Unidad 5

Configuración y administración básica de routers y switches

Planificación y Administración de Redes

5

Índice

Introducción

A lo largo de las unidades anteriores hemos visto los diferentes niveles del modelo OSI y sus aplicaciones, así como los dispositivos en los que se basa la red para su correcto funcionamiento.

Bien, en este apartado hemos visto dos principales dispositivos dedicados a la interconexión de redes como son los switches y los routers.

Los primeros funcionan en la capa 2 del modelo OSI y nos dan una interconexión a nivel generalmente de red interna con la intención de distribuir esta de forma equitativa y así evitar futuras complicaciones.

A lo largo de la unidad veremos que hay diferentes configuraciones y tipos de switches dependiendo de la función que queramos que realice.

En el caso de los routers, su función es la de encaminar las tramas de la red hasta su correcto destino, generalmente internet.

Dentro de estos veremos que hay diversos tipos que podemos trabajar y se tratarán a lo lago de la unidad. Al igual que hablaremos de la arquitectura de estos y de todos los modos que tienen para su configuración.

Por último, nos basaremos en el programa CISCO Packet Tracert para hacer todas las prácticas que durante la unidad se plantean.

Al finalizar esta unidad

- Conoceremos cómo funciona un switch y sus principales características.
- Podremos distinguir las principales técnicas de reenvió que usan los switches.
- Sabremos que tipos de switches existen y como realizar una configuración básica con ellos.
- Conoceremos la arquitectura de un router y cómo funciona.
- Diferenciaremos las funciones de un router y como se clasifican según su funcionamiento.
- Podremos configurar los diferentes modos de un router.

5.1. El switch

5.1.1. Funcionamiento

Un switch es capaz de realizar las siguientes tareas:

- Aprendizaje de direcciones MAC
- Inundación de tramas.
- Actualización de direcciones MAC
- Reenvío selectivo de tramas.
- Filtrado de tramas.
- Evitar los bucles con otros switches (STP).

Aprendizaje de direcciones MAC

Todos los switches contienen una tabla dinámica que se guarda en memoria RAM y que asocia cada puerto con la dirección MAC del equipo al que conecta. Esta tabla estará vacía en primera instancia.

El comando para visualizar esta tabla es:

```
show mac address-table
```

```
Switch>
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Switch>
```

Imagen 1. Prompt de un switch

Si creáramos una red como la siguiente:

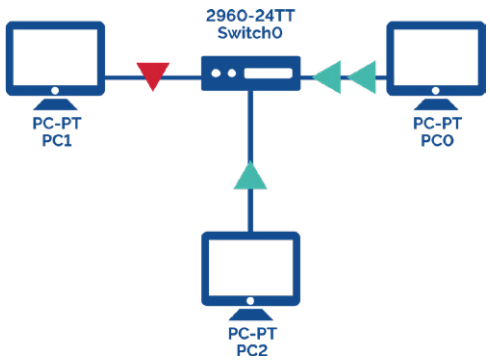

Imagen 2. Estructura de tres ordenadores conectados a un switch

Entonces los equipos se conectarían entre sí. Esta conexión haría que cuando haya un primer envío de tramas, si la dirección no está contemplada en la tabla, se añadiría una nueva entrada con la MAC del cada equipo y los puertos que conectan con cada uno de estos.

Inundación de tramas

Cada vez que el switch recibe una trama y no sabe cuál es el puerto asociado a la dirección MAC marcada como destino, se lleva a cabo la inundación de tramas. Este proceso consiste en mandar la trama a todos los puertos del switch menos al que ha enviado la trama.

Cuando llegue al equipo propietario de esa MAC la trama, este avisará al switch para que añada la asociación MAC y puerto a la tabla antes nombrada.

Para editar un switch debemos primero de activar la configuración, para lo que se usa el comando `enable`.

```
Switch>enable
Switch#
```

Imagen 3. Comando enable

Si queremos borrar la tabla de direcciones MAC, usaremos el siguiente comando:

```
clear mac address-table
```

```
Switch#clear mac address-table
```

Imagen 4. Comando para borrar tabla de máscaras de red

Puede que un equipo quiera enviar una trama a todos los equipos de la red y entonces la MAC de destino sea la dirección de difusión, que es 0xFFFFFFFFFFFF, y en este caso el switch también llevará a cabo una inundación de tramas.

Actualización de direcciones MAC

Cuando se produce una entrada dinámica en la tabla de direcciones MAC, estos tienen un tiempo de vida limitado y predeterminado que cuando expira, la entrada se borra. Para que no pase esto, cada vez que una trama pasa a través del switch, la tabla se actualiza.

Por ejemplo, en el software usado en este módulo, Cisco Packet Tracer, el tiempo de vida es de 5 minutos, es decir, si pasado este tiempo no se actualiza la tabla, la entrada se borra.

Muchas veces el administrador quiere que esto no suceda, y es para eso para lo que se definen las entradas estáticas. Estas entradas son definidas por parte del usuario. Estas mismas entradas no tienen tiempo de vida y permanecen para siempre en la tabla a no ser que se eliminen manualmente.

Vamos a ver como añadir una entrada estática en nuestra tabla, para eso seguimos el siguiente proceso:

1. Lo primero es habilitar el switch como vimos en la entrada anterior.
2. Una vez realizado esto procedemos a entrar en el modo de configuración del switch. Para esto se usa el comando: `conf term`

```
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
```

Imagen 5. Configure terminal

3. El comando para poder añadir una entrada estática es:

   `mac address-table static dirección_mac vlan id interface puerto`

4. Si ahora queremos ver la tabla de direcciones, esto nos da un error debido a que estamos en el modo de visualización.

```
Switch(config)#mac address-table static 7685.5000.da3a vlan 1 interface FastEthernet0/3
Switch(config)#show mac address-table
              ^
% Invalid input detected at '^' marker.
```

Imagen 6. Añadir MAC estática

5. Para salir del modo de configuración usamos el comando `exit`.

6. Y entonces sí que podemos comprobar la tabla de direcciones.

```
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    7685.5000.da3a    STATIC      Fa0/3
```

Imagen 7. Comprobar la lista de direcciones MAC

7. Para poder borrar las entradas, deberemos de volver a ingresar en modo de configuración.

8. El comando es igual que el anterior, pero añadiendo `no`, delante.

```
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no mac address-table static 7685.5000.da3a vlan 1 interface FastEthernet0/3
Switch(config)#
```

Imagen 8. Borrado de direcciones MAC

Reenvío selectivo

Esta es la principal función de un switch, que trata de detectar la trama que llega, comprobar a que dirección debe de ser enviada, ver la lista de direcciones MAC y entonces mandar la trama por la opción correcta.

Filtrado de tramas

Hay ocasiones en las que el switch decide que en vez de enviar la trama es mejor que sea descartada, lo que se conoce como filtrado de trama. El filtrado se usa, por ejemplo, en las siguientes situaciones:

- El switch nunca va a reenviar una trama por el mismo puerto por el que llegó.
- Si hay una trama corrupta o errónea.
- Si durante la comprobación de errores CRC se encuentra un fallo.
- Si por seguridad se ha bloqueado una de las MAC o algún puerto.

El filtrado de seguridad nos da lugar a hablar de la aplicación de seguridad a un puerto:

Vamos a establecer un ejemplo en el que el puerto 3 solo pueda recibir tramas de la dirección MAC que nombrábamos antes como estática.

1. Lo primero que debemos de hacer es habilitar el switch y entrar en la interfaz de configuración.
2. Después, debemos de ingresar en la configuración propia del mismo puerto, eso se hace con el comando: `Interface puerto`

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Fa0/3
Switch(config-if)#
```

Imagen 9. Entrat en una interfaz del switch

3. Ahora lanzamos estos tres comandos seguidos para establecer el modo de seguridad comentado:

   ```
   switchport mode access

   switchport port-security

   switchport port-security mac-address dirección_MAC
   ```

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 7685.5000.da3a
Switch(config-if)#
```

Imagen 10. Modo de seguridad de un puerto

4. Si ahora queremos comprobar esta configuración, lo primero que hacemos es salir de la configuración del switch.
5. Una vez fuera, lanzamos el comando:

   ```
   show port-security interface Fa0/3
   ```

```
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show port-security interface Fa0/3
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Switch#
```

Imagen 11. Mostrar seguridad de un puerto

6. Por último, para poder desactivar el puerto, volvemos a ingresar en la configuración de la interfaz.
7. Para desactivarla lanzamos el comando `shutdown`.
8. Para poder activarla de nuevo usamos `no shutdown`.

```
Switch(config-if)#interface Fa0/3
Switch(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
Switch(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to down
Switch(config-if)#
```

Imagen 12. Activación/Desactivación de una interfaz

Evitar bucles mediante el protocolo STP

Cuando en una organización tenemos varios switches, se recomienda que entre ellos haya una serie de redundancias. Esto es con el fin de que no haya congestiones o si alguno de ellos falla, la red no se caiga y se pueda seguir funcionando con relativa normalidad. Esto, aunque ayuda, también conlleva una serie de problemas, puesto que la redundancia crea ciertos bucles que, en caso de tramas de difusión, pueden provocar la llamada tormenta de broadcast, que se trata de la trama circulando de manera indefinida por la red.

El protocolo STP o Spanning Tree Protocol ayuda en la evitación de estos bucles. Su función es la de bloquear ciertas interfaces de los switches que causan los bucles para desprendernos de ellos. Este protocolo es transparente para el usuario, y una vez configurado funciona de manera automática. La manera en la que bloquea los puertos es automática y estos cambian si cambia la red por cualquier motivo como por ejemplo la adición de un nuevo switch.

El único inconveniente de este protocolo es que es algo lento, pero para eso se han implementado algunas variantes de este como RSTP (Rapid Spanning Tree Protocol) o SPB (Shortest Path Bridging).

Hay ocasiones en las que, por la necesidad de la red, el STP cambia las topologías de la red.

5.1.2. Características del switch

Las características de un switch son las siguientes:

Rendimiento de la red

- Cuando el switch ya conoce cuál es la situación de cada uno de los equipos, entonces enviará las tramas solo a su correspondiente destinatario, lo que se conoce como reenvío selectivo. Esto hará que el tráfico innecesario se reduzca en gran medida y el ancho de banda de cada puerto siga estable.
- Su capacidad de procesamiento de tramas es muy alta, pudiendo procesar millones por segundo. Esto es debido a que utiliza conmutación por circuitos integrados de aplicación específica (ASIC). Su tasa de reenvío es muy alta.
- Consta de comunicación full-dúplex, es decir, puede enviar y recibir información por el mismo cable. Si le conectamos un hub también podría funcionar en modo half-dúplex.
- Si solo usamos switches para la comunicación entre equipos, esto será un entorno libre de colisiones porque, aunque varios equipos intenten transmitir a la vez, el switch secuenciará las tramas.

Seguridad en la red

- El reenvío selectivo del que antes hablábamos hace que el número de tramas que sean sensibles de ser interceptadas baje ampliamente.
- La seguridad establecida en los puertos anula que un equipo no autorizado se conecte a la red.

Funcionalidad

- Auto-sensing. Detecta la velocidad de cada uno de los equipos que tenemos conectados y permite que cada puerto trabaje a velocidad distinta.
- Auto-MDI/MDI-X. Se pueden usar tanto cables cruzados como paralelos para la interconexión de equipos y switches.
- La gestión del switch se puede hacer de manera remota, facilitando el trabajo del administrador de la red.
- Casi todos los switches modernos permiten la creación de algunas VLAN para la segmentación de la red.
- Power over Ethernet o PoE. Esto permite que el switch además de transmitir datos transmita electricidad, es decir, que no sea necesario que un dispositivo conectado a este necesite de dobles conexiones a red y a luz, porque simplemente con el primero tendría corriente eléctrica también.
- QoS. Se les da prioridad a ciertas aplicaciones para garantizar el ancho de banda.
- Densidad de puerto. Nos referimos al número de puertos del que dispone el switch. Por lo general con un máximo de 48 puertos ethernet, pero algunos switches también tienen un máximo de 4 puertos SPF para fibra óptica.
- Agregación de enlaces. Se pueden agrupar varios puertos en una misma interfaz que gestione el mismo tráfico.
- ACL o listas de control de acceso. Limitan el tráfico no deseado.
- Funciones multicapa. Aunque casi todos los switches son dispositivos que pertenecen al nivel de enlace, hay algunos que pueden desencapsular las tramas a diferentes niveles para el filtrado del tráfico. Son los llamados switches multicapa.

5.1.3. Técnicas de reenvío

Store and fordward (Almacenamiento y reenvío)

Esta técnica consiste en el guardado de la trama completa por parte del switch en memoria RAM para posteriormente reenviarla. Durante su almacenamiento, el switch mide el tamaño de la trama y así calcula su CRC.

Si el tamaño de la trama es muy pequeño, por ejemplo, menos de 64 bytes o muy grande, que sería más de 1518 bytes, las tramas son consideradas corruptas y son descartadas. Si la CRC que se ha calculado anteriormente no coincide con la que se ha recibido, esto también conlleva un descarte de la trama. En caso de no haber ningún problema, se continúa con el envío de la trama de manera normal.

Este método nos ayuda a que no haya tramas inválidas circulando por la red, de manera que el tráfico se acelere. Pero esto conlleva un retardo en el procesamiento de las tramas por tener que analizarlas y comprobarlas una por una. Esto es el llamado tiempo de latencia, pero hoy en día los switches más modernos han conseguido que este retardo sea casi imperceptible.

El CRC es el código de detección de errores de redundancia cíclica.

Cut-through (Cortar y enviar)

Los switches cut-through se diseñaron con la intención de que se reduzca la latencia antes nombrada. Este mecanismo funciona leyendo solo los 6 primeros bytes que se encuentran después del preámbulo, que contienen la MAC de destino y entonces envían la trama por el puerto adecuado.

Estos switches tienen el problema de que no detectan las tramas corruptas que causan las colisiones o lo errores de CRC. Hay una variante llamada **fragment free** que fue diseñada para que este problema no perdurase. Ahora lo que hace el switch es leer siempre los primeros 64 bytes de cada trama para saber que mínimo alcanza este tamaño con la intención de no propagar runts.

Las tramas de menos de 64 bytes son llamadas runts y cuando tienen más de 1518 bytes las llamamos giants.

Adaptative switching (Conmutación adaptativa)

Este tipo de switches son capaces de procesar tramas con las dos técnicas vistas en los anteriores apartados: store and forward y cut-through. Dependiendo del número de tramas erróneas en cada puerto, el switch decidirá que técnica usa, aunque esto también puede ser definido por el administrador del sistema.

Por lo general, llevará el siguiente funcionamiento:

1. Empezará usando la técnica cut-through.
2. Si el número de tramas corruptas supera un cierto nivel preestablecido, pasará a modo store and forward.
3. Cuando descienda de nuevo el número de tramas, entonces pasará de nuevo al primer modo.

5.1.4. Tipos de switches

Los switches se pueden clasificar de dos modos:

Dependiendo del número de puertos que tengan:

- Switch de configuración fija.
- Switches apilables.
- Switches modulares.

Dependiendo de la capa en la que trabajen:

- Switch de capa 2.
- Switch de capa 2 gestionable.
- Switch multicapa.

Switch de configuración fija

Tiene un número de puertos fijo y no hay posibilidad de agregar ninguno más. Puede tener 5, 8, 16, 24 y 48 puertos dependiendo del modelo.

Imagen 13. Switch de 48 puertos

Switches apilables

Se trata de un conjunto de switches que se encuentran interconectados por un puerto de alta velocidad con el fin de que uno sea la propagación del otro y así de manera sucesiva. Esto difiere de cuando conectamos varios switches en una misma red formando una topología, porque en ese caso cada uno actúa de manera autónoma.

Imagen 14. Switches apilables. *Fuente: fs.com*

Switches modulares

Es un chasis metálico con distintos tamaños donde se pueden ir añadiendo distintos módulos que no tienen por qué tener todo el mismo número de puertos.

Imagen 15. Switch modular. *Fuente: industriaembebidahoy.com*

Switch de capa 2

Son los switches más habituales, porque funcionan en la capa dos y no permiten gestión ninguna por parte del administrador de la red. Aunque es más económico que los otros, sus prestaciones suelen ser bajas.

Switch de capa 2 gestionable

Estos switches al igual que el anterior, trabajan en la capa 2, pero en este caso sí permiten configuraciones por parte del administrador de la red. La conexión se hará a través de puerto consola a o vía web y además el switch cuenta con un ligero sistema operativo que permita su configuración.

Sus prestaciones son algo superiores a los no gestionables.

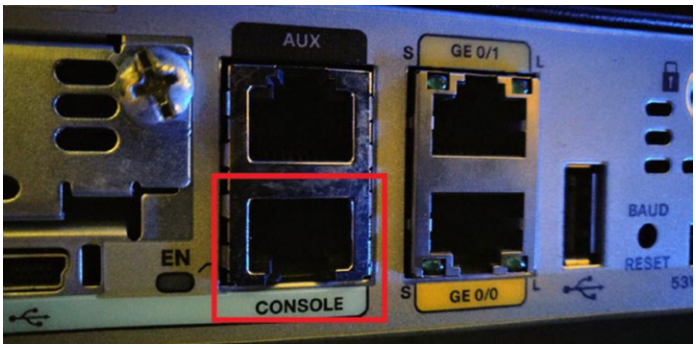

Imagen 16. Puerto consola de un switch. *Fuente: alexariza.net*

Switch multicapa

Estos switches son capaces de realizar funciones de capas superiores a la capa 2, como puede ser el direccionamiento IP, lo que hace que en muchas ocasiones puedan hacer la labor de un router. Además de esto, siempre son gestionables y su gestión de procesos es mucho mayor que la de los routers, por eso son mucho más caros. Existen los llamados content-swicthes que son capaces de filtrar el tráfico de las capas 4 a la 7.

5.1.5. Configuración básica de un switch gestionable

Ahora vamos a ver los comandos más usados en un switch y un ejemplo de cómo se haría una configuración básica de este.

- Para ver la lista de los comandos disponibles usamos el comando `?`.

```
Switch>?
Exec commands:
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
Switch>
```

Imagen 17. Comandos de un switch

- Para ver la información relativa al hardware y software del switch, usamos el comando: `show version`

```
Switch>show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

Switch uptime is 35 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbasek9-mz.150-2.SE4.bin"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 65536K bytes of memory.
Processor board ID FOC1010X104
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0B:BE:A4:7C:00
Motherboard assembly number     : 73-10390-03
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC10093R12
Power supply serial number      : AZS1007032H
Model revision number           : B0
Motherboard revision number     : B0
Model number                    : WS-C2960-24TT-L
System serial number            : FOC1010X104
Top Assembly Part Number        : 800-27221-02
Top Assembly Revision Number    : A0
Version ID                      : V02
CLEI Code Number                : COM3L00BRA
Hardware Board Revision Number  : 0x01

Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE4            C2960-LANBASEK9-M

Configuration register is 0xF
```

Imagen 18. Versión del switch

- Si queremos configurar una fecha:

  `clock set hh:mm:ss día mes(tres primeras letras) año`

- Para comprobar que se ha establecido bien la fecha:

  `show clock`

```
Switch#clock set 07:51:59 11 mar 2022
Switch#show clock
7:52:25.454 UTC Fri Mar 11 2022
Switch#
```

Imagen 19. Reloj del switch

- Para establecer la contraseña del modo privilegiado, en modo configuración:
  - En texto plano: `enable password contraseña`
  - Encriptada: `enable secret contraseña`

```
Switch#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password password
Switch(config)#enable secret universael23
Switch(config)#
```

Imagen 20. Configuración de contraseña del switch

- Para asignar una contraseña a la conexión por consola:
  - Para entrar en la configuración del puerto consola: `line con 0`
  - Para asignar la contraseña: `password contraseña`
- Para loguear y salir:

  `login`

  `exit`

```
Switch(config)#line con 0
Switch(config-line)#password password
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#
```

Imagen 21. Contraseña de puerto consola

- Si queremos asignar una IP a una interfaz VLAN:
  - Para entrar en la configuración de la interfaz: `Interface vlan id`
  - Para asignar la dirección IP: `ip address ip máscara`
  - Para levantar la interfaz y salir:

  `no shutdown`

  `exit`

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 10.0.0.21 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#
```

Imagen 22. IP para una VLAN

- Para establecer una contraseña de acceso por Telnet y posteriormente encriptarla:
  - Para entrar en la configuración telnet:

    `line vty 0 15`
  - Para establecer la contraseña:

    `password contraseña`
  - Para loguear y después salir:

    `login`

    `exit`
  - Para activar la encriptación de la contraseña:

    `service password-encryption`

```
Switch(config)#line vty 0 15
Switch(config-line)#password password
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#service password-encryption
Switch(config)#
```

Imagen 23. Contraseña para Telnet

- Para establecer el gateway por defecto:

  `ip default-gateway ip`

```
Switch(config)#ip default-gateway 10.20.0.1
Switch(config)#
```

Imagen 24. Establecer el gateway

- Para establecer el mensaje diario que muestra el switch al iniciar sesión:

  `banner motd &mensaje&`

```
Switch(config)#banner motd &Bienvenido&
Switch(config)#
```

Imagen 25. Mensaje del día

- Para guardar la configuración actual del switch en NVRAM y así esté preparada cuando volvamos a iniciar:
  - La configuración actual, en el momento, se llama running-config.

» La configuración del inicio y que perdura se llama startup-config.

```
copy running-config startup-config
```

```
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

Imagen 26. Volcado de la configuración

> Para copiar la configuración en un servidor tftp:

```
copy startup-config tftp
```

```
Switch#copy startup-config tftp
Address or name of remote host []? 10.20.0.1
Destination filename [Switch-confg]?

Writing startup-config.......
```

Imagen 27. Volcado a servidor tftp

> Ahora a la inversa:

```
copy tftp startup-config
```

```
Switch#copy tftp startup-config
Address or name of remote host []? 10.20.0.1
Source filename []? startup-config
Destination filename [startup-config]?

Accessing tftp://10.20.0.1/startup-config...
```

Imagen 28. Descarga desde tftp

Hay que tener en cuenta que las dos últimas acciones anteriores funcionarán si tenemos un servidor tftp activo y una VLAN que conecte con él.

> Si queremos ver la configuración actual del switch.

```
show running-config
```

```
Switch#show running-config
Building configuration...

Current configuration : 1403 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$5dvP/kQh8/iKCPbnvv26b/
enable password 7 08314D5D1A0E0A0516
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
 --More--
```

```
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
 --More--
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.0.0.21 255.255.255.0
!
ip default-gateway 10.20.0.1
!
banner motd ^CBienvenido^C
!
!
!
line con 0
 password 7 08314D5D1A0E0A0516
 login
!
line vty 0 4
 password 7 08314D5D1A0E0A0516
 login
line vty 5 15
 password 7 08314D5D1A0E0A0516
 login
!
mac-address-table static 0000.abac.5063 vlan 1 interface FastEthernet0/1
 --More--
```

Imagen 29. Configuración actual de un switch

- Si queremos ver la configuración de inicio (que se podrá ver que es la misma que la actual porque se han copiado: `show startup-config`

```
Switch#show startup-config
Using 1403 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$5dvP/kQh0/iKCPbnvv26b/
enable password 7 08314D5D1A0E0A0516
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
 --More--
```

Imagen 30. Configuración de inicio de un switch

- Si se quiere ver estado de un puerto: `show interface puerto`

```
Switch#show interface Fa0/1
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is Lance, address is 0010.11c9.2d01 (bia 0010.11c9.2d01)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Imagen 31. Mostrar estado de un puerto

- Si queremos reiniciar el switch se usa el comando `reload`.

```
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: 000B.BEA4.7C08
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 2 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4671858
flashfs[0]: Bytes available: 59344526
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"...
############
```

Imagen 32. Reinicio de un switch

5.2. El router

5.2.1. Arquitectura del router

Aunque un router tienen muchos componentes que encontramos en un ordenador, la verdad es que el primero realiza operaciones mucho más específicas y restringidas que el segundo.

Los componentes físicos que se puede destacar de un router son:

- **Puertos de entrada y de salida.** Dependiendo de su uso, los hay de varios tipos, desde para redes LAN hasta para conexiones telefónicas.
- **Memoria.** Tiene diferentes tipos de memoria, volátil y no volátil dependiendo de la información que se vaya a almacenar en él. En el router se almacenan los paquetes mientras que se procesan y también guarda las tablas de enrutamiento para saber guiar a los paquetes hasta su dirección correcta.
- **CPU.** Como pasa en el caso de un equipo, la CPU ejerce de cerebro del router y se encarga de procesar toda la información referida a los paquetes guiándose por las tablas de enrutamiento. Además, también aplica algoritmos de enrutamiento para recalcular la tabla donde se distinguen las distintas rutas.

El componente de software lógico más destacado que tienen un router es:

- **El sistema operativo.** Al igual que en los ordenadores, se trata del software que administra el dispositivo, en este caso para permitir el enrutamiento. Se carga en memoria y a veces tienen una interfaz web que permite su administración remota.

Para poder establecer el rendimiento de un router tendremos que fijarnos en la capacidad de proceso que este tiene, el almacenamiento que posee y el ancho de banda de cada uno de sus buses.

5.2.2. Nivel de operación

Los routers trabajan en el nivel 3 del modelo OSI y se encarga de interconectar varias LAN o enlaces WAN. Que funcione en el nivel 3 hace que sea algo más lento en rendimiento que otros dispositivos que operan en niveles inferiores porque tiene que analizar los paquetes de red, primeramente. De igual modo, los routers son muy usado porque permiten flexibilizar en gran medida las redes.

5.2.3. Funcionamiento

Si queremos resumir, cuando un paquete llega a un router, este sigue el siguiente procedimiento:

1. Lo recibe en su puerto de entrada.
2. Separa cabecera IP y contenido, pero se guarda el contenido para luego reensamblarlo antes del envío.
3. En la cabecera IP, separa la dirección de destino del paquete, se fija en la tabla de enrutamiento y entonces realiza el siguiente subproceso:
   a. Si la red a la que debe de ir el paquete se encuentra directamente conectada, vuelve a formarlo y el paquete sale por la interfaz que conecta con esa red.
   b. Si la red a la que debe de ir el paquete no está directamente conectada, entonces comprobará si es accesible pasando por otro router, si es así, se vuelve a formar el paquete y se envía por la interfaz que conecte con el otro router.
   c. Si la red no es accesible de ningún modo, el paquete se elimina y al usuario le llega un mensaje de error tipo ICMP.

5.2.4. Tipos de router según su función

Router LAN/WAN o SOHO (Small Office /Home office)

Estos routers ejercen como una frontera entre la red interna de una organización o un domicilio con Internet.

Suelen tener unos cuantos puertos LAN, generalmente 4, un punto de acceso inalámbrico y un puerto WAN para la conexión a Internet.

Las principales funciones de reste router son:

- Enrutamiento entre LAN y WAN, un enrutamiento muy simple entre solo una LAN y solo una WAN.
- Switch entre los puertos Ethernet que tenga y la red inalámbrica.
- Punto de acceso Wifi o AP.
- Modulación. Por la interfaz WAN saldrán señales analógicas, pero por la LAN las señales que salen son digitales.
- Como tiene varias interfaces privadas y una sola pública, realiza NAT.
- Sirve para varios servicios en red como DHCP, DNS, etc.

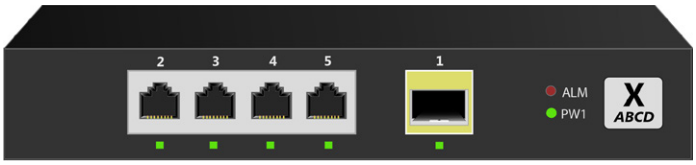

Imagen 33. Router SOHO

Router WAN

Estos pueden ser para fines privados o públicos, Los privados suelen usarse en los DMZ de ciertas organizaciones mientras que los públicos se suelen usar para la interconexión de grandes zonas geográficas y se puede acceder a ellos desde cualquier punto de la red. Estos routers tienen unas prestaciones muy altas y eso hace que su precio también sea bastante alto.

Otros dispositivos que pueden funcionar como router

Los dos tipos anteriores, son dispositivos cuya función final es el enrutamiento, pero hay dispositivos como puede ser un equipo con varias tarjetas de red, que también podrían ejercer de router si su sistema operativo se lo permite. Esto se da a veces en LAN pequeñas.

5.3. Configuración de routers CISCO

Como la mayoría de los dispositivos de erutación son CISCO y tienen una implantación tan extendida, la configuración de uno de estos en su sistema operativo IOS se puede tomar como estándar para la configuración de cualquier otro componente de la red. Esto ya lo vimos en el caso de los *switches*.

5.3.1. Modos de operación

Cuando nos conectemos a un router CISCO, tenemos distintos modos de trabajo y vamos a ver cómo funcionan:

Modos de operación				
Modo	**Acceso**	**Prompt**	**Salida**	**Uso**
Usuario *EXEC*	Conexión		`logout` `exit`	**Cambiar configuraciones del terminal y comprobar el estado del** *router*.
Privilegiado *EXEC*	`enable`		`disable` `exit`	**Mostrar la información y realizar trazas.** **Recargar la configuración y manejar los archivos del** *router*.
Configuración **global**	`configure terminal`		`end` `exit`	**Configuración general del** *router*
Configuración **de interfaz**	`Interface`	`Router (config-if)#`	`end` `exit`	**Configuración de una interfaz del** *router*.
Configuración **de Subinterfaz**	Definición de la sub-interfaz	`Router (config-subif)#`	`end` `exit`	**Configuración de una subinterfaz de una interfaz del** *router*.
Configuración **de Línea**	`line vty` `line console`		`end` `exit`	Configuración de líneas individuales de terminal.
Monitor de ROM	`reload`	`rommon#>`	`continue`	Procesos especiales e imágenes

Los comandos que en el modo EXEC se han ejecutado, no se grabarán en el router para que se carguen cuando ser reinicie. En cambio, los comandos que se han ejecutado en el modo Configuración se pueden volcar en la configuración de inicio igual que hicimos con los switches para que perduren incluso si se reinicia el router.

El modo que vimos en el cuadro de Configuración Global es el más elevado de todos y el que nos permite que podamos acceder a otros modos de configuración.

Lógicamente, como este es un modelo algo exclusivo de router, no todos van a contar con las mismas funcionalidades, cuanto más sofisticado, más tendrá.

En cualquiera de los modos que tenemos en el router, estos comandos son comunes:

- `?` → nos muestra la ayuda.
- Tabulando se completan los comandos.
- Si usamos las teclas de dirección hacia arriba y hacia abajo, se recuperan comandos anteriores.
- Si hay un comando que con sus primeras letras ya se distingue cual es, usando solo esas letras se puede ejecutar. Por ejemplo: `configure terminal` → `conf term`.

5.3.2. Modo Usuario EXEC

Este es el modo más sencillo, y al que se accede nada más conectarnos al router.

Los comandos más usados son:

Modo de usuario EXEC		
Comando	**Alias**	**Uso**
`enable`	`en`	Pasa al modo privilegiado
`end | logout`	`lo`	Sale del modo.
`connect`	`co`	Abre una conexión por terminal.
`disconnect`	`disc`	Cierra una conexión de red
`ping nombre_host | ip dirección_IP`		Hace ping a alguna dirección IP o nombre de host.
`show interfaces`	`sh in`	Muestra información detallada de las interfaces del router.
`show ip route`	`sh ip ro`	Muestra la tabla de rutas IP.
`show arp`	`sh arp`	Muestra la tabla de traducciones ARP.
`show ip protocols`	`sh ip pr`	Muestra los parámetros y estadísticas del proceso de protocolos de enrutamiento IP.
`ssh [-l] [-v] nombre_host | ip dirección_IP`		Establece una conexión SSH con un host remoto por su nombre o su dirección IP.
`telnet [ nombre_host | ip dirección_IP ]`		Establece una conexión Telnet a una dirección remota.
`traceroute [ nombre_host | ip dirección_IP]`	`tr`	Traza una ruta a una dirección IP o nombre de host.

Tanto en este modo como en el privilegiado, si introducimos una instrucción que es desconocida para el router, lanzará consultas DNS porque lo interpreta como un nombre de host y la consola se quedará durante un tiempo procesándola.

```
Router>prueba
Translating "prueba"...domain server (255.255.255.255)
```

Imagen 34. Resolución por nombre DNS

Si usamos el siguiente comando, esto se desactiva:

```
no ip domain-lookup
```

5.3.3. Modo Privilegiado EXEC

Aquí se incluyen todos los comandos del modo de usuario más los que vamos a mostrar a continuación. Por esta razón muchas veces directamente se accede a este modo sin hacer nada en el de usuario.

Los comandos más usados son:

Modo Privilegiado EXEC		
Comando	**Alias**	**Uso**
`disable`	sisa	Sale del modo Privilegiado.
`reload`	sel	Reinicia el router.
`configure terminal`	conf t	Entra al modo de Configuración Global.
`show running-config`	sh ru	Muestra la configuración actual ene ejecución.
`show startup-config`	lo	Muestra la configuración en el arranque.
`show line`	sh li	Muestra información de las líneas TTY.
`show file system`	sh fi sy	Muestra la información del sistema de ficheros sobre el que opera el router
`show version`	sh ve	Muestra la versión del sistema operativo e información relativa al hardware del router
`copy`		Copia un archivo.
`delete`		Borrar un archivo.
`dir`		Se muestran los archivos de una ubicación concreta del router.
`erase startup-config`	er st	Borra el contenido de la configuración de inicio.
`dkdir`	mk	Crear un directorio
`dmdir`	rm	Borra un directorio.
`write [ memory | network | terminal }`		Se vuelca la configuración actual en ejecución en memoria, red o terminal.
`do write`	do wr	Se guarda la configuración actual.
`debug protocolo`	deb	Se activa el rastreo de diferentes protocolos.
`undebug protocolo`	und	Se desactiva el rastreo de los protocolos.

5.3.4. Modo Configuración Global

Los comandos que más se usan en este modo son:

Modo de configuración global		
Comando	**Alias**	**Uso**
`hostname nombre`	h	Establece un nombre para el router.
`enable [ password | secret contraseña ]`	ena	Se establece la contraseña en texto plano o cifrada.
`interface`	in	Selecciona una interfaz y se accede a su modo de Configuración.
`aaa [ authentication | authorization | new_model ]`		Se fijan parámetros para la autenticación, autorización y cuentas.
`banner [login | motd] texto`	ba	Se fija un mensaje de bienvenida o mensaje para el día.
`username [ password contraseña | privilege nivel | secret contraseña ]`	us	Se especifican las características de autenticación de un usuario en concreto.
`boot system`	bo sys	Se modificación los archivos de imagen del sistema para modificar el arranque.
`acces-list número`	acc	Se crea una lista de acceso.
`[ no ] ip domain-lookup`		Se activa o desactiva la resolución de nombres DNS en el router.
`line vty nº_min_conexiones nº_max_conexiones`	li	Se configura el acceso Telnet.
`line con 0`	li	Se configura el acceso por consola.
`router protocolo`		Se configura un protocolo de enrutamiento en específico.

5.3.5. Modo Configuración de una interfaz del router

Cuando configuremos una interfaz debemos de tener en cuenta que ciertos comandos o parámetros van a depender de la interfaz en específico, por lo que ahora solo vamos a mostrar algunos de los comandos y puede que no sirvan en otras interfaces puntualmente.

Los comandos más usados son:

Modo de configuración de una interfaz		
Comando	**Alias**	**Uso**
`shutdown`	sh	Se desactiva la interfaz.
`no shutdown`	no sh	Se arranca la interfaz
`ip address dhcp`	ip add	Se configura la interfaz para que la IP sea dinámica y asignada por DHCP
`ip address dirección_IP máscara [ secondary ]`	ip add	Se establece una dirección IP estática de manera manual para la interfaz.
`mac-address dirección_MAC`	mac	Se fija la dirección MAC para la interfaz.
`bandwith ancho_banda`	b	Se fija el ancho de banda que irá en kilobits.
`delay`	del	Nos permite que se fije un valor, en decenas de milisegundos para el delay. Los valores deben de estar comprendidos entre 1 y 16 777 215.
`clock rate frecuencia`	cl ra	Se fija la frecuencia de reloj de la interfaz en bits/segundo. Debe de estar entre 300 4 000 000.
`duplex [ auto | full | half ]`	du	Se establece si usa auto, full o half dúplex.
`mtu tamaño`		Se fija la unidad máxima de transmisión que debe estaré entre 64 y 17 940.
`speed [ 10 | 100 | auto ]`	sp	Se configura la velocidad de la interfaz.

5.3.6. Modo Configuración de una línea

Este modo nos permite que se hagan configuraciones para conexiones telnet, consola, etc.

Algunos de los comandos más usados, son:

Modo de configuración de una línea		
Comando	**Alias**	**Uso**
`password contraseña`	pas	Se establece una contraseña para la línea.
`login`	log	Establecemos la conexión.
`exit`	ex	Se cierra la conexión.
`enable secret password`	en se	Se establece una contraseña cifrada o secreto. Para Telnet es obligatorio.

5.3.7. Configuración de una conexión SSH

Para configurar la conexión SSH al router, tenemos que hacerlo en la configuración global y en la configuración de línea general.

Para configurar la conexión debemos de ejecutar mínimo los siguientes comandos:

Configuración para una conexión SSH		
Comando	**Modo**	**Uso**
`ip domain-name nombre`	Configuración global	Se establece el nombre de dominio del router.
`crypto key generate rsa`	Configuración global	Se establece el tipo de encriptación para las claves.
`line vty nº_min_conexiones nº_max_conexiones`	Configuración global.	Se entra en el modo de configuración de SSH.
`transport input ssh`	Configuración de línea	Permitimos la conexión y el protocolo SSH.
`login local`	Configuración de línea.	Logueamos de manera local.
`username usuario privilege 15 password contraseña`	Configuración global.	Se establecen los permisos y acreditación para el usuario conectado.
`enable secret password`	Configuración global.	Se establece la contraseña cifrada del usuario conectado.

5.3.8. Configuración del servicio DHCP

Los router CISCO también se pueden configurar como un servidor DHCP.

Hay que ejecutar los siguientes comandos para configurar el router como servidor de DHCP:

1. Entramos en el modo privilegiado del router.
2. Se entra en el modo de Configuración Global.
3. Para crear o eliminar un pool de DHCP, usamos el siguiente comando:

   `ip dhcp pool nombre`

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool prueba
Router(dhcp-config)#
```

Imagen 35. Pool dhcp

4. Para definir la red y la máscara de red de las direcciones IP que se van a asignar: `network dirección_red máscara`

```
Router(dhcp-config)#network 10.20.0.0 255.0.0.0
Router(dhcp-config)#
```

Imagen 36. Red de DHCP

5. Establecemos la que va a ser la puerta de enlace que van a tener los equipos que reciban IP: `default-server dirección_IP`

```
Router(dhcp-config)#default-router 10.20.0.1
Router(dhcp-config)#
```

Imagen 37. Gateway de los clientes IP

6. Para establecer el que será el servidor DNS para los clientes que obtienen las direcciones: `dns-server dirección_servidor`

```
Router(dhcp-config)#dns-server 10.20.0.2
Router(dhcp-config)#
```

Imagen 38. DNS de los clientes IP

7. Salimos del modo de configuración propio de DHCP.

8. Se dictaminan las direcciones IP que quedan excluidas de ser asignadas, con el comando:

   `ip dhcp excluded-address dirección_IP_inferior dirección_IP_superior`

```
Router(dhcp-config)#
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 10.20.0.3 10.20.0.10
Router(config)#
```

Imagen 39. Exclusión de direcciones IP

9. Salimos del modo de Configuración Global.

10. Si queremos ver las concesiones de IP que el router ha recibido de otro servidor DCHP (en la imagen no se muestra nada, porque no las hay):

    `show dhcp lease`

```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show dhcp lease
Router#
```

Imagen 40. show dhcp lease

11. Para mostrar las vinculaciones de IPs estáticas que se han hecho con clientes del servicio DHCP (si no se muestran en la imagen es porque no hay todavía):

    `show ip dhcp binding`

```
Router#
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
Router#
```

Imagen 41. show ip dhcp binding

12. Para mostrar las direcciones IP que hay en conflicto (de momento no tenemos ninguna): `show ip dhcp conflicto`

```
Router#
Router#show ip dhcp conflict
IP address       Detection method   Detection time          VRF
Router#
```

Imagen 42. show ip dhcp conflict

5.4. Router linksys

Para los routers de casa SOHO, CISCO ofrece unos routers tipo LAN/WAN que cuenta con una interfaz WAN RJ-11, cuatro interfaces LAN Ethernet RJ-15 y un punto de acceso inalámbrico. Estos son los llamados Routers Linksys.

Estos routers como la mayoría de los SOHO, realmente no realizan un enrutamiento, sino una traducción de direcciones de red privadas a la IP pública para acceso a internet, lo que se llama NAT, Network Addreess Translation.

Para configurar estos routers se accede vía web al servidor HTTP para la administración del servidor. Los principales parámetros de configuración que se pueden establecer en este router son:

Configuración de Internet

- Nombre del host, dominio y MTU.
- Asignación de la dirección IP pública del router:
  - Estática.
  - Dinámica: dirección IP, máscara, puerta de enlace y servidor DNS.
  - PPPoE: nombre y contraseña de usuario y nombre del servicio.

Configuración inalámbrica

- Básica: nombre de la red (SSID), canal, distribución del SSID (activo e inactivo), etc.
- Seguridad inalámbrica: Modo de seguridad (Ninguna, WEP, WPA-P. WPA-E. WPA2-P, WPA2-E), Contraseña, etc.

Configuración de Administración

- Contraseña de acceso al router.
- Habilitar o denegar el acceso remoto al router.
- Actualización del firmware.

Configuración LAN-WAN

- Mapeo de puertos y equipos.
- DMZ.
- Quality of Service.

Imagen 43. Router Linksys.
Fuente: wikimedia.org

www.universae.com