

# CONFIGURACIÓN GENERAL

## Configuración del nombre de host

Router>enable	modo privilegiado
Router#config terminal	Modo de Config
Router(config)#hostname myRouter	Nuevo nombre: <i>myRouter</i>

## Configuración de las contraseñas

### Contraseña de acceso a consola

Router>enable	modo privilegiado
Router#config terminal	Modo de Config
Router(config)#line console 0	config consola
Router(config-line)#password cisco	contraseña de acceso
Router(config-line)#login	

### Contraseña de acceso a modo privilegiado

Router>enable	modo privilegiado
Router#config terminal	Modo de Config
Router(config)#enable password cisco	Contraseña: <i>cisco</i>

### Contraseña secreta de acceso a modo privilegiado

Router>enable	modo privilegiado
Router#config terminal	Modo de Config
Router(config)#enable secret cisco	Contraseña: <i>cisco</i>

### Contraseña Terminal virtual (Telnet)

Router>enable	modo privilegiado
Router#config terminal	Modo de Config
Router(config)#line vty 0 4	Config puerto virtual
Router(config-line)#password cisco	Contraseña: <i>cisco</i>
Router(config-line)#login	

## Configuración servidor SSH

```
Router>enable
Router#config terminal
Router(config)#hostname R2
Router(config)#ip domain-name cisco.com
Router(config)#crypto key generate rsa
Router(config)#username felipe secret cisco
Router(config)#line vty 0 4
Router(config-line)#transport input ssh
Router(config-line)#login local
Router(config)#ip ssh time-out 15
Router(config)#ip authentication-retries 2
```

## Mostrar el running-config y mostrar configuraciones

Router>enable

Router#show run

## Guardar cambios

```
Router>enable
Router#copy run start
Router#wr
```

## Guardar cambios

```
Router(config)#line console
Router(dhcp-config)# logging synchronous
```

## Configuración de interfaces

### Configuración de la interfaz FastEthernet 0/0

Router>enable	modo privilegiado
Router#config terminal	Modo de Config
Router(config)#interface fastEthernet 0/0	Config Interfaz
Router(config-if)#ip address 192.168.1.1 255.255.255.0	Asignación IP
Router(config-if)#clockrate 56000	Tasa de transmisión
Router(config-if)#no shutdown	Activación Interfaz

### Configuración de la interfaz WAN Serial 0/0/0

#### Interfaz Serial DCE (Proporciona el reloj)

Router>enable	modo privilegiado
Router#config terminal	Modo de Config
Router(config)#interface Serial x/y/z	Config Interfaz
Router(config-if)#ip address 192.168.50.5 255.255.255.0	Asignación IP
Router(config-if)#clockrate 56000	Tasa de transmisión
Router(config-if)#no shutdown	Activación Interfaz

#### Interfaz Serial DTE

```
Router>enable
Router#config terminal
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address 192.168.50.7 255.255.255.0
Router(config-if)#no shutdown
```

### Interfaz de loopback

```
Router>enable
Router#config terminal
Router(config)#interface loopback number
Router(config-if)#ip address ip-address subnet-mask
```

### Determinar qué extremo del cable DCE o DTE está conectado a esa interfaz serial

```
Router#show controllers serial 0/0/0
```

## Configuración del servidor DHCP

Router(config)#ip dhcp pool POOL1	Pool de direcciones
Router(dhcp-config)#network 192.168.1.0 255.255.255.0	Red para POOL1
Router(dhcp-config)#dns-server 192.168.1.10	Servidor DNS
Router(dhcp-config)#default-router 192.168.1.1	Router por defecto
Router(dhcp-config)#exit	
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.49	

Router(config)#show ip dhcp binding (Mostrar asignaciones DHCP)  
Router(config)#show ip dhcp pool (Mostrar ambitos o pool DHCP)

## Configurar una interfaz del route como cliente DHCP

```
Router#configure terminal
Router(config)#interface f0/0
Router(config-if)#ip address dhcp
Router(config-if)#no shutdown
```

## Relay DHCP

```
Router#configure terminal
Router(config)#interface f0/0
Router(config-if)#ip helper-address 192.168.2.1 (Dirección IP del servidor DHCP)
Router(config-if)#no shutdown
```

## Depuración de DHCP

```
Router(config)#debug ip dhcp server events
```

## Historial de comandos

```
Router#terminal history
Router#terminal history size 50
Router#terminal no history size 50
Router#terminal no history size 50
```

# ENRUTAMIENTO (ROUTING)

## Comportamiento de enrutamiento

```
Router(config)#no ip classless
Router(config)#ip classless
```

## Rutas estáticas

```
Router(config)#ip route [IP Red destino] [Mask red destino] [IP Interfaz siguiente router | Interfaz de salida]
```

### ➤ Verificación de rutas

```
Router#debug ip routing
Router#show ip route
Router#show ip route [Dirección IP de la red]
Router#show run
Router#ping [Ruta de destino]
```

### ➤ Eliminación de rutas:

```
Router(config)#no ip route [IP Red destino] [Mask red destino] [IP Interfaz siguiente router | Interfaz de salida]
```

### ➤ Caso especial para una interfaz de salida fastEthernet

```
R1(config)#ip route 192.168.2.0 255.255.255.0 [Interfaz de salida] [IP Interfaz siguiente router]
```

## Rutas por defecto

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address ]
```

## Enrutamiento dinámico RIP

```
Router>enable
Router#config terminal
Router(config)#router rip
Router(config-router)#network [dirección de red con clase directamente conectada]
```

### ➤ Impedir actualizaciones innecesarias

```
Router(config)#router rip
Router(config-router)#passive-interface FastEthernet 0/0 (No se realiza broadcast por esta interfaz)
```

### ➤ Desactivar RIP

```
Router(config)#no router RIP
```

### ➤ Propagar la ruta estática por defecto "quad-zero" en las actualizaciones RIP

```
Router(config-router)#default-information originate
```

➤ **Enviar fuente de enrutamiento estático a otra fuente de enrutamiento**

```
Router(config-router)#redistribute static
```

➤ **Rip versión 2**

```
Router(config)#router rip  
Router(config-router)#version 2
```

➤ **Deshabilitar el resumen automático de rutas**

```
Router(config)#router rip  
Router(config-router)#no auto-summary
```

➤ **Verificación y resolución de problemas:**

```
Router#show ip interface brief  
Router#show ip route  
Router#show ip protocols  
Router#debug ip rip  
Router#show ip rip database  
Router#undebug all
```

**NOTA:** Las siguientes recomendaciones son útiles para la solución de problemas:

1. Asegúrese de que todos los enlaces (interfaces) estén activados y en funcionamiento.
2. Verifique el cableado.
3. Verifique que tiene la máscara de subred y dirección IP correcta en cada interfaz.
4. Elimine los comandos de configuración que sean innecesarios o se hayan reemplazado con otros comandos.

## Enrutamiento dinámico EIGRP

**NOTA:** EIGRP utiliza los siguientes valores en su métrica compuesta para calcular la ruta preferida hacia una red:

- Ancho de banda
- Retraso
- Confiabilidad
- Carga

```
Router(config)#router eigrp [autonomous-system]  
Router(config-router)#network [dirección de red con clase directamente conectada]
```

➤ **No incluir interfaz en EIGRP**

```
Router(config-router)#network network-address [wildcard-mask]  
R2(config-router)#network 192.168.10.8 0.0.0.3
```

➤ **Modificar el ancho de banda**

```
Router(config-if)#bandwidth [kilobits]
```

➤ **Verificación y resolución de problemas:**

```
Router#show ip eigrp neighbors (Muestra los vecinos EIGRP)
Router#show ip protocols
Router#show ip route
Router#show interface (Visualización de BW y del retraso)
Router#show ip eigrp topology
Router#show ip eigrp topology [Network]
```

## Enrutamiento dinámico OSPF

```
Router(config)#router ospf [process ID]
Router(config-router)#network [network-address] [wildcard-mask] area [area-id]
```

### ➤ Configuración manual del Router-ID

```
Router(config)#router ospf process-id
Router(config-router)#router-id ip-address
```

### ➤ Volver a cargar el router

```
Router#clear ip ospf process
```

### ➤ Verificación y resolución de problemas:

```
Router#show ip protocols (Visualizar Router ID)
Router#show ip route
Router#show ip ospf
Router#show ip ospf interface
Router#show ip ospf neighbor
```

### ➤ Modificar el costo:

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip ospf cost 1562
```

### ➤ Propagar la ruta estática por defecto "quad-zero" en las actualizaciones RIP

```
Router(config)#router ospf [process ID]
Router(config-router)#default-information originate
```

### ➤ Forzar la prioridad de una interfaz

**NOTA:** Debido a que las prioridades son un valor específico según la interfaz, suministran un mejor control de las redes de accesos múltiples de OSPF. También permiten a un router ser DR en una red y DROther en otra.

```
Router(config-if)#ip ospf priority {0 - 255}
```

### ➤ Modificación de intervalos OSPF

```
Router(config-if)#ip ospf hello-intervalseconds
Router(config-if)#ip ospf dead-intervalseconds
```

## RECUPERAR CONTRASEÑAS

1. Detener el boot (puede hacerse mediante ctrl+espacio o si usas teraterm control -> send break).
2. Ejecutar el comando: Rommon1>**confreg 0x2142** (hacemos que el router al arrancar no cargue la configuración).
3. Ejecutamos el comando Rommon2>**reset** (reiniciamos el router).
4. Al iniciar preguntará si se desea usar un asistente para la configuración rápida, nosotros de momento decimos que **no**.
5. Router#**enable**
6. Router#**erase startup-config** (borra la configuración inicial)
7. Router#**conf t** (comenzamos a configurar)
8. Router(config)#**config-register 0x2102** (para dejar el registro tal cual estaba originalmente, y poder cargar la configuración en los sucesivos arranques, deshacer lo anterior hecho vamos).
9. Reiniciar sin guardar configuración y sin volver a parar el boot. Para esto ejecutamos el siguiente comando: Router#**reload**

# COMANDOS DE CONFIGURACIÓN DE SWITCHES

## Configurar Interfaz de administración

```
Switch#configure terminal
Switch(config)#interface vlan 99
Switch(config-if)#ip address [direccion IP] [mask]
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#configure terminal
Switch(config)#interface fastethernet 0/18
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
```

## Configurar gateway predeterminada

```
Switch#configure terminal
Switch(config)#ip default-gateway [IP address]
Switch(config)#end
```

## Verificar configuracion

```
Switch#show run
Switch#show ip interface brief
```

## Función automática de conexión cruzada de interfaz

```
Switch#mdix auto
```

## Configurar dúplex y velocidad

```
Switch#configure terminal
S1(config)#Interface fastethernet 0/1
S1(config-if)#duplex auto
S1(config-if)#speed auto
S1(config-if)#end
```

## Configurar una interfaz Web

```
S1#configure terminal
S1(config)#ip http authentication enable
S1(config)#ip http server
S1(config)#end
```

## Administración de la tabla de direcciones MAC

```
Switch#show mac-address-table
Switch#mac-address-table static <dirección MAC> vlan {1-4096, ALL} interface ID de interfaz (Este es un ejemplo de asignación estática en la tabla de direcciones MAC)
Switch#no mac-address-table static <dirección MAC> vlan {1-4096, ALL} interface ID de interfaz (Eliminar entrada)
```



## Comandos show

```
Switch#show interfaces [interface ID]
Switch#mac-address-table static <dirección MAC> vlan {1-4096, ALL} interface ID de interfaz (Este es un ejemplo de asignación estática en la tabla de direcciones MAC)
Switch#no mac-address-table static <dirección MAC> vlan {1-4096, ALL} interface ID de interfaz (Eliminar entrada)
```

## Respalidar y restaurar el Switch

```
Switch#copy startup-config flash:filename (Guarda la configuración en la flash con otro nombre)
Switch#copy startup-config flash:config.bak1 (ejemplo)
```

### Restaurar la copia de seguridad

```
Switch#copy flash:config.bak1 startup-config
Switch#reload
Se ha modificado la configuración del sistema. Save? [yes/no]: n
Proceed with reload? [confirm]?
```

### Copia de seguridad de seguridad con servidor TFTP

Para subir un archivo de configuración del switch al servidor TFTP para su almacenamiento, se deberán seguir los siguientes pasos:

**Paso 1.** Verifique que el servidor TFTP se esté ejecutando en la red.

**Paso 2.** Inicie sesión en el switch a través del puerto de consola o sesión Telnet. Habilite el switch y luego haga ping al servidor TFTP.

**Paso 3.** Suba la configuración del switch en el servidor TFTP. Especifique la dirección IP o el nombre de host del servidor TFTP y el nombre del archivo de destino. El comando del IOS de Cisco es:

```
Switch#copy system:running-config tftp:[[/ubicación]/directorio]/nombre del archivo] o
Switch#copy nvram:startup-config tftp:[[/ubicación]/directorio]/nombre del archivo]
```

### Restauración configuración con servidor TFTP

**Paso 1.** Copie el archivo de configuración en el correspondiente directorio del servidor TFTP (si es que ya no se encuentra allí).

**Paso 2.** Verifique que el servidor TFTP se esté ejecutando en la red.

**Paso 3.** Inicie sesión en el switch a través del puerto de consola o sesión Telnet. Habilite el switch y luego haga ping al servidor TFTP.

**Paso 4.** Descargue el archivo de configuración del servidor TFTP para configurar el switch. Especifique la dirección IP o el nombre de host del servidor TFTP y el nombre del archivo que desea descargar. El comando del IOS de Cisco es:

```
Switch#copy tftp:[[/ubicación]/directorio]/nombre del archivo] system:running-config o
Switch#copy tftp:[[/ubicación]/directorio]/nombre del archivo] nvram:startup-config
```

## Eliminar archivos

```
Switch#erase nvram:
Switch#erase startup-config
Switch#delete flash: filename
```

## Recuperación de contraseñas

Para recuperar la contraseña de un switch Cisco 2960, lleve a cabo los siguientes pasos:

**Paso 1.** Conecte un terminal o PC, con el software de emulación de terminal, al puerto de consola del switch.

**Paso 2.** Establezca la velocidad de línea del software de emulación en 9600 baudios.

**Paso 3.** Apague el switch. Vuelva a conectar el cable de alimentación al switch y, en no más de 15 segundos, presione el botón **Mode** mientras la luz verde del LED del sistema esté parpadeando. Siga presionando el botón **Mode** hasta que el LED del sistema cambie al color ámbar durante unos segundos y luego verde en forma permanente. Suelte el botón Mode.

**Paso 4.** Inicialice el sistema de archivos Flash a través del comando **flash\_init**.

**Paso 5.** Cargue archivos helper mediante el comando **load\_helper**.

**Paso 6.** Visualice el contenido de la memoria Flash a través del comando **dir flash**:

Se mostrará el sistema de archivos del switch:

```
Directory of flash:/  
13 drwx 192 Mar 01 1993 22:30:48 c2960-lanbase-mz.122-25.FX  
11-rwx 5825 Mar 01 1993 22:31:59 config.text  
18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat  
16128000 bytes total (10003456 bytes free)
```

**Paso 7.** Cambie el nombre del archivo de configuración por config.text.old, que contiene la definición de la contraseña, mediante el **comando rename flash:config.text flash:config.text.old**.

**Paso 8.** Reinicie el sistema con el comando **boot**.

**Paso 9.** Se solicitará que ejecute el programa de configuración inicial. Ingrese N ante la solicitud y, luego, cuando el sistema pregunte si desea continuar con el diálogo de configuración, ingrese N.

**Paso 10.** Ante la indicación de switch, ingrese al modo EXEC privilegiado por medio del comando **enable**.

**Paso 11.** Cambie el nombre del archivo de configuración y vuelva a colocarle el nombre original mediante el comando **rename flash:config.text.old flash:config.text**.

**Paso 12.** Copie el archivo de configuración en la memoria a través del comando **copy flash:config.text system:running-config**. Después de ingresar este comando, se mostrará el siguiente texto en la consola:

```
Source filename [config.text]?  
Destination filename [running-config]?
```

Presione Enter en respuesta a las solicitudes de confirmación. El archivo de configuración se ha cargado nuevamente y, ahora, se puede cambiar la contraseña.

**Paso 13.** Ingrese al modo de configuración global mediante el comando **configure terminal**.

**Paso 14.** Cambie la contraseña mediante el comando **enable secret password**.

**Paso 15.** Regrese al modo EXEC privilegiado mediante el comando **exit**.

**Paso 16.** Escriba la configuración en ejecución en el archivo de configuración de inicio mediante el comando **copy running-config startup-config**.

**Paso 17.** Vuelva a cargar el switch mediante el comando **reload**.

## Configurar mensaje

```
S1(config)#banner login "¡Personal autorizado únicamente!"  
S1(config)#banner motd "¡El mantenimiento del dispositivo se realizará el viernes!"
```

## Configuración de SSH

```
Switch(config)#configure terminal.  
Switch(config)#hostname nombre de host.  
Switch(config)#ip domain-name nombre de dominio.  
Switch(config)#crypto key generate rsa  
Switch(config)#ip ssh version 2  
Switch(config)#line vty 0 15  
Switch(config-line)#transport input SSH
```

## Snooping de DHCP

**Paso 1.** Habilitar el snooping de DHCP mediante el comando de configuración global **ip dhcp snooping**.

**Paso 2.** Habilitar el snooping de DHCP para VLAN específicas mediante el comando **ip dhcp snooping vlan number [número]**

**Paso 3.** Definir los puertos como confiables o no confiables a nivel de interfaz identificando los puertos confiables mediante el comando **ip dhcp snooping trust**

**Paso 4.** (Opcional) Limitar la tasa a la que un atacante puede enviar solicitudes de DHCP bogus de manera continua a través de puertos no confiables al servidor de DHCP mediante el comando **ip dhcp snooping limit rate rate**

## Configurar costos de los puertos en STP (Spanning Tree Protocol)

```
Switch(config)#interface f0/1  
Switch(config-if)#spanning-tree cost 25
```

## Verificar costos de los puertos en STP (Spanning Tree Protocol)

```
Switch#show spanning-tree  
  
Switch#show spanning-tree detail
```

## Configurar y verificar el BID en STP (Spanning Tree Protocol)

```
Switch(config)#spanning-tree vlan [vlan-id] root primary (asegurar que el switch posea el menor valor de prioridad de puente)  
Switch(config)#spanning-tree vlan vlan-id root secondary (Configurar Puente raíz alternativo)  
Switch(config)#spanning-tree vlan vlan-id root 24576 (Método 2 para forzar la prioridad)
```

**NOTA:** El valor de prioridad se configura en incrementos de 4096 entre 0 y 65536

## Configurar y verificar el BID en STP (Spanning Tree Protocol)

```
Switch(config)#interface f0/1  
Switch(config-if)#spanning-tree port priority  
Switch(config-if)#end
```

## Configurar PortFast en STP (Spanning Tree Protocol)

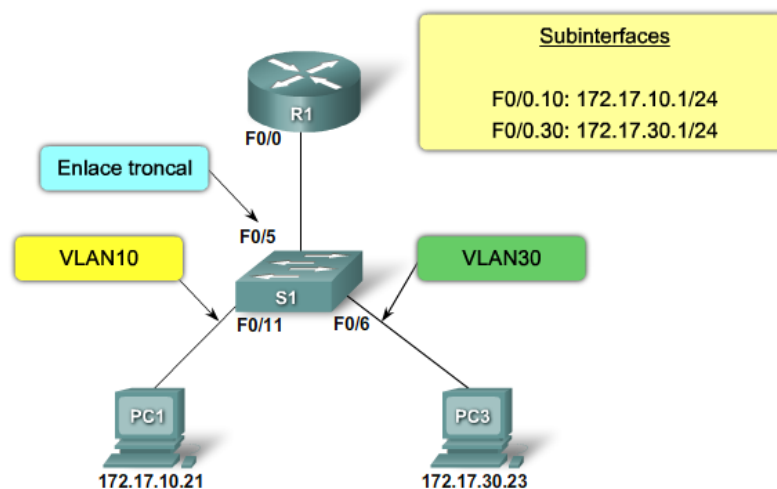
```
Switch(config)#interface f0/5
Switch(config-if)#spanning-tree portfast
Switch(config-if)#end
```

```
Switch(config)#interface f0/5
Switch(config-if)#no spanning-tree portfast
Switch(config-if)#end
```

```
Switch#show run
```

**NOTA:** Usado para que los puertos entren en estado de ENVIAR antes de que la red Spanning tree converja.

## Enrutamiento inter VLAN



### Configuración de la subinterfaz en el Router

```
Router(config)#interface f0/0.10 (Subinterfaz 10)
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 172.16.10.1 255.255.255.0
Router(config)#interface f0/0.20 (Subinterfaz 10)
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 172.16.20.1 255.255.255.0
```

```
Router(config-subif)#interface f0/0
Router(config-if)#no shutdown
```

**NOTA:** La configuración de las subinterfaces del router es similar a la configuración de las interfaces físicas, excepto que es necesario crear la subinterfaz y asignarla a una VLAN.

### Configuración del switch para el enrutamiento inter VLAN

```
Switch(config)#vlan 10
Switch(config-vlan)#vlan 30
Switch(config-vlan)#exit
Switch(config)#interface f0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan [vlan id]
Switch(config)#interface f0/5
Switch(config-if)#switchport mode trunk
```

### Comandos de verificación del Switch

```
Switch#show interface interface-id switchport  
Switch#show running config
```

### Comandos de verificación del Router

```
Switch#show interface  
Switch#show run  
Switch#show vlan
```

## CCNA4: ACCESO A LA WAN

### Configuración PPP

Router(config-if)#encapsulation ppp (Habilitar PPP en una interfaz)  
Router(config-if)#compress [predictor | stac] (Configurar compression)  
Router(config-if)#ppp quality *porcentaje* (Configurar la calidad del enlace)

NOTA: La calidad de salida se calcula al comparar la cantidad total de paquetes y bytes enviados con la cantidad total de paquetes y bytes recibidos por el nodo de destino. La calidad de entrada se calcula al comparar la cantidad total de paquetes y bytes recibidos con la cantidad total de paquetes y bytes enviados por el nodo de destino.

Router(config-if)#ppp authentication pap

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed]
[list-name | default] [callin]
```

#### El comando ppp authentication

<b>chap</b>	Habilita CHAP en una interfaz serial.
<b>pap</b>	Habilita PAP en una interfaz serial.
<b>chap pap</b>	Habilita CHAP y PAP y realiza la autenticación de CHAP antes que la de PAP.
<b>pap chap</b>	Habilita CHAP y PAP y realiza la autenticación de PAP antes que la de CHAP.
<b>if-needed</b> (opcional)	Usado con TACACS y XTACACS. No realice la autenticación CHAP o PAP si el usuario ya ha proporcionado la autenticación. Esta opción está disponible sólo en interfaces asíncronas.
<b>list-name</b> (opcional)	Usado con AAA/TACACS+. Especifica el nombre de una lista de métodos TACACS+ de nombre de lista auténtico, el sistema utiliza la opción predeterminada. Las listas se crean con el comando <b>aaa authentication ppp</b> .
<b>default</b> (opcional)	Usado con AAA/TACACS+. Creado con el comando <b>aaa authentication ppp</b> .
<b>callin</b>	Especifica la autenticación sólo en las llamadas entrantes (recibidas).

Router(config-if)#ppp multilink (Configurar PPP multienlace)  
Router#show interfaces serial (Verificar configuración PPP)  
Router#debug ppp (debug PPP)

```
debug ppp {packet | negotiation | error | authentication | compression |  
         cbcp}
```

Parámetro	Uso
paquete	Muestra los paquetes PPP enviados y recibidos. (Este comando muestra las descargas de los paquetes de bajo nivel).
negociacin	Muestra los paquetes PPP enviados durante el inicio de PPP, cuando se negocian las opciones de PPP.
error	Muestra los errores de protocolo y las estadísticas de error relacionadas con la negociación y operación de la conexión PPP.
autenticacin	Muestra mensajes de protocolo de autenticación, incluidos los intercambios de paquetes del protocolo de autenticación de señales (CHAP, Challenge Authentication Protocol) y del protocolo de autenticación de contraseña (PAP, Password Authentication Protocol).
compresin	Muestra información específica para el intercambio de conexiones PPP mediante MPPC. Este comando es útil para obtener información sobre los números de secuencias de los paquetes incorrectos cuando la compresión MPPC se encuentra habilitada.
cbcp	Muestra los errores de protocolo y las estadísticas relacionadas con las negociaciones de conexión PPP mediante el uso de MSCB.

Router#undebug all

(desactiva debug PPP)

## Frame Relay

### Configuración de Frame relay

```
Router(config)#int s0/0/0
Router(config-if)#ip address [ip] [mask]
Router(config-if)#encapsulation frame-relay
Router(config-if)#bandwidth 64
```

### Asignación de direcciones estáticas Frame relay

```
Router(config)#int s0/0/0
Router(config-if)#ip address [ip] [mask]
Router(config-if)#encapsulation frame-relay
Router(config-if)#bandwidth 64
Router(config-if)#no frame-relay inverse-arp
Router(config-if)# frame-relay map protocol protocol-address dlci [broadcast] [ietf] [cisco]
Router(config-if)#no shutdown
```

NOTA: Use la palabra clave ietf al conectarse a un router no perteneciente a Cisco.

La opción [broadcast] Permite broadcasts y multicasts por medio de VC. Esto permite el uso de protocolos de enrutamiento dinámico en el VC.

```
Router#show frame relay map (Verificación de un mapa estático frame relay)
Router#show frame-relay lmi
```

NOTA: LMI es un mecanismo activo que proporciona información de estado sobre las conexiones Frame Relay entre el router (DTE) y el switch Frame Relay (DCE). Cada 10 segundos aproximadamente, el dispositivo final sondea la red en busca de una respuesta de secuencia no inteligente o información de estado de canal.

```
Router(config-if)#frame-relay lmi-type [cisco | ansi | q933a] (Configurar el tipo de LMI)
```

NOTA: La configuración del tipo de LMI deshabilita la función de detección automática.

```
Router(config-if)#keepalive (Cambiar el intervalo activo)
```

### Configuración de las interfaces punto a punto

**Paso 1.** Quitar cualquier dirección de capa de red asignada a la interfaz física. Si la interfaz física tiene una dirección, las subinterfaces locales no reciben las tramas.

**Paso 2.** Configurar la encapsulación Frame Relay en la interfaz física mediante el comando encapsulation frame-relay.

**Paso 3.** Para cada uno de los PVC definidos, crear una subinterfaz lógica. Especifique el número de puerto, seguido de un punto (.), y luego del número de la subinterfaz. Para solucionar problemas con más facilidad, se sugiere que el número de la subinterfaz coincida con el número de DLCI.

**Paso 4.** Configurar una dirección IP para la interfaz y el ancho de banda.

En este punto, configuraremos el DLCI. Recuerde que el proveedor de servicios de Frame Relay asigna los números de DLCI.

**Paso 5.** Configurar el DLCI local en la subinterfaz mediante el comando frame-relay interface-dlci.

```
R1(config-if)#interface serial 0/0/0.103 point-to-point
R1(config-subif)#frame-relay interface-dlci 103
```

### Verificación del funcionamiento de frame relay

```
Router#show interfaces
Router#show frame-relay lmi
Router#show frame-relay pvc 102
Router#show frame-relay map
```



Router#debug frame-relay lmi

## ACL: Listas de control de acceso

### Configuración de las ACL estándar

Router(config)#access-list *número-de-lista-de-acceso* deny permit remark origen [wildcard origen] [log]

Por ejemplo, para crear una ACL numerada nombrada 10 que permita la red 192.168.10.0 /24, debe ingresar:

R1(config)#access-list 10 permit 192.168.10.0

### Eliminar access list

R1(config)# no access-list 10

### Aplicar ACLs estándar a interfaces

Router(config-if)#ip access-group {número de lista de acceso | nombre de lista de acceso} {in | out}

### Restringir el acceso vty

Router(config-line)#access-class access-list-number {in [vrf-also] | out}

### Creación de ACLs estándar nombradas

```
Router(config)#ip access-list standard NO_ACCESS
Router(config-std-nacl)#deny host 192.168.11.10
Router(config-std-nacl)#permit 192.168.10.0 0.0.0.255
Router(config-std-nacl)#int f0/0
Router(config-if)#ip access-group NO_ACCESS out
```

### Creación de ACLs extendidas

Router(config)#access-list *number* {permit | deny} protocolo origen wildcard\_de\_origen [operador] [puerto] destino wildcard\_de\_destino [operator *operand*] [puerto] [established]

*Ejemplos:*

```
access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
```

- La ACL 103 permite el tráfico que ingresa de cualquier dirección en la red 192.168.10.0 para dirigirse a cualquier destino, sujeto a la limitación que el tráfico se dirige solo a los puertos 80 (HTTP) y 443 (HTTPS).
- La ACL 104 lo hace bloqueando el tráfico entrante, a excepción de las conexiones establecidas

*Ejemplo de denegación de FTP de una 192.168.10.0 a 192.168.11.0*

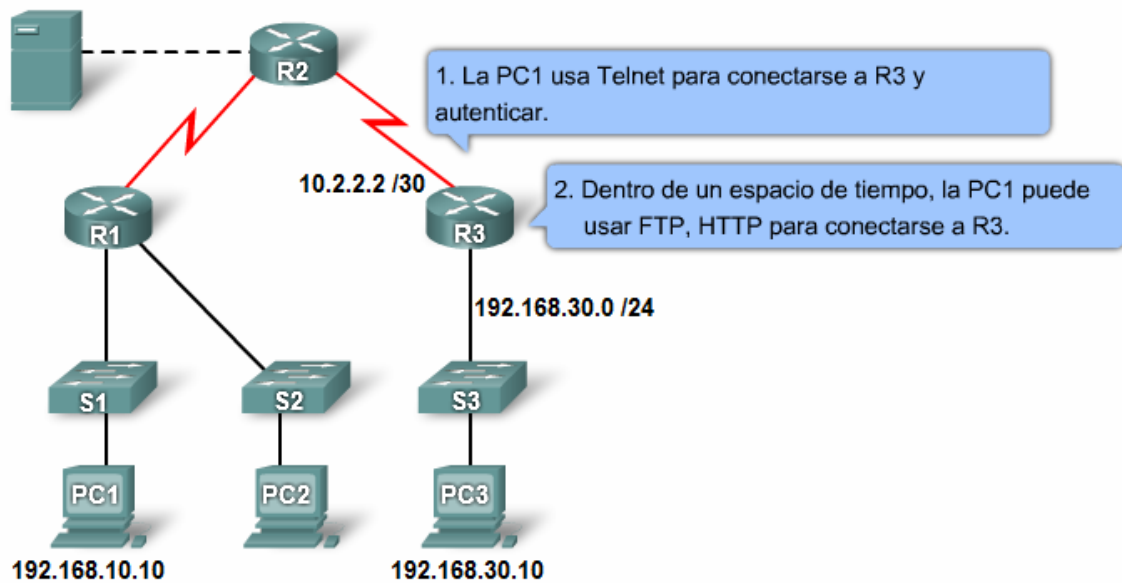
```
access-list 100 deny tcp 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255 eq 21
access-list 100 deny tcp 192.168.10.0 0.0.0.255 192.168.11.0 0.0.0.255 eq 20
```

### Creación de ACLs extendidas nombradas

```
Router(config)#ip access-list extended SURFING
Router(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 80
```

```
Router(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq 443
```

## ACL dinámicas



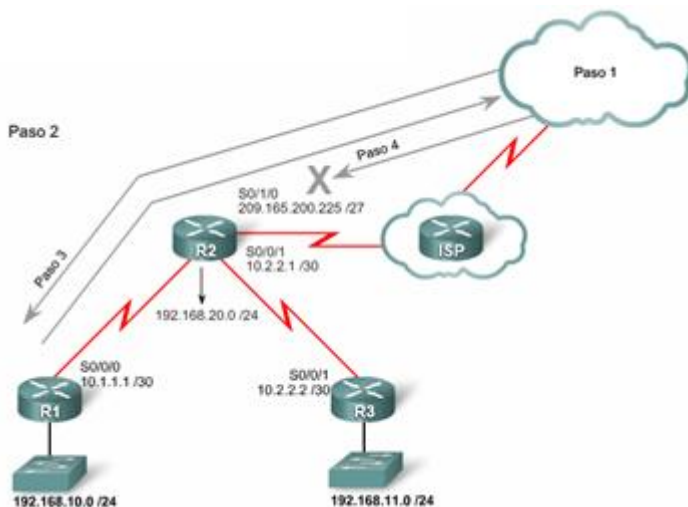
```
Router(config)#username felipe password 0 BBBbbb111
Router(config)#access-list 101 permit any host 10.2.2.2 eq telnet
Router(config)#access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

**NOTA:** La ACL fue creada para permitir el acceso a la red 192.168.30.0 durante 15 minutos

```
Router(config)#int s0/0/1
Router(config)#ip access-group 101 in

Router(config)#line vty 0 4
Router(config-line)#login local
Router(config-line)#autocommand access-enable host timeout 5
```

## ACL Reflexivas



```
Router(config)#ip access-list extended OUTBOUNDFILTERS
Router(config-ext-nacl)#permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC
Router(config-ext-nacl)#permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC

Router(config)#ip access-list extended INBOUNDFILTERS
```

```
Router(config-ext-nacl)#evaluate TCPTRAFFIC
Router(config-ext-nacl)#evaluate ICMPTRAFFIC
```

```
Router(config)#interface s0/1/0
Router(config-if)#ip access-group INBOUNDFILTERS in
Router(config-if)#ip access-group OUTBOUNDFILTERS out
```

### **ACL basadas en tiempo**

```
Router(config)#time-range THREEDAYS (El nombre del rango que se definirá será THREEDAYS)
Router(config-time-range)#periodic Monday Wednesday Friday 8:00 to 17:00
Router(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range THREEDAYS
Router(config)#int s0/0/0
Router(config-if)#ip access-group 101 out
```