**

S1(config-line)# **password cisco**

S1(config-line)# **login**

* + - 1. Cifre las contraseñas de texto sin formato.

S1(config)# **service password-encryption**

* + - 1. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

S1(config)# **banner motd $ Authorized Users Only! $**

* + - 1. Guardar la configuración en ejecución en el archivo de configuración de inicio

S1(config)# **exit**

S1# **copy running-config startup-config**

Cerrar la ventana de configuración

## Configure las VLAN en los Switches.

### Crear las VLAN en los switches

Abrir la ventana de configuración

* + - 1. Cree y asigne un nombre a las VLAN necesarias en cada switch de la tabla anterior.

S1(config)# **vlan 20**

S1(config-vlan)# **name Management**

S1(config-vlan)# **vlan 30**

S1 (config-vlan) # **name Operations**

S1(config-vlan)# **vlan 40**

S1(config-vlan)# **name Sales**

S1(config-vlan)# **vlan 999**

S1(config-vlan)# **name ParkingLot**

S1 (config-vlan) # **vlan 1000**

S1(config-vlan)# **name Native**

S1(config-vlan)# **exit**

S2(config)# **vlan 20**

S2(config-vlan)# **name Management**

S2(config-vlan)# **vlan 30**

S2 (config-vlan) # **name Operations**

S2(config-vlan)# **vlan 40**

S2(config-vlan)# **name Sales**

S2(config-vlan)# **vlan 999**

S2(config-vlan)# **name ParkingLot**

S2 (config-vlan) # **vlan 1000**

S2(config-vlan)# **name Native**

S2(config-vlan)# **exit**

* + - 1. Configure la interfaz de administración y el gateway predeterminado en cada switch con la información de dirección IP incluida en la tabla de direccionamiento.

S1(config)# **interface vlan 20**

S1 (config-if) # **ip address 10.20.0.2 255.255.255.0**

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

S1(config)# **ip default-gateway 10.20.0.1**

S1(config)# **end**

S2(config)# **interface vlan 20**

S2 (config-if) # **ip address 10.20.0.3 255.255.255.0**

S2(config-if)# **no shutdown**

S2(config-if)# **exit**

S2(config)# **ip default-gateway 10.20.0.1**

S2 (config) # **final**

* + - 1. Asigne todos los puertos no utilizados del switch a la VLAN del estacionamiento, configúrelos para el modo de acceso estático y desactívalos administrativamente.

**Nota**: El comando interface range es útil para llevar a cabo esta tarea con los pocos comandos que sea necesario.

S1(config)# **interface range f0/2 - 4, f0/7 - 24, g0/1 - 2**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 999**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S2(config)# **interface range f0/2 - 17, f0/19 - 24, g0/1 - 2**

S2(config-if-range)# **switchport mode access**

S2(config-if-range)# **switchport access vlan 999**

S2(config-if-range)# **shutdown**

S2(config-if-range)# **end**

### Asignar las VLAN a las interfaces del switch correctas

* + - 1. Asigne los puertos usados a la VLAN apropiada (especificada en la tabla VLAN anterior) y configúrelos para el modo de acceso estático.

S1(config)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 30**

S2(config)# **interface f0/18**

S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 40**

* + - 1. Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

S1# **show vlan breve**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/5

10 Management active

20 Sales active Fa0/6

30 Operations active

999 ParkingLot activo Fa0/2, Fa0/3, Fa0/4, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

1000 Native active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S2 # **show vlab brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1

10 Management active

30 Operations active

40 Sales active Fa0/18

999 ParkingLot activo Fa0/2, Fa0/3, Fa0/4, Fa0/5

Fa0/6, Fa0/7, Fa0/8, Fa0/9

Fa0/10, Fa0/11, Fa0/12, Fa0/13

Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gi0/1, Gi0/2

Cerrar la ventana de configuración

## Configurar enlaces troncales.

### Configurar manualmente la interfaz de enlace troncal F0/1

Abrir la ventana de configuración

* + - 1. Cambie el modo de switchport en la interfaz F0/1 para forzar el enlace troncal. Haga esto en ambos switches.

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode trunk**

S2(config)# **interface f0/1**

S2(config-if)# **switchport mode trunk**

* + - 1. Como parte de la configuración troncal, establezca la vlan nativa en 1000 en ambos conmutadores. Puede ver mensajes de error temporalmente mientras las dos interfaces están configuradas para diferentes VLAN nativas.

S1(config-if)# **switchport trunk native vlan 1000**

S2(config-if)# **switchport trunk native vlan 1000**

* + - 1. Como otra parte de la configuración troncal, especifique que las VLAN 10, 20, 30 y 1000 pueden cruzar el troncal.

S1(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

S2(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

* + - 1. **Ejecute el comando show interfaces trunk** para verificar los puertos de enlace troncal, la VLAN nativa y las VLAN permitidas en el troncal.

S1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 en el enlace troncal 802.1q 1000

Port Vlans allowed on trunk

Fa0/1 20,30,40,1000

Port Vlans allowed and active in management domain

Fa0/1 20,30,40,1000

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 20,30,40,1000

S2# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 en el enlace troncal 802.1q 1000

Port Vlans allowed on trunk

Fa0/1 20,30,40,1000

Port Vlans allowed and active in management domain

Fa0/1 30,40,1000

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 30,40

### Configurar manualmente la interfaz de enlace troncal F0/5.

* + - 1. Configure la interfaz F0/5 de S1 con los mismos parámetros de troncal que F0/1. Este es el tronco del router.

S1(config)# **interface f0/5**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 1000**

S1(config-if)# **switchport trunk allowed vlan 20,30,40,1000**

* + - 1. Guardar la configuración en ejecución en el archivo de configuración de inicio

S1# **copy running-config startup-config**

* + - 1. Use el comando **show interfaces trunk** para verificar la configuración de los enlaces troncales.

Cerrar la ventana de configuración

## Configuración de

### Configuración de enrutamiento de InterVLAN en R1.

Abrir la ventana de configuración

* + - 1. Active las interfaz G0/0/1 en el router.

R1(config)# **interface g0/0/1**

R1(config-if)# **no shutdown**

* + - 1. Configure las subinterfaces para cada VLAN como se especifica en la tabla de direcciones IP. Todas las subinterfaces utilizan encapsulación 802.1Q. Asegúrese de que la subinterfaz de la VLAN nativa no tenga asignada una dirección IP. Incluya una descripción para cada subinterfaz.

R1(config) # **interfaz g0/0/1.20**

R1(config-subif)# **description Management Network**

R1(config-subif)# **encapsulation dot1q 20**

R1(config-subif)# **ip address 10.20.0.1 255.255.0**

R1(config-subif)# **interfaz g0/0/1.30**

R1(config-subif)# **encapsulation dot1q 30**

R1(config-subif)# **description Operations Network**

R1(config-subif)# **ip address 10.30.0.1 255.255.0**

R1(config-subif)# **interfaz g0/0/1.40**

R1(config-subif)# **encapsulation dot1q 40**

R1(config-subif)# **description Sales Network**

R1(config-subif)# **ip address 10.40.0.1 255.255.0**

R1(config-subif)# **interfaz g0/0/1.1000**

R1(config-subif)# **encapsulation dot1q 1000 nativo**

R1(config-subif)# **description Native VLAN**

* + - 1. Configure la interfaz Loopback 1 en R1 con direccionamiento de la tabla anterior.

R1(config)# **interface Loopback 1**

R1(config-if)# **ip address 172.16.1.1 255.255.255.0**

* + - 1. Use the **show ip interface brief** command para verificar la configuración de las subinterfaces

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 unassigned YES unset administratively down down

GigabitEthernet0/0/1 unassigned YES unset up up

Gi0/0/1.20 10.20.0.1 YES manual up up

Gi0/0/1.30 10.30.0.1 YES manual up up

Gi0/0/1.40 10.40.0.1 YES manual up up

Gi0/0/1.1000 unassigned YES unset up up

Serial0/1/0 unassigned NO unset down down

Serial0/1/1 unassigned NO unset down down

GigabitEthernet0 unassigned YES unset administratively down down

Loopback1 172.16.1.1 YES manual up up

### Configure la interfaz R2 g0/0/1 utilizando la dirección de la tabla y una ruta predeterminada con el salto siguiente 10.20.0.1

R2(config)# **interface g0/0/1**

R2(config-if)# **ip address 10.20.0.4 255.255.255.0**

R2(config-if)# **no shutdown**

R2(config-if)# **exit**

R2(config)# **ip route 0.0.0.0 0.0.0 10.20.0.1**

Cerrar la ventana de configuración

## Configurar acceso remoto.

### Configure todos los dispositivos de red para obtener soporte básico SSH.

Abrir la ventana de configuración

* + - 1. Crear un usuario local con el nombre de usuario sshAdmin y la contraseña cifrada $cisco123!

R1(config)# **username SSHadmin secret $cisco123!**

* + - 1. Use **ccna-lab.com** como nombre de dominio.

R1(config)# **ip domain name ccna-lab.com**

* + - 1. Generar claves criptográficas usando un módulo de 1024 bits.

R1(config)# **crypto key generate rsa general-keys modulus 1024**

* + - 1. Configure las primeras cinco líneas de VTY en cada dispositivo para admitir únicamente conexiones SSH y para autenticarse en la base de datos de usuarios local.

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

R1(config-line)# **login local**

R1(config-line)# **exit**

### Habilite servicios web seguros y autenticados en R1.

* + - 1. Habilite el servidor HTTPS en R1.

R1(config)# **ip http secure-server**

* + - 1. Configure R1 para autenticar a los usuarios que intenten conectarse al servidor web.

R1(config)# **ip http authentication local**

Cerrar la ventana de configuración

## Verificar la conectividad

### Configurar los equipos host

Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

### Complete las siguientes pruebas. Esto debe tener éxito.

**Nota:** Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

| De | de Internet | Destino |
| --- | --- | --- |
| PC-A | Ping | 10.40.0.10 |
| PC-A | Ping | 10.20.0.1 |
| PC-B | Ping | 10.30.0.10 |
| PC-B | Ping | 10.20.0.1 |
| PC-B | Ping | 172.16.1.1 |
| PC-B | HTTPS | 10.20.0.1 |
| PC-B | HTTPS | 172.16.1.1 |
| PC-B | SSH | 10.20.0.1 |
| PC-B | SSH | 172.16.1.1 |

## Configurar y verificar listas de control de acceso extendido

Cuando se verifica la conectividad básica, la empresa requiere que se implementen las siguientes políticas de seguridad:

**Directiva 1**: La red de ventas no está permitida para SSH a la red de administración (pero se permite otro SSH).

**Directiva 2**: La red de ventas no tiene permiso para acceder a las direcciones IP de la red de administración mediante ningún protocolo web (HTTP/HTTPS). La Red de Ventas tampoco puede acceder a interfaces R1 usando ningún protocolo web. El resto del tráfico web está permitido (nota — Ventas pueden acceder a la interfaz Loopback 1 en R1).

**Directiva 3**: La red de ventas no puede enviar solicitudes de eco ICMP a las redes de operaciones o de administración. Se permiten solicitudes de eco ICMP a otros destinos.

**Directiva 4**: La red de operaciones no puede enviar solicitudes de eco ICMP a la red de ventas. Se permiten solicitudes de eco ICMP a otros destinos.

### Analice la red y los requisitos de la política de seguridad para planificar la implementación de ACL.

Las respuestas pueden variar. Los requisitos enumerados anteriormente exigen que se apliquen dos listas de acceso ampliadas. Siguiendo la orientación de colocar listas de acceso ampliado lo más cerca posible del origen del tráfico que se va a filtrar, estas ACL se instalarán en las interfaces G0/0/0.30 y G0/0/0.40.

### Desarrolle y aplique listas de acceso extendido que cumplan las instrucciones de política de seguridad.

Abrir la ventana de configuración

Las respuestas pueden variar. Las ACL deben ser similares a las siguientes:

R1 (config) # **access-list 101 remark ACL 101 fulfills policies 1, 2, and 3**

R1 (config) # **access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 22**

R1 (config) # **access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 80**

R1 (config) # **access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.30.0.1 0.0.0.0 eq 80**

R1 (config) # **access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.40.0.1 0.0.0.0 eq 80**

R1 (config) # **access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 443**

R1 (config) # **access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.30.0.1 0.0.0.0 eq 443**

R1 (config) # **access-list 101 deny tcp 10.40.0.0 0.0.0.255 10.40.0.1 0.0.0.0 eq 443**

R1 (config) # **access-list 101 deny icmp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 echo**

R1 (config) # **access-list 101 deny icmp 10.40.0.0 0.0.0.255 10.30.0.0 0.0.0.255 echo**

R1 (config) # **access-list 101 permit ip any any**

R1 (config) # **interfaz g0/0/1.40**

R1 (config-subif)# **ip access-group 101 in**

R1 (config) # **access-list 102 observación ACL 102 cumple la política 4**

R1 (config) # **access-list 102 deny icmp 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255 echo**

R1 (config) # **access-list 102 permit ip any any**

R1 (config) # **interfaz g0/0/1.30**

R1 (config-subif)# **ip access-group 102 in**

Cerrar la ventana de configuración

### Compruebe que las listas de acceso implementadas aplican las directivas de seguridad.

Ejecute las siguientes pruebas. Los resultados esperados se muestran en la tabla:

|  |  |  |  |
| --- | --- | --- | --- |
| De | de Internet | Destino | Resultado |
| PC-A | Ping | 10.40.0.10 | Falla |
| PC-A | Ping | 10.20.0.1 | Correcto |
| PC-B | Ping | 10.30.0.10 | Falla |
| PC-B | Ping | 10.20.0.1 | Falla |
| PC-B | Ping | 172.16.1.1 | Correcto |
| PC-B | HTTPS | 10.20.0.1 | Falla |
| PC-B | HTTPS | 172.16.1.1 | Correcto |
| PC-B | SSH | 10.20.0.4 | Falla |
| PC-B | SSH | 172.16.1.1 | Correcto |

Fin del documento

# Configuraciones de dispositivos

# Router R1

R1# **show run**

Building configuration...

Current configuration : 5264 bytes

!

version 16.9

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

platform qfp utilization monitor load 80

no platform punt-keepalive disable-kernel-core

!

hostname R1

!

boot-start-marker

boot-end-marker

!

vrf definition Mgmt-intf

!

address-family ipv4

exit-address-family

!

address-family ipv6

exit-address-family

!

enable secret 5$1$.dkb$dhzfcwc9ttcbwur3lmee10

!

no aaa new-model

!

no ip domain lookup

ip domain name ccna-lab.com

!

!

login on-success log

!

subscriber templating

!

multilink bundle-name authenticated

!

<output omitted>

!

no license smart enable

diagnostic bootup level minimal

!

spanning-tree extend system-id

!

!

username sshAdmin secret 5 $1$829R$mk6kzq/cckw0irnuoa.tm1

!

redundancy

mode none

!

!

interface Loopback1

ip address 172.16.1.1 255.255.255.0

!

interfaz GigabiteThernet0/0/0

no ip address

negotiation auto

!

interface GigabitEthernet0/0/1

no ip address

negotiation auto

!

interfaz GigabiteThernet0/0/1.20

description Management Network

encapsulation dot1Q 20

ip address 10.20.0.1 255.255.255.0

!

interfaz GigabiteThernet0/0/1.30

description Operations Network

encapsulation dot1Q 30

ip address 10.30.0.1 255.255.255.0

ip access-group 102 in

!

interfaz GigabiteThernet0/0/1.40

description Sales Network

encapsulation dot1Q 40

ip address 10.40.0.1 255.255.255.0

ip access-group 101 in

!

interfaz GigabiteThernet0/0/1.1000

description Native VLAN

encapsulation dot1Q 1000 native

!

interface Serial0/1/0

no ip address

!

interface Serial0/1/1

no ip address

!

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

negotiation auto

!

ip forward-protocol nd

no ip http server

ip http authentication local

ip http secure-server

ip tftp source-interface GigabitEthernet0

!

!

ip access-list extended 101

remark ACL 101 fulfills policies 1, 2, and 3

deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 22

deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq www

deny tcp 10.40.0.0 0.0.0.255 host 10.30.0.1 eq www

deny tcp 10.40.0.0 0.0.255 host 10.40.0.1 eq www

deny tcp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 eq 443

deny tcp 10.40.0.0 0.0.0.255 host 10.30.0.1 eq 443

deny tcp 10.40.0.0 0.0.0.255 host 10.40.0.1 eq 443

deny icmp 10.40.0.0 0.0.0.255 10.20.0.0 0.0.0.255 echo

deny icmp 10.40.0.0 0.0.0.255 10.30.0.0 0.0.0.255 echo

permit ip any any

ip access-list extended 102

remark ACL 102 fulfills policy 4

deny icmp 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255 echo

permit ip any any

!

!

control-plane

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password 7 094F471A1A0A

login

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

password 7 14141B180F0B

login local

transport input ssh

!

end

# Router R2

R2# **show run**

Building configuration...

Current configuration : 1660 bytes

!

version 16.9

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

platform qfp utilization monitor load 80

no platform punt-keepalive disable-kernel-core

!

hostname R2

!

boot-start-marker

boot-end-marker

!

!

vrf definition Mgmt-intf

!

address-family ipv4

exit-address-family

!

address-family ipv6

exit-address-family

!

enable secret 5 $1$dklp$GTX20dmmb.e9aczmg74ey1

!

no aaa new-model

!

no ip domain lookup

ip domain name ccna-lab.com

!

!

login on-success log

!

subscriber templating

!

multilink bundle-name authenticated

!

spanning-tree extend system-id

!

username sshAdmin secreto 5 $1$EGZ8$LTF/V6F6x90ALYQMLNYYK/

!

redundancy

mode none

!

!

interfaz GigabiteThernet0/0/0

no ip address

negotiation auto

!

interface GigabitEthernet0/0/1

ip address 10.20.0.4 255.255.255.0

negotiation auto

!

interface Serial0/1/0

no ip address

!

interface Serial0/1/1

no ip address

!

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

negotiation auto

!

ip forward-protocol nd

no ip http server

ip http secure-server

ip tftp source-interface GigabitEthernet0

ip route 0.0.0.0 0.0.0.0 10.20.0.1

!

!

control-plane

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password 7 02050D480809

login

transport input none

stopbits 1

line aux 0

stopbits 1

line vty 0 4

password 7 070C285F4D06

login local

transport input ssh

!

end

# Switch S1

S1# **show run**

Building configuration...

Current configuration : 3361 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 5 $1$bro6$r7vhzdic7ukcy7pkqdrpt.

!

username sshAdmin secreto 5 $1$fvd5$93v97umbqbigyyvm25yro.

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

ip domain-name ccna-lab.com

!

!

spanning-tree mode rapid-pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

interface FastEthernet0/1

switchport trunk allowed vlan 20,30,40,1000

switchport trunk native vlan 1000

switchport mode trunk

!

interface FastEthernet0/2

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/3

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/4

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/5

switchport trunk allowed vlan 20,30,40,1000

switchport trunk native vlan 1000

switchport mode trunk

!

interface FastEthernet0/6

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/7

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/8

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/9

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/10

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/11

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/12

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/14

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/19

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/21

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/22

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/23

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/24

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/1

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/2

switchport access vlan 999

switchport mode access

shutdown

!

interface Vlan1

no ip address

!

interface Vlan20

ip address 10.20.0.2 255.255.255.0

!

ip default-gateway 10.20.0.1

ip http server

ip http secure-server

!

banner motd ^C Authorized Users Only! ^C

!

line con 0

password 7 094F471A1A0A

login

line vty 0 4

password 7 094F471A1A0A

login local

transport input ssh

line vty 5 15

password 7 094F471A1A0A

login

!

end

# Switch S2

S2# **show run**

Building configuration...

Current configuration : 3247 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname S2

!

boot-start-marker

boot-end-marker

!

enable secret 5 $1$GA7R$4qxUHJCSRZgvZesdovpuw.

!

username sshAdmin secreto 5 $1$x0mr$slspheu7xxlv8hw1.bld3.

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

ip domain-name ccna-lab.com

!

!

spanning-tree mode rapid-pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

interface FastEthernet0/1

switchport trunk allowed vlan 20,30,40,1000

switchport trunk native vlan 1000

switchport mode trunk

!

interface FastEthernet0/2

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/3

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/4

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/5

switchport access vlan 20

switchport mode access

!

interface FastEthernet0/6

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/7

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/8

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/9

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/10

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/11

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/12

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/13

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/14

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/15

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/16

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/17

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/18

switchport access vlan 40

switchport mode access

!

interface FastEthernet0/19

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/20

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/21

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/22

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/23

switchport access vlan 999

switchport mode access

shutdown

!

interface FastEthernet0/24

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/1

switchport access vlan 999

switchport mode access

shutdown

!

interface GigabitEthernet0/2

switchport access vlan 999

switchport mode access

shutdown

!

interface Vlan1

no ip address

!

interface Vlan20

ip address 10.20.0.3 255.255.255.0

!

ip default-gateway 10.20.0.1

ip http server

ip http secure-server

!

banner motd ^C Sólo usuarios autorizados ^C ^C

!

line con 0

password 7 030752180500

login

line vty 0 4

password 7 030752180500

login local

transport input ssh

line vty 5 15

password 7 030752180500

login

!

end