Manual de usuario del iRouter v1.0.3

Teldat S.A.

19 de enero de 2011

Índice general

1. Protocolo Telnet **2**
1.1. Acceso a Telnet . . . 2
1.2. Ayuda . . . 3
1.3. Show Config . . . 3
1.4. Exit . . . 3
1.5. Logout . . . 4

2. LAN **5**
2.1. Configuración de LAN . . . 5
2.2. Configuración de Dispositivo LAN . . . 5
2.2.1. Habilitar cliente DHCP . . . 5
2.2.2. Direcciones IP . . . 5
2.2.3. Habilitar UPnP . . . 6
2.2.4. Habilitar IGMP snooping . . . 6
2.2.5. Dirección IP secundaria . . . 6
2.2.6. Direcciones MAC permitidas . . . 6
2.3. Configuración de Servidor DHCP . . . 6
2.3.1. Nombre de dominio . . . 7
2.3.2. Pool del servidor DHCP . . . 7
2.3.3. Tiempo de expiración . . . 7
2.3.4. Habilitar . . . 7
2.3.5. Servidores DNS . . . 7
2.3.6. Puertas de enlace . . . 7
2.3.7. Opciones . . . 8
2.3.8. Pool de direcciones condicional . . . 8

3. WAN **9**
3.1. Configuración de WAN . . . 9
3.2. Configuración de Dispositivo WAN . . . 9
3.2.1. Conexiones . . . 9
3.3. Configuración de Conexión IP . . . 10
3.3.1. Nombre . . . 10
3.3.2. Descripción . . . 10
3.3.3. Número/prioridad VLAN . . . 10
3.3.4. Tipo de NAT . . . 10
3.3.5. Protocolo de routing entrante . . . 11
3.3.6. Habilitar cliente DHCP . . . 11
3.3.7. IP . . . 11
3.3.8. Utilizar DNSs externos . . . 11
3.3.9. Dirección DMZ . . . 11
3.3.10. Reiniciar conexión . . . 12
3.3.11. Habilitar conexión . . . 12

3.3.12. Opciones del cliente DHCP . . . 12
3.3.13. Servidores DNS . . . 12
3.3.14. Tabla de mapeo de puertos . . . 13
3.4. Configuración de Conexión PPPoE . . . 13
3.4.1. Nombre . . . 13
3.4.2. Descripción . . . 14
3.4.3. Número/prioridad VLAN . . . 14
3.4.4. Tipo de NAT . . . 14
3.4.5. Protocolo de routing entrante . . . 14
3.4.6. Inicio conexión . . . 15
3.4.7. Usuario . . . 15
3.4.8. Contraseña . . . 15
3.4.9. Nombre de AC . . . 15
3.4.10. Nombre del servicio . . . 15
3.4.11. Utilizar DNSs externos . . . 15
3.4.12. Dirección DMZ . . . 15
3.4.13. Reiniciar conexión . . . 15
3.4.14. Habilitar conexión . . . 16
3.4.15. Servidores DNS . . . 16
3.4.16. Tabla de mapeo de puertos . . . 16
3.5. Configuración de Proxy IGMP . . . 17
3.5.1. Conexión de subida . . . 17
3.5.2. Habilitar proxy IGMP . . . 17

4. Ethernet **18**
4.1. Configuración de Ethernet . . . 18
4.2. Configuración de Interfaz Ethernet LAN . . . 18
4.2.1. Apagar . . . 18
4.2.2. Modo . . . 18
4.2.3. Control de MAC . . . 18
4.2.4. Tasa de bit máxima . . . 19
4.3. Configuración de Interfaz WAN Ethernet . . . 19
4.3.1. Modo . . . 19
4.3.2. Tasa de bit máxima . . . 19

5. Wi-Fi **20**
5.1. Configuración de Wi-Fi . . . 20
5.2. Configuración de Interfaz inalámbrico . . . 20
5.2.1. Deshabilitar radio . . . 20
5.2.2. SSID . . . 20
5.2.3. Ocultar SSID . . . 20
5.2.4. Estándar . . . 21
5.2.5. Canal . . . 21
5.2.6. Ancho de canal . . . 21
5.2.7. Potencia de transmisión . . . 21
5.2.8. Modo de operación . . . 22
5.2.9. Intervalo de guarda . . . 22
5.2.10. Protección 802.11b/g . . . 22
5.2.11. Habilitar transmisión de AMSDU . . . 22
5.2.12. Filtrado de MAC . . . 22
5.2.13. Habilitar punto de acceso . . . 23
5.3. Configuración de Seguridad inalámbrica . . . 23
5.3.1. Modo de seguridad . . . 23
5.3.2. Clave pre-compartida . . . 23

5.4. Configuración de Seguridad básica . . . 23
5.4.1. Autenticación . . . 23
5.4.2. Primera clave WEP . . . 24
5.4.3. Segunda clave WEP . . . 24
5.4.4. Tecera clave WEP . . . 24
5.4.5. Cuarta clave WEP . . . 24
5.4.6. Clave WEP por defecto . . . 24
5.5. Configuración de Seguridad para el acceso protegido Wi-Fi . . . 25
5.5.1. Autenticación . . . 25
5.6. Configuración de Seguridad para el acceso protegido Wi-Fi 2 . . . 25
5.6.1. Autenticación . . . 25
5.7. Configuración de Wi-Fi Protected Setup . . . 26
5.7.1. Habilitar WPS . . . 26
5.7.2. Código PIN WPS . . . 26
5.8. Configuración de Wi-Fi Multimedia . . . 26
5.8.1. Habilitar APSD . . . 26
5.8.2. Habilitar WMM . . . 26
5.9. Configuración de Punto de acceso virtual . . . 27
5.9.1. Añadir AP virtual . . . 27
5.10. Configuración de Punto de acceso virtual . . . 27
5.10.1. SSID . . . 27
5.10.2. Ocultar SSID . . . 27
5.10.3. Control de MAC . . . 27
5.10.4. Habilitar punto de acceso . . . 27

6. Forwarding **28**
6.1. Configuración de Forwarding . . . 28
6.1.1. Conexión por defecto . . . 28
6.1.2. Rutas via gateway . . . 28
6.1.3. Rutas via interfaz . . . 29

7. Firewall **30**
7.1. Configuración de Firewall . . . 30
7.1.1. Firewall . . . 30
7.2. Configuración de Información de firewall . . . 31
7.2.1. Nombre . . . 31
7.2.2. Configuración . . . 31
7.2.3. Acción por defecto . . . 31
7.2.4. Reglas . . . 31
7.3. Configuración de Regla . . . 32
7.3.1. Regla de configuración . . . 32
7.3.2. Tipo de ICMP . . . 33
7.3.3. IP origen . . . 35
7.3.4. Puerto origen . . . 35
7.3.5. IP destino . . . 36
7.3.6. Puerto destino . . . 36
7.3.7. Habilitar . . . 36

8. Gestión **37**
8.1. Configuración de Gestión . . . 37
8.1.1. Contraseña . . . 37
8.2. Configuración de Parámetros del TR069 . . . 37
8.2.1. URL . . . 37
8.2.2. Nombre de usuario . . . 37

8.2.3. Contraseña . . . 37
8.2.4. Nombre del usuario para la conexión . . . 37
8.2.5. Contraseña de conexión . . . 38
8.2.6. Actualizaciones gestionadas . . . 38
8.3. Configuración de Información periódica . . . 38
8.3.1. Intervalo de información periódica . . . 38
8.3.2. Referencia de hora . . . 38
8.3.3. Habilitar . . . 38
8.4. Configuración de STUN . . . 38
8.4.1. Dirección del servidor STUN . . . 38
8.4.2. Puerto del servidor STUN . . . 38
8.4.3. Periodo mínimo del keepalive para el STUN binding . . . 39
8.4.4. Periodo máximo del keepalive para el STUN binding . . . 39
8.4.5. Habilitar . . . 39

9. Hora **40**
9.1. Configuración de Hora . . . 40
9.1.1. Zona de hora local . . . 40
9.1.2. Primer servidor NTP . . . 40
9.1.3. Segundo servidor NTP . . . 40
9.1.4. Habilitar . . . 40

10. Almacenamiento **41**
10.1. Configuración de Almacenamiento . . . 41
10.1.1. Grupo de trabajo . . . 41
10.1.2. Habilitar servicio CIFS . . . 41
10.1.3. Actualizar el contenido del USB . . . 41
10.1.4. Desmontar todos los dispositivos de almacenamiento . . . 41
10.1.5. Carpetas compartidas . . . 41
10.1.6. Usuarios de almacenamiento . . . 42

11. Impresión **43**
11.1. Configuración de Impresión . . . 43
11.1.1. Habilitar servidor de impresora . . . 43

12. Servidor DNS **44**
12.1. Configuración de Servidor DNS . . . 44
12.1.1. Habilitar servidor DNS . . . 44
12.1.2. Hosts DNS . . . 44

13. QoS **45**
13.1. Configuración de QoS . . . 45
13.1.1. Cola por defecto . . . 45
13.1.2. Cola multicast por defecto . . . 45
13.1.3. Habilitar . . . 45
13.2. Configuración de Colas . . . 45
13.2.1. Colas . . . 46
13.3. Configuración de Cola . . . 47
13.3.1. Nombre . . . 47
13.3.2. Interfaz . . . 47
13.3.3. Prioridad . . . 47
13.3.4. Algoritmo del planificador . . . 47
13.3.5. Peso . . . 47
13.3.6. Shaping rate . . . 47

13.3.7. Etiquetado del tamaño de la ráfaga 48
13.3.8. Habilitar 48
13.4. Configuración de Clasificaciones 48
13.4.1. Clasificaciones 48
13.5. Configuración de Clasificación 48
13.5.1. Orden 48
13.5.2. Interfaz 49
13.5.3. Cola 49
13.5.4. IP destino 49
13.5.5. Excluir IP destino 49
13.5.6. IP origen 49
13.5.7. Excluir IP origen 50
13.5.8. Protocolo 50
13.5.9. Excluir protocolo 50
13.5.10. Puerto destino 50
13.5.11. Excluir puerto destino 50
13.5.12. Puerto origen 50
13.5.13. Excluir puerto origen 51
13.5.14. MAC origen 51
13.5.15. Excluir MAC origen 51
13.5.16. MAC destino 51
13.5.17. Excluir MAC destino 51
13.5.18. DSCP 51
13.5.19. Excluir DSCP 52
13.5.20. Marcado DSCP 52
13.5.21. Habilitar 52

14. DynDNS **53**
14.1. Configuración de DynDNS 53
14.1.1. Nombre de usuario 53
14.1.2. Contraseña 53
14.1.3. Host 53
14.1.4. Habilitar DynDNS 53

Capítulo 1

Protocolo Telnet

El propósito del protocolo Telnet es proporcionar un sistema de comunicaciones general, bidireccional y cuya unidad mínima de transmisión sea el byte. De esta forma, se puede considerar un método estándar de interconectar dispositivos terminales y procesos orientados a terminal entre sí. TELNET es uno de los primeros intentos de desarrollar un protocolo de terminal virtual (VTP), y fue desarrollado como una parte del conjunto de protocolos TCP/IP. TELNET está construido sobre tres principios básicos:

- El concepto de terminal virtual de red (NVT).
- Una vista simétrica de terminales y procesos.
- El principio de opciones negociadas.

El NVT es un dispositivo imaginario que proporciona una representación intermedia de un terminal canónico. Si la entidad de comunicación es un proceso, se necesita un módulo (servidor TELNET) para realizar la conversión entre la representación NVT y la representación del proceso. Si la entidad de comunicación es un terminal, se necesita un módulo (cliente TELNET) para convertir las características del terminal a las del NVT. Se espera que la comunicación se realice sobre una conexión TCP. TELNET asume que se utilizará el código ASCII para la comunicación. Toda conexión TELNET comienza con una fase de negociación de opciones con las que se indican las características de la conexión. Después de dicha negociación se realiza la transmisión de datos, pudiendo incluir en la misma comandos mediante la utilización de caracteres de escape. Los equipos de Teldat incorporan un servidor Telnet (cuya configuración y monitorización se describen en este manual) que permite acceder a la consola de los mismos, con lo que se puede realizar la configuración o monitorización remotamente, del mismo modo que se haría en la consola de modo local.

1.1. Acceso a Telnet

Para acceder al entorno de configuración propio del protocolo TELNET, se deben introducir los siguientes comandos:

```
telnet <IProuter>
```

A continuación se deberá introducir el User y el Password. Por defecto, ambos parámetros tienen el valor 1234. Ejemplo de acceso a Telnet:

```
$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
User: 1234
```

```
Password:
iRouter1214-W2D CLI 1.0.3
TELDAT S.A. 2010
1234@irouter$
```

1.2. Ayuda

Una vez que se ha accedido al terminal remoto mediante telnet, se pueden visualizar los diferentes comandos posibles introducindo el símbolo ?. Cuando se teclea ? se muestran todos los comandos disponibles. También se puede utilizar el símbolo ? para visualizar las distintas opciones de cada comando. El tabulador permite autocompletar cuando se está introduciendo el nombre de un comando. Cuando se utiliza el símbolo ?, pueden aparecen tres opciones posibles:

Comando	Comando disponible
<valor>	Valor del parámetro
<cr>	Solo se admite retorno de carro

Ejemplo de todos los comandos disponibles:

```
1234@irouter$ ?
```

delete-config	Delete all configuration
lan	LAN configuration
wan	WAN configuration
ethernet	Ethernet configuration
wireless	Wireless configuration
forwarding	Routes configuration
firewalls	Firewall configuration
management	Management configuration
time	Time configuration
storage	Storage configuration
printing	Printing configuration
dns-server	DNS Server configuration
qos	Quality of Service configuration
dyndns	Dyndns configuration
factory-reset	Reset to factory settings and reboot
reboot	Reboot the gateway
no	No command
show	Show configuration
exit	Exit from the current menu
logout	Closes the console

1.3. Show Config

Se muestra la configuración actual del router.

```
1234@irouter$ show config
```

1.4. Exit

Se utiliza este comando para volver al prompt anterior. En el siguiente ejemplo se accede al menú wan. Si se desea volver al prompt anterior, se debe introducir el comando exit.

```
1234@irouter$ wan
1234@irouter>wan$ exit
1234@irouter$
```

1.5. Logout

Permite la desconexión del terminal remoto.

```
1234@irouter$ logout
```

Capítulo 2

LAN

2.1. Configuración de LAN

```
1234@irouter>$ lan
```

Contiene todas las opciones de configuración aplicables a la red de área local. Una red de área local, red local o LAN (del inglés local area network) es la interconexión de varias computadoras y periféricos.

2.2. Configuración de Dispositivo LAN

```
1234@irouter>lan$ device <value>
```

Contiene las diferentes opciones que condicionan el funcionamiento del dispositivo LAN actual.

2.2.1. Habilitar cliente DHCP

```
1234@irouter>lan>Home$ ip dhcp
```

Activando esta opción se habilitará el cliente DHCP, de esta forma, se configuraran todos los parámetros proporcionados por el servidor DHCP de la interfaz ubicada en la LAN.

2.2.2. Direcciones IP

```
1234@irouter>lan>Home$ ip address <value> mask <value>
```

Dirección IP

Dirección IP de la interfaz de la pasarela ubicada en la LAN. Podemos definir formalmente una dirección IP como una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol).

Máscara de subred

Máscara de red que se aplicará la dirección IP ubicada en la LAN. La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

2.2.3. Habilitar UPnP

```
1234@irouter>lan>Home$ upnp
```

Permite el descubrimiento y publicación de dispositivos por UpnP (Universal Plug and Play). UPnP define protocolos y procedimientos comunes para garantizar la interoperatividad sobre PC permitidos por red, aplicaciones y dispositivos inalámbricos.

2.2.4. Habilitar IGMP snooping

```
1234@irouter>lan>Home$ igmp-snoop
```

Permite escuchar el tráfico IGMP de la LAN. Escuchando este tráfico, el router guarda un mapa con todos los enlaces utilizados por los flujos multicast.

2.2.5. Dirección IP secundaria

```
1234@irouter>lan>Home$ ip secondary address <value> mask <value>
```

Permite asignar varias direcciones IP a una misma la LAN. Esto resulta especialmente útil cuando deseemos tener a la pasarela en más de una LAN simultáneamente.

Dirección IP

Dirección IP secundaria con la que también se conocerá la LAN.

Máscara de subred

Máscara de red aplicada a la dirección IP.

2.2.6. Direcciones MAC permitidas

```
1234@irouter>lan>Home$ allowed-macs <value>
```

Listado con las direcciones físicas permitidas en la LAN. Los clientes no permitidos explícitamente no tendrán acceso al área local.

Dirección MAC

Listado de las direcciones MACs permitidas. La dirección MAC permite diferenciar de forma única a los interfaces de los dispositivos conectados a la LAN. Una interfaz de un dispositivo con una MAC diferente a las listadas no tendrá acceso al área local.

2.3. Configuración de Servidor DHCP

```
1234@irouter>lan>Home$ dhcp-server
```

En esta opción se listan los diferentes parámetros de configuración del servidor DHCP que actuará en la LAN. DHCP (del inglés Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido, a quien se la ha asignado después.

2.3.1. Nombre de dominio

```
1234@irouter>lan>Home>dhcp-server$ domain-name <value>
```

Nombre de dominio del servidor DHCP. Un nombre de dominio identificad de forma única un recurso IP (Internet Protocol).

2.3.2. Pool del servidor DHCP

```
1234@irouter>lan>Home>dhcp-server$ pool minaddress <value> maxaddress <value>
     mask <value>
```

Dirección IP mínima

Cota inferior del rango de direcciones de red que se proporcionarán a los clientes DHCP de este pool.

Dirección IP máxima

Cota superior del rango de direcciones de red que se proporcionarán a los clientes DHCP de este pool.

Máscara de subred

Máscara de red que se aplicará al rango de direcciones de red acotado por el valor mínimo y máximo especificados anteriormente.

2.3.3. Tiempo de expiración

```
1234@irouter>lan>Home>dhcp-server$ leaseTime <value>
```

Tiempo máximo de expiración de las direcciones de red asignadas por el servidor DHCP. Acabado este tiempo, el cliente deberá solicitar la renovación o la asignación de una nueva dirección de red.

2.3.4. Habilitar

```
1234@irouter>lan>Home>dhcp-server$ enable
```

La pasarela actuará como servidor DHCP dentro del área local

2.3.5. Servidores DNS

```
1234@irouter>lan>Home>dhcp-server$ dns-server <value>
```

Listado de servidores DNS que proporcionará la pasarela a los clientes que lo soliciten.

Servidor DNS

Listado de servidores DNS que se proporcionarán a los clientes que lo soliciten. Un servidor DNS (Domain Name System) es el encargado de responder las peticiones de resolución de nombres realizadas por los clientes.

2.3.6. Puertas de enlace

```
1234@irouter>lan>Home>dhcp-server$ gateway <value>
```

Listado con las diferentes puertas de enlace que se proporcionarán a los clientes que lo soliciten.

Puerta de enlace

Listado de direcciones ip a las que se redirigirá el tráfico saliente de la red. Si se asigna la dirección de red de la interfaz de la pasarela ubicada en la LAN, la propia pasarela se encargará de redirigir el tráfico.

2.3.7. Opciones

```
1234@irouter>lan>Home>dhcp-server$ option code <value> value <value>
```

Listado de opciones disponibles. Una opción es un par opción-valor siendo el campo opción único para cada entrada. De esta forma, si un cliente DHCP solicita un determinado código, se le devuelve su valor asociado.

Código

Código de la opción utilizado para diferenciarla del resto.

Valor

Valor asociado al código que se servirá al cliente que lo solicite.

2.3.8. Pool de direcciones condicional

```
1234@irouter>lan>Home>dhcp-server$ add cond-pool order <value> name <value>
```

Permite añadir un nuevo pool condicional sobre el cual realizar una serie de acciones personalizadas en función de su vendor info.

Orden

Orden de evaluación de los pools. Dos pools no pueden tener el mismo valor y su evaluación es en orden ascendente.

Nombre

Nombre del pool condicional utilizado para diferenciarlo con respecto al resto. El nombre debe ser único.

Capítulo 3

WAN

3.1. Configuración de WAN

```
1234@irouter>$ wan
```

Permite añadir, modificar o eliminar conexiones WAN. Estas conexiones pueden basarse en el protocolo IP (Internet Protocol) o bien en el protocolo PPPoE (Point-to-Point Protocol over Ethernet).

3.2. Configuración de Dispositivo WAN

```
1234@irouter>wan$ device <value>
```

Listado de las conexiones WAN existentes actualmente.

3.2.1. Conexiones

```
1234@irouter>wan>FTTH$ add connection <value> type <value>
```

Permite añadir una nueva conexión dentro del área extensa.

Nombre

Nombre, en formato legible para el usuario, necesario para identificar la conexión WAN con respecto al resto..

Tipo

Protocolo utilizado por la conexión. El protocolo utilizado puede ser IP o PPPoE.

ip Internet Protocol (en español Protocolo de Internet) o IP es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados no fiable de mejor entrega posible sin garantias.

pppoe En esencia, es un protocolo túnel, que permite implementar una capa IP sobre una conexión entre dos puertos Ethernet, pero con las características de software del protocolo PPP, por lo que es utilizado para virtualmente marcar a otra máquina dentro de la red Ethernet, logrando una conexión serie con ella, con la que se pueden transferir paquetes IP, basado en las características del protocolo PPP.

3.3. Configuración de Conexión IP

```
1234@irouter>wan>FTTH$ connection <value>
```

Muestra el listado completo de los diferentes parámetros configurables para una conexión basada en el protocolo IP. Este protocolo se caracteriza por no estar orientado a conexión y es utilizado para la comunicación de datos por medio de paquetes dentro de una red conmutada.

3.3.1. Nombre

```
1234@irouter>wan>FTTH>ConIP$ name <value>
```

Nombre de la conexión en formato legible para el usuario.

3.3.2. Descripción

```
1234@irouter>wan>FTTH>ConIP$ description <value>
```

Proporciona una breve descripción, en formato legible para el usuario, acerca del objetivo de la conexión.

3.3.3. Número/prioridad VLAN

```
1234@irouter>wan>FTTH>ConIP$ vlan tag <value> priority <value>
```

Número de VLAN

Etiqueta utilizada para discernir la VLAN (Virtual Local Area Network) correspondiente a la conexión editada con respecto al resto de conexiones existentes. Los valores asignables están comprendidos entre 0 y 4094 siendo 0 el indicador de que no se usará etiqueta alguna.

Prioridad de VLAN

Prioridad de la VLAN con respecto al resto. El valor de la prioridad debe de estar comprendido entre 0 y 7 siendo 0 la menor prioridad y 7 la máxima. El valor -1 indica que se usará la prioridad por defecto.

3.3.4. Tipo de NAT

```
1234@irouter>wan>FTTH>ConIP$ nat <value>
```

Especifica el tipo de NAT (Network Address Protocol) utilizado. El NAT es un mecanismo que permite el intercambio de información entre dos redes incompatibles haciendo a la pasarela el único elemento visible de la red interna.

none Con esta opción el NAT se encuentra desactivado por lo que no se realizará traducción alguna de direcciones y puertos.

symmetric Similar al Full-cone NAT con la distinción de que en este caso se aplica una restricción de la dirección destino y del puerto, de tal forma que solamente el host de la red externa con el que cual ha establecido la comunicación previamente puede comunicarse con el host de la red interna, siendo descartadas las peticiones provenientes de cualquier otro host y puerto de la red externa.

full-cone En el Full-Cone NAT las peticiones de los hosts de la red interna son mapeados a una dirección y puerto diferentes a los del origen siendo el host inaccesible desde la red externa a menos que la comunicación, iniciada por el host de la red interna, se haya establecido anteriormente. Una vez mapeado la dirección y el puerto, el resto de hosts de la red externa pueden comunicarse con el host de la red interna por medio de este mapeado.

3.3.5. Protocolo de routing entrante

```
1234@irouter>wan>FTTH>ConIP$ route-protocol-rx <value>
```

Protocolo utilizado para el aprendizaje de rutas de rutado óptimas anunciadas por otros hosts de la red. En ningún caso de anunciarán las rutas de rutado creadas por la pasarela.

none Esta opción indica que no se aprenderán las rutas de rutado óptimas anunciadas por otros elementos de la red para alcanzar un destino.

rip2 Se trata de un protocolo a nivel de puerta de enlace que permite determinar la mejor ruta a seguir por los paquetes para alcanzar su destino utilizando como métrica el número de saltos. La versión 2 aporta mecanismos de autenticación además de añadir soporte para subredes CIDR (Classless Inter-Domain Routing) y VLSM (Variable Length Subnet Mask).

3.3.6. Habilitar cliente DHCP

```
1234@irouter>wan>FTTH>ConIP$ ip dhcp
```

Habilita el cliente DHCP (Dynamic Host Configuration Protocol) el cual se encarga de solicitar y configurar los parámetros indicados en la tabla –Opciones del cliente DHCP–.

3.3.7. IP

```
1234@irouter>wan>FTTH>ConIP$ ip address <value> mask <value> gateway <value>
```

Dirección IP

Dirección de red asignada a la interfaz WAN. La dirección de red permite diferenciar a un host dentro de la red en la que se encuentra.

Máscara de subred

Máscara de red que se aplicará a la dirección de red de la interfaz WAN. La máscara de red permite diferenciar la parte de la dirección de red correspondiente al identificador de la red de la parte que identifica al host.

Puerta de enlace por defecto

Puerta de enlace utilizada para encaminar los paquetes dirigidos a una red externa a la WAN.

3.3.8. Utilizar DNSs externos

```
1234@irouter>wan>FTTH>ConIP$ dns-override
```

Habilitando esta opción, siempre que se tenga activado el cliente DHCP, los servidores DNS anunciados a través de la WAN prevalecen sobre los configurados manualmente.

3.3.9. Dirección DMZ

```
1234@irouter>wan>FTTH>ConIP$ dmz <value>
```

Dirección de red a la que se redirigirá todo el tráfico que no haya sido encaminado hacia la red interna. Las siglas DMZ hacen referencia a una red local que se encuentra entre la red interna y la externa. Se puede decir que el objetivo principal de la DMZ es permitir que únicamente la red externa tenga acceso la DMZ mientras que para la red interna es inaccesible.

3.3.10. Reiniciar conexión

```
1234@irouter>wan>FTTH>ConIP$ reset
```

Reinicia la conexión volviendo a realizar todo el proceso de negociación como si se tratase de una nueva conexión.

3.3.11. Habilitar conexión

```
1234@irouter>wan>FTTH>ConIP$ enable
```

Habilita la conexión WAN. Solamente se puede habilitar una conexión WAN con etiqueta VLAN igual a 0.

3.3.12. Opciones del cliente DHCP

```
1234@irouter>wan>FTTH>ConIP$ dhcp-option <value>
```

Listado de opciones disponibles. Una opción es un par opción-valor siendo el campo opción único para cada entrada. De esta forma, si un cliente DHCP solicita un determinado código, se le devuelve su valor asociado.

Opción del cliente DHCP

Listado con los distintos tipos de información peticionable por el cliente DHCP de la red WAN en caso de que este se encuentre activo.

6 El cliente DHCP solicitará la dirección de red del servidor DNS.

15 El nombre del dominio se asignará por medio del protocolo DHCP.

42 Con esta opción se indica al cliente DHCP que deberá solicitar la dirección de red del servidor NTP (Network Time Protocol) de la WAN. Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

43 El cliente DHCP solicitará su vendor info que deberá suministrar en caso de que se le solicite.

66 Se solicita la dirección de red del servidor TFTP (Trivial File Transfer Protocol). Protocolo de transferencia de archivos sencillo, similar al FTP, definido por primera vez en 1980. Suele utilizarse en la transferencia de archivos pequeños entre computadoras de una red.

120 El cliente DHCP solicitará la información relevante al servidor SIP. Un servidor SIP es el principal componente de una centralita IP, que maneja la configuración de todas las llamadas SIP en la red. Un servidor SIP es también conocido como Proxy SIP o Registrador.

250 Se solicita la dirección de red de un servicio propietario.

3.3.13. Servidores DNS

```
1234@irouter>wan>FTTH>ConIP$ dns-server <value>
```

Lista de servidores DNS (Domain Name Server). Un servidor DNS es el encargado de traducir nombres de dominio a direcciones de red. El orden en el cual se realizan las peticiones es descendente.

Servidor DNS

Dirección de red del servidor DNS a la cual se encaminará las peticiones de resolución de dominios.

3.3.14. Tabla de mapeo de puertos

```
1234@irouter>wan>FTTH>ConIP$ port-mapping protocol <value> external-port <value>
     internal-client <value> internal-port <value> description <value>
```

Tabla para la redirección o mapeado de puertos. El mapeado de puertos es un mecanismo que permite redireccionar el tráfico dirigido a un puerto determinado de una pasarela con NAT hacia una dirección y un puerto de un host de la red interna.

Protocolo

Protocolo de la capa de transporte sobre el cual se aplica la redirección.

tcp Aplica el redireccionamiento sobre el tráfico TCP. Este protocolo está orientado a la transmisión segura de información por lo que las aplicaciones más comunes basadas en éste protocolo son WEBs, correos y FTPs.

udp Aplica el redireccionamiento sobre el tráfico UDP. A diferencia del protocolo TCP, el protocolo UDP está orientado a la transferencia rápida de información con el riesgo de pérdida de paquetes. Debido a la naturaleza de este protocolo, su ámbito está enfocado principalmente a aplicaciones multimedia.

Puerto externo

Puerto de la red interna sobre el cual se aplicará la redirección. Se puede utilizar el separador - para especificar rangos. Por ejemplo, la entrada 40000 - 50000 indicaría que se direccionarían los puertos desde el 40000 a 50000, ambos inclusive.

Cliente interno

Dirección IP del dispositivo de la red interna al que se redirigirá todo el tráfico.

Puerto interno

Puerto del host de la red interna al que el router redirigirá el tráfico.

Descripción

Muestra una breve descripción acerca del objetivo de la regla de redirección.

3.4. Configuración de Conexión PPPoE

```
1234@irouter>wan>FTTH$ connection <value>
```

Muestra las diferentes opciones aplicables a una conexión PPPoE (Point-to-Point Protocol over Ethernet). Su propósito habitual es el de establecer una comunicación entre el router y una pasarela ATM (Asynchronous Transfer Mode) de un proveedor.

3.4.1. Nombre

```
1234@irouter>wan>FTTH>ConPPPoE$ name <value>
```

Nombre de la conexión en formato legible para el usuario.

3.4.2. Descripción

```
1234@irouter>wan>FTTH>ConPPPoE$ description <value>
```

Proporciona una breve descripción, en formato legible para el usuario, acerca del objetivo de la conexión.

3.4.3. Número/prioridad VLAN

```
1234@irouter>wan>FTTH>ConPPPoE$ vlan tag <value> priority <value>
```

Número de VLAN

Etiqueta utilizada para discernir la VLAN (Virtual Local Area Network) correspondiente a la conexión editada con respecto al resto de conexiones existentes. Los valores asignables están comprendidos entre 0 y 4094 siendo 0 el indicador de que no se usará etiqueta alguna.

Prioridad de VLAN

Prioridad de la VLAN con respecto al resto. El valor de la prioridad debe de estar comprendido entre 0 y 7 siendo 0 la menor prioridad y 7 la máxima. El valor -1 indica que se usará la prioridad por defecto.

3.4.4. Tipo de NAT

```
1234@irouter>wan>FTTH>ConPPPoE$ nat <value>
```

Especifica el tipo de NAT (Network Address Protocol) utilizado. El NAT es un mecanismo que permite el intercambio de información entre dos redes incompatibles haciendo a la pasarela el único elemento visible de la red interna.

none Con esta opción el NAT se encuentra desactivado por lo que no se realizará traducción alguna de direcciones y puertos.

symmetric Similar al Full-cone NAT con la distinción de que en este caso se aplica una restricción de la dirección destino y del puerto, de tal forma que solamente el host de la red externa con el que cual ha establecido la comunicación previamente puede comunicarse con el host de la red interna, siendo descartadas las peticiones provenientes de cualquier otro host y puerto de la red externa.

full-cone En el Full-Cone NAT las peticiones de los hosts de la red interna son mapeados a una dirección y puerto diferentes a los del origen siendo el host inaccesible desde la red externa a menos que la comunicación, iniciada por el host de la red interna, se haya establecido anteriormente. Una vez mapeado la dirección y el puerto, el resto de hosts de la red externa pueden comunicarse con el host de la red interna por medio de este mapeado.

3.4.5. Protocolo de routing entrante

```
1234@irouter>wan>FTTH>ConPPPoE$ route-protocol-rx <value>
```

Protocolo utilizado para el aprendizaje de rutas de rutado óptimas anunciadas por otros hosts de la red. En ningún caso de anunciarán las rutas de rutado creadas por la pasarela.

none Esta opción indica que no se aprenderán las rutas de rutado óptimas anunciadas por otros elementos de la red para alcanzar un destino.

rip2 Se trata de un protocolo a nivel de puerta de enlace que permite determinar la mejor ruta a seguir por los paquetes para alcanzar su destino utilizando como métrica el número de saltos. La versión 2 aporta mecanismos de autenticación además de añadir soporte para subredes CIDR (Classless Inter-Domain Routing) y VLSM (Variable Length Subnet Mask).

3.4.6. Inicio conexión

```
1234@irouter>wan>FTTH>ConPPPoE$ trigger <value>
```

Determina el comportamiento de la conexión PPPoE pudiéndose así poder utilizar la conexión en función de las características de la red a la que pertenezca.

demand El tráfico viaja a través de esta conexión solo cuando se necesita.

persist No se establece ninguna limitación con respecto a la información que viaja a través de esta conexión.

3.4.7. Usuario

```
1234@irouter>wan>FTTH>ConPPPoE$ username <value>
```

Nombre de usuario que se utilizará en la autenticación de la conexión.

3.4.8. Contraseña

```
1234@irouter>wan>FTTH>ConPPPoE$ password <value>
```

Contraseña a utilizar para la autenticación de la conexión PPPoE.

3.4.9. Nombre de AC

```
1234@irouter>wan>FTTH>ConPPPoE$ ac-name <value>
```

Nombre del AC (Access Concentrator) o servidor PPPoE.

3.4.10. Nombre del servicio

```
1234@irouter>wan>FTTH>ConPPPoE$ service-name <value>
```

Nombre del servicio utilizado internamente por la conexión.

3.4.11. Utilizar DNSs externos

```
1234@irouter>wan>FTTH>ConPPPoE$ dns-override
```

Habilitando esta opción, siempre que se tenga activado el cliente DHCP, los servidores DNS anunciados a través de la WAN prevalecen sobre los configurados manualmente.

3.4.12. Dirección DMZ

```
1234@irouter>wan>FTTH>ConPPPoE$ dmz <value>
```

Dirección de red a la que se redirigirá todo el tráfico que no haya sido encaminado hacia la red interna. Una zona desmilitarizada es una red local que se encuentra entre la red interna y la externa. Se puede decir que el objetivo principal de la DMZ es permitir que únicamente la red externa tenga acceso la DMZ mientras que para la red interna es inaccesible.

3.4.13. Reiniciar conexión

```
1234@irouter>wan>FTTH>ConPPPoE$ reset
```

Reinicia la conexión volviendo a realizar todo el proceso de negociación como si se tratase de una nueva conexión.

3.4.14. Habilitar conexión

```
1234@irouter>wan>FTTH>ConPPPoE$ enable
```

Habilita la conexión WAN. Solamente se puede habilitar una conexión WAN con etiqueta VLAN igual a 0.

3.4.15. Servidores DNS

```
1234@irouter>wan>FTTH>ConPPPoE$ dns-server <value>
```

Lista de servidores DNS (Domain Name Server). Un servidor DNS es el encargado de traducir nombres de dominio a direcciones de red. El orden en el cual se realizan las peticiones es descendente.

Servidor DNS

Dirección de red del servidor DNS a la cual se encaminará las peticiones de resolución de dominios.

3.4.16. Tabla de mapeo de puertos

```
1234@irouter>wan>FTTH>ConPPPoE$ port-mapping protocol <value> external-port
     <value> internal-client <value> internal-port <value> description <value>
```

Tabla para la redirección o mapeado de puertos. El mapeado de puertos es un mecanismo que permite redireccionar el tráfico dirigido a un puerto determinado de una pasarela con NAT hacia una dirección y un puerto de un host de la red interna.

Protocolo

Protocolo de la capa de transporte sobre el cual se aplica la redirección.

tcp Aplica el redireccionamiento sobre el tráfico TCP. Este protocolo está orientado a la transmisión segura de información por lo que las aplicaciones más comunes basadas en este protocolo son WEBs, correos y FTPs.

udp Aplica el redireccionamiento sobre el tráfico UDP. A diferencia del protocolo TCP, el protocolo UDP está orientado a la transferencia rápida de información con el riesgo de pérdida de paquetes. Debido a la naturaleza de este protocolo, su ámbito está enfocado principalmente a aplicaciones multimedia.

Puerto externo

Puerto de la red interna sobre el cual se aplicará la redirección. Se puede utilizar el separador - para especificar rangos. Por ejemplo, la entrada 40000 - 50000 indica que se direccionan los puertos desde el 40000 a 50000, ambos inclusive.

Cliente interno

Dirección IP del host de la red interna al que se redirigirá todo el tráfico.

Puerto interno

Puerto del host de la red interna al que el router redirigirá el tráfico. El valor 0 no está permitido.

Descripción

Muestra una breve descripción acerca del objetivo de la regla de redirección.

3.5. Configuración de Proxy IGMP

```
1234@irouter>wan$ igmp-proxy
```

Permite que la pasarela funcione como proxy multicast en las interfaces downstream (interfaces que se alejan del nodo raíz del árbol IGMP). Se selecciona una interfaz como upstream (interfaz que se acerca al nodo raíz del árbol IGMP) por la cual se recibe todo el tráfico multicast. El proxy IGMP conoce las interfaces downstream en función de los informes de pertenencia que ha ido recibiendo anteriormente. El proxy duplica el tráfico, en las interfaces downstream, que va recibiendo por la interfaz upstream minimizándose, de ésta forma, el uso del ancho de banda de la red.

3.5.1. Conexión de subida

```
1234@irouter>wan>igmp-proxy$ upstream <value>
```

Nombre de la interfaz upstream por la cual se recibe el tráfico multicast.

3.5.2. Habilitar proxy IGMP

```
1234@irouter>wan>igmp-proxy$ enable
```

Permite que la pasarela funcione como proxy IGMP.

Capítulo 4

Ethernet

4.1. Configuración de Ethernet

```
1234@irouter>$ ethernet
```

Muestra todos los aspectos relacionados con las interfaces Ethernet. Ethernet (también conocido como estándar IEEE 802.3) es un estándar de transmisión de datos para redes de área local.

4.2. Configuración de Interfaz Ethernet LAN

```
1234@irouter>ethernet$ interface <value>
```

Permite monitorizar y modificar aspectos relacionados con la entrada del switch seleccionado a bajo nivel.

4.2.1. Apagar

```
1234@irouter>ethernet>switch0$ shutdown
```

Deshabilita la entrada del switch seleccionada.

4.2.2. Modo

```
1234@irouter>ethernet>switch0$ duplex-mode <value>
```

Modo de operación utilizado en las comunicaciones a nivel de la capa de enlace.

auto La selección del modo de operación es automático y es determinado en función de las características de la comunicación.

half En este modo, el envío de información y recepción de la información es bidireccional pero no simultáneo.

full En este modo, el envío de información y recepción de la información es bidireccional y simultáneo.

4.2.3. Control de MAC

```
1234@irouter>ethernet>switch0$ mac-control
```

Habilita el control de acceso de los clientes de la LAN en función de su dirección física o MAC. De tal modo que, un cliente con una MAC distinta a las permitidas, no tendrá acceso al área local.

4.2.4. Tasa de bit máxima

```
1234@irouter>ethernet>switch0$ max-bit-rate <value>
```

Velocidad máxima de transmisión. Los valores son 10, 100 y 1000 y todos ellos están dados en Mb.

auto La velocidad de transmisión se establece en función de las características del medio.

4.3. Configuración de Interfaz WAN Ethernet

```
1234@irouter>ethernet$ interface <value>
```

Muestra toda la información relevante a la interfaz de Ethernet conectada a la red WAN (waneth0).

4.3.1. Modo

```
1234@irouter>ethernet>waneth0$ duplex-mode <value>
```

Modo de operación utilizado en las comunicaciones a nivel de la capa de enlace.

auto La selección del modo de operación es automático y es determinado en función de las características de la comunicación.

half En este modo, el envío de información y recepción de la información es bidireccional pero no simultáneo.

full En este modo, el envío de información y recepción de la información es bidireccional y simultáneo.

4.3.2. Tasa de bit máxima

```
1234@irouter>ethernet>waneth0$ max-bit-rate <value>
```

Velocidad máxima de transmisión. Los valores son 10, 100 y 1000 y todos ellos están dados en Mb.

auto La velocidad de transmisión se establece en función de las características de la red.

Capítulo 5

Wi-Fi

5.1. Configuración de Wi-Fi

```
1234@irouter>$ wireless
```

Wi-Fi es una marca de la Wi-Fi Alliance la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

5.2. Configuración de Interfaz inalámbrico

```
1234@irouter>wireless$ interface <value>
```

Muestra todos los parámetros de configuración de la red inalámbrica.

5.2.1. Deshabilitar radio

```
1234@irouter>wireless>2.4GHz$ disable-radio
```

Deshabilita la interfaz inalámbrica de la pasarela por lo que no se emitirá información alguna por medio del interfaz inalámbrico.

5.2.2. SSID

```
1234@irouter>wireless>2.4GHz$ ssid <value>
```

El SSID (Service Set Identifier) permite diferenciar una red inalámbrica del resto mediante una cadena de texto en formato legible para el usuario. La longitud de la cadena está limitada a un máximo de 32 caracteres.

5.2.3. Ocultar SSID

```
1234@irouter>wireless>2.4GHz$ hide-ssid
```

Activando esta opción, el SSID no se publicará por difusión, sino que se ocultará. De esta forma, para un usuario medio que ignore el valor del SSID, la red será inexistente.

5.2.4. Estándar

```
1234@irouter>wireless>2.4GHz$ standard <value>
```

Especifica el estándar del IEEE (Institute of Electrical and Electronics Engineers) a utilizar a la hora de realizar las comunicaciones inalámbricas. La elección del estándar deberá de corresponder con las características de los potenciales clientes de la red.

a Modo compatible con el estándar 802.11a con velocidad teórica máxima de hasta 54 Mbit/s.

b Modo compatible con el estándar 802.11b con velocidad máxima de transferencia de hasta 11 Mbit/s.

b/g Modo compatible con los estándares 802.11b/g con velocidades máximas de transferencia de hasta 54 Mbit/s.

g Modo compatible con el estándar 802.11g con velocidades máximas de transferencia de hasta 54 Mbit/s.

b/g/n Modo compatible con los estándares 802.11b/g/n con velocidades teóricas de hasta 300 Mbit/s.

n Modo compatible con el estándar 802.11n con una velocidad teórica de hasta 300 Mbit/s.

5.2.5. Canal

```
1234@irouter>wireless>2.4GHz$ channel <value>
```

Listado de las diferentes bandas de frecuencia en la que se descompone el estándar seleccionado. Una selección errónea del canal aumenta significativamente el número de colisiones, mientras que uno adecuado, las minimiza.

auto La selección del canal la realizará automáticamente la pasarela en función del uso de las diferentes bandas por el resto de dispositivos inalámbricos.

5.2.6. Ancho de canal

```
1234@irouter>wireless>2.4GHz$ width-channel <value>
```

Permite configurar el ancho de banda del canal.

20 Ancho de banda de 20 Mhz (canal individual).

40 Ancho de banda de 40 Mhz (doble canal). Permite coexistencia con canales de 20 Mhz.

5.2.7. Potencia de transmisión

```
1234@irouter>wireless>2.4GHz$ tx-power <value>
```

Porcentaje de la potencia máxima de transmisión de la red inalámbrica. El alcance de la red inalámbrica varía en función de la potencia de transmisión, aumentando proporcionalmente con ésta.

5.2.8. Modo de operación

```
1234@irouter>wireless>2.4GHz$ op-mode <value>
```

Permite configurar el modo de operación HT (High Throughput) del punto de acceso.

mixed En este modo los paquetes serán transmitidos con un preámbulo compatible con los antiguos modos 802.11g - los campos STF, LTF y SF se transmitirán para que puedan ser decodificados por los dispositivos 802.11g. El resto del paquete tiene un nuevo formato.

green-field En este modo los paquetes de alto bitrate serán transmitidos sin preámbulo de compatibilidad con dispositivos 802.11g.

5.2.9. Intervalo de guarda

```
1234@irouter>wireless>2.4GHz$ guard-interval <value>
```

Permite configurar el intervalo de guarda. El propósito del intervalo de guarda es introducir inmunidad a los retardos, a los ecos y a las reflexiones de propagación, a los cuales los datos digitales son normalmente muy sensibles. Cuanto más corto es el intervalo de guarda, más alta es la tasa de error en la transferencia de paquetes, si el retardo de propagación del canal es superior al intervalo de guarda y/o cuando la sincronización de tiempo entre el transmisor y el receptor no es precisa.

long Intervalo de guarda de 800 ns.

short Intervalo de guarda de 400 ns.

5.2.10. Protección 802.11b/g

```
1234@irouter>wireless>2.4GHz$ bg-protection <value>
```

Permite configurar el modo de funcionamiento de la red inalámbrica para activar o no la adaptación de la velocidad de la misma en función del tipo de clientes.

auto En el caso de existir clientes funcionando en modo 802.11b, reduce la velocidad de transmisión a la velocidad del estándar 802.11b, en caso contrario, su funcionamiento es el normal.

enabled Reduce la velocidad de transmisión al del estándar 802.11b independientemente de la existencia o no de clientes que utilicen este estándar.

disabled Deshabilita la reducción de la velocidad de transmisión.

5.2.11. Habilitar transmisión de AMSDU

```
1234@irouter>wireless>2.4GHz$ tx-amsdu
```

Habilita la transmisión de múltiples MSDUs agregadas en una MPDU.

5.2.12. Filtrado de MAC

```
1234@irouter>wireless>2.4GHz$ mac-control
```

Habilita el control de acceso por medio de las direcciones MAC permitidas explícitamente dentro de la pestaña de configuración de la LAN.

5.2.13. Habilitar punto de acceso

```
1234@irouter>wireless>2.4GHz$ enable
```

Habilita la red inalámbrica.

5.3. Configuración de Seguridad inalámbrica

```
1234@irouter>wireless>2.4GHz$ security
```

Gestiona los aspectos relacionados con la seguridad de los diferentes modos de protección de la red inalámbrica.

5.3.1. Modo de seguridad

```
1234@irouter>wireless>2.4GHz>security$ mode <value>
```

Listado con los diferentes sistemas de protección aplicables a la red inalámbrica.

basic Modo básico de seguridad. Se trata del mecanismo de protección de la red inalámbrico más básico. En este modo, se puede operar sin protección alguna o con seguridad WEP.

wpa Red inalámbrica protegida por WPA (Wi-Fi Protected Access). Se trata de un sistema de seguridad inalámbrica cuyo objetivo principal es paliar las carencias del sistema WEP.

wpa2 Red inalámbrica protegida por WPA (Wi-Fi Protected Access 2). Sustituye el algoritmo de cifrado del WPA por otro basado de AES lo que mejora la seguridad.

wpa/wpa2 Modo de compatibilidad con los modos WPA/WPA2. De esta manera, la red inalámbrica es capaz de operar con los clientes que utilicen alguno de estos dos sistemas.

5.3.2. Clave pre-compartida

```
1234@irouter>wireless>2.4GHz>security$ psk <value>
```

Clave utilizada para la autenticación del cliente dentro de la red inalámbrica.

5.4. Configuración de Seguridad básica

```
1234@irouter>wireless>2.4GHz>security$ basic-settings
```

Modo básico de seguridad. Se trata del mecanismo de protección de la red inalámbrico más simple. En este modo, se puede operar sin protección alguna o con seguridad WEP.

5.4.1. Autenticación

```
1234@irouter>wireless>2.4GHz>security>basic$ authentication mode <value>
     encryption <value>
```

Modo de autenticación

No se utilizará mecanismo de autenticación alguno, por lo que cualquier cliente, sin importar su identidad, podrá acceder a la red.

shared Se utiliza una clave compartida como método de control de acceso.

Modo de cifrado

Sistema de protección aplicado a la información que viaje a través de la red inalámbrica.

none La información viaja sin cifrado alguno a través de la red.

wep La información viaja cifrada por medio del sistema cifrado WEP (Wired Equivalent Privacy). La clave debe ser un valor ASCII con una longitud mínima de 13 caracteres y una longitud máxima de 26.

5.4.2. Primera clave WEP

```
1234@irouter>wireless>2.4GHz>security>basic$ wepkey 1 <value>
```

Asigna la primera de las contraseñas WEP, especificadas en el cuadro de texto correspondiente, como clave actual de acceso a la red inalámbrica.

5.4.3. Segunda clave WEP

```
1234@irouter>wireless>2.4GHz>security>basic$ wepkey 2 <value>
```

Asigna la segunda de las contraseñas WEP, especificadas en el cuadro de texto correspondiente, como clave actual de acceso a la red inalámbrica.

5.4.4. Tecera clave WEP

```
1234@irouter>wireless>2.4GHz>security>basic$ wepkey 3 <value>
```

Asigna la tercera de las contraseñas WEP, especificadas en el cuadro de texto correspondiente, como clave actual de acceso a la red inalámbrica.

5.4.5. Cuarta clave WEP

```
1234@irouter>wireless>2.4GHz>security>basic$ wepkey 4 <value>
```

Asigna la cuarta de las contraseñas WEP, especificadas en el cuadro de texto correspondiente, como clave actual de acceso a la red inalámbrica.

5.4.6. Clave WEP por defecto

```
1234@irouter>wireless>2.4GHz>security>basic$ default-wepkey <value>
```

Clave WEP utilizada por defecto.

1 Primera de la cuatro contraseñas WEP seleccionables posteriormente por medio del desplegable correspondiente.

2 Segunda de la cuatro contraseñas WEP seleccionables posteriormente por medio del desplegable correspondiente.

3 Tercera de la cuatro contraseñas WEP seleccionables posteriormente por medio del desplegable correspondiente.

4 Cuarta de la cuatro contraseñas WEP seleccionables posteriormente por medio del desplegable correspondiente.

5.5. Configuración de Seguridad para el acceso protegido Wi-Fi

```
1234@irouter>wireless>2.4GHz>security$ wpa-settings
```

Gestiona los aspectos relacionados con el sistema de seguridad para redes inalámbricas WPA. WPA utiliza cifrado de clave dinámico de esta forma, la clave varia constantemente. WPA proporciona una seguridad elevada y es el método recomendado si los clientes de la red soportan este sistema. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

5.5.1. Autenticación

```
1234@irouter>wireless>2.4GHz>security>wpa$ authentication mode <value>
     encryption <value>
```

Modo de autenticación

Modo de autenticación utilizado para identificar a un cliente dentro de la red inalámbrica.

psk Clave utilizada para la autenticación del cliente dentro de la red inalámbrica.

Modo de cifrado

Sistema de encriptación a utilizar para cifrar la información que viaje a través de la red inalámbrica.

tkip Se trata de un protocolo que es capaz de cambiar las claves dinámicamente a medida que el sistema es utilizado. De esta forma, evita los ataques de recuperación de clave (que no son más que ataques estadísticos) a los que es susceptible el sistema WEP.

aes El criptosistema AES (Advanced Encryption Standard) es un esquema de cifrado por bloques que soporta tamaños de clave de 128, 192, 256 bits. Ha sido adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

tkip/aes Modo de compatibilidad con los modos AES y TKIP. Así, la pasarela es capaz de comunicarse con clientes que utilicen uno de estos dos métodos indistintamente.

5.6. Configuración de Seguridad para el acceso protegido Wi-Fi 2

```
1234@irouter>wireless>2.4GHz>security$ wpa2-settings
```

Gestiona los aspectos relaciones con el sistema de seguridad WPA 2.

5.6.1. Autenticación

```
1234@irouter>wireless>2.4GHz>security>wpa2$ authentication mode <value>
     encryption <value>
```

Modo de autenticación

Modo de autenticación utilizado para identificar a un cliente dentro de la red inalámbrica.

psk Clave utilizada para la autenticación del cliente dentro de la red inalámbrica.

Modo de cifrado

Sistema de encriptación a utilizar para cifrar la información que viaje a través de la red inalámbrica.

tkip Se trata de un protocolo que es capaz de cambiar las claves dinámicamente a medida que el sistema es utilizado. De esta forma, evita los ataques de recuperación de clave (que no son más que ataques estadísticos) a los que es susceptible el sistema WEP.

aes El criptosistema AES (Advanced Encryption Standard) es un esquema de cifrado por bloques que soporta tamaños de clave de 128, 192, 256 bits. Ha sido adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

tkip/aes Modo de compatibilidad con los modos AES y TKIP. Así, la pasarela es capaz de comunicarse con clientes que utilicen unos de estos dos métodos indistintamente.

5.7. Configuración de Wi-Fi Protected Setup

```
1234@irouter>wireless>2.4GHz$ wps
```

Simplifica el proceso de autenticación dentro de redes inalámbricas permitiendo conectar estaciones Wi-Fi mediante la pulsación de un botón o introduciendo un código PIN.

5.7.1. Habilitar WPS

```
1234@irouter>wireless>2.4GHz>wps$ enable
```

Habilita la funcionalidad WPS (Wi-Fi Protected Setup).

5.7.2. Código PIN WPS

```
1234@irouter>wireless>2.4GHz>wps$ password <value>
```

Código PIN de la estación Wi-Fi que desea conectarse al punto de acceso protegido. El código PIN debe de tener una longitud de 8 dígitos.

5.8. Configuración de Wi-Fi Multimedia

```
1234@irouter>wireless>2.4GHz$ wmm
```

Wi-fi Multimedia, también conocido como Wireless Multimedia Extensions (WME), es una certificación de interoperabilidad de la Wi-Fi Alliance, basado en el estándar IEEE 802.11e. Proporciona funcionalidades Qos (Quality of Service) básicas en redes IEEE 802.11

5.8.1. Habilitar APSD

```
1234@irouter>wireless>2.4GHz>wmm$ apsd
```

Habilita la utilización del sistema APSD (Automatic Power Save Delivery). Este mecanismo posibilita la reducción del consumo energético de los clientes conectados a la red inalámbrica siempre que los clientes también soporten APSD.

5.8.2. Habilitar WMM

```
1234@irouter>wireless>2.4GHz>wmm$ enable
```

Habilita la funcionalidad WMM.

5.9. Configuración de Punto de acceso virtual

```
1234@irouter>wireless>2.4GHz$ virtual-ap
```

Permite crear puntos de acceso virtuales de tal forma que, aunque exista un único punto de acceso físico, virtualmente pueden existir varios redes inalámbricas cada una con su propia configuración. El número máximo de redes inalámbricas virtuales está limitado a 4.

5.9.1. Añadir AP virtual

```
1234@irouter>wireless>2.4GHz>virtual-ap$ add virtual-ap <value>
```

Añade una nueva red inalámbrica virtual. Se pueden añadir un máximo de 3 redes inalámbricas virtuales.

AP Virtual

Permite crear una nueva red inalámbrica virtual.

5.10. Configuración de Punto de acceso virtual

```
1234@irouter>wireless>2.4GHz>virtual-ap$ virtual-ap <value>
```

Muestra las distintas opciones aplicables al punto de acceso inalámbrico virtual.

5.10.1. SSID

```
1234@irouter>wireless>2.4GHz>virtual-ap>2.4GHz:1$ ssid <value>
```

El SSID (Service Set Identifier) permite diferenciar una red inalámbrica del resto mediante una cadena de texto en formato legible para el usuario. La longitud de la cadena está limitada a un máximo de 32 caracteres.

5.10.2. Ocultar SSID

```
1234@irouter>wireless>2.4GHz>virtual-ap>2.4GHz:1$ hide-ssid
```

Oculta el SSID o identificador de la red. De esta manera, el identificador no se publicará y los clientes tendrán que conocerlo previamente para poder conectarse a la red.

5.10.3. Control de MAC

```
1234@irouter>wireless>2.4GHz>virtual-ap>2.4GHz:1$ mac-control
```

Habilita el filtrado de los clientes de la red inalámbrica en función de su MAC. Así, solo se permitirá el acceso de aquellos clientes permitidos explícitamente dentro de la tabla de filtrado MAC.

5.10.4. Habilitar punto de acceso

```
1234@irouter>wireless>2.4GHz>virtual-ap>2.4GHz:1$ enable
```

Habilita la red inalámbrica virtual-.

Capítulo 6

Forwarding

6.1. Configuración de Forwarding

```
1234@irouter>$ forwarding
```

Permite redirigir el tráfico con un determinado destino a una puerta de enlace o a un conexión creada previamente.

6.1.1. Conexión por defecto

```
1234@irouter>forwarding$ default-connection <value>
```

Permite seleccionar la conexión por defecto a la que se redirigirá todo el tráfico que no va a una red directamente conectada a la pasarela o no encaja en ninguna de las rutas definidas en esta página.

6.1.2. Rutas via gateway

```
1234@irouter>forwarding$ gw-route destip <value> mask <value> gateway <value>
     metric <value>
```

Listado de reglas de redirección que tienen como destino una puerta de enlace específica.

Dirección IP

Dirección de red destino a la que se aplicará la regla de redirección. Si la dirección a la que va dirigido el tráfico pertenece a la red indicada por ésta IP o si concuerda con ésta, se aplicará la regla, en otro caso se evaluará la siguiente. En el caso de que se hayan evaluado todas las reglas y no se haya encontrado ninguna que concuerde y, en caso de que la pasarela no esté conectada directamente a la red a la que va dirigida el paquete, se aplicará la regla por defecto.

Máscara de subred

Máscara de red que se aplicará a la dirección de red destino.

Puerta de enlace

Puerta de enlace a la que se redireccionará el paquete. La puerta de enlace deberá conocer el camino hacia la red o host destino.

Métrica

Se trata de un atributo utilizado por los protocolos de rutado para determinar el coste relativo de enviar un paquete a través de un enlace. Este valor puede ser -1, el cual es el valor por defecto, o estar comprendido entre 1 65535.

6.1.3. Rutas via interfaz

```
1234@irouter>forwarding$ if-route destip <value> mask <value> interface <value>
     metric <value>
```

Listado de reglas de redirección que tienen como destino una interfaz específica creada previamente.

Dirección IP

Dirección de red destino a la que se aplicará la regla de redirección. Si la dirección a la que va dirigido el tráfico pertenece a la red indicada por esta IP o si concuerda con ésta, se aplicará la regla. En el caso de que se hayan evaluado todas las reglas y no se haya encontrado ninguna que concuerde y, en caso de que la pasarela no esté conectada directamente a la red a la que va dirigida el paquete, se aplicará la regla por defecto.

Máscara de subred

Máscara de red que se aplicará a la dirección de red destino.

Interfaz

Interfaz a la que se redirigirá el tráfico que verifique la regla.

Métrica

Se trata de un atributo utilizado por los protocolos de rutado para determinar el coste relativo de enviar un paquete a través de un enlace. Este valor puede ser -1, el cual es el valor por defecto, o estar comprendido entre 1 65535.

Capítulo 7

Firewall

7.1. Configuración de Firewall

```
1234@irouter>$ firewalls
```

Permite definir y visualizar la configuración actual de firewall. Dicho elemento controla el tráfico de paquetes que entra y sale en una determinada conexión de red. Cada interfaz podrá disponer de un conjunto diferente de reglas de filtrado para determinados flujos de paquetes objetivo.

7.1.1. Firewall

```
1234@irouter>firewalls$ add name <value> interface <value> type <value>
```

La siguiente tabla muestra información sobre los diferentes conjuntos de reglas de filtrado que se llevarán a cabo en el sistema. Además permite la creación de nuevos conjuntos de reglas de filtrado.

Nombre

Se trata del nombre que identificará al conjunto de reglas de filtrado que afectarán a una determinada interfaz.

Interfaz

Define la interfaz sobre la que se aplicará el conjunto de reglas de filtrado. Debe tratarse de una interfaz previamente definida.

all Establece que el conjunto de reglas de filtrado afetará a toda las interfaces del router.

Tipo

Define si el conjunto de reglas de filtrado afecta al tráfico de paquetes entrante o saliente para la interfaz previamente establecida.

in El conjunto de reglas de filtrado afecta al tráfico de paquetes entrante para la interfaz previamente definida.

out El conjunto de reglas de filtrado afecta al tráfico de paquetes saliente para la interfaz previamente definida.

7.2. Configuración de Información de firewall

```
1234@irouter>firewalls$ firewall <value>
```

Permite configurar el conjunto de reglas de filtrado que realizarán la función de firewall en el sistema. Básicamente permite añadir nuevas reglas de filtrado para una determinada interfaz.

7.2.1. Nombre

```
1234@irouter>firewalls>firewall1$ name <value>
```

Se trata del nombre que identificará al conjunto de reglas de filtrado para una determinada interfaz.

7.2.2. Configuración

```
1234@irouter>firewalls>firewall1$ set-firewall interface <value> type <value>
```

Interfaz

Define la interfaz sobre la que se aplicará el conjunto de reglas de filtrado. Debe tratarse de una interfaz previamente definida.

all Establece que el conjunto de reglas de filtrado afectará a toda las interfaces del router.

Tipo

Define si el conjunto de reglas de filtrado afecta al tráfico de paquetes entrante o saliente para la interfaz definida.

in El conjunto de reglas de filtrado afecta al tráfico de paquetes entrante para la interfaz previamente definida.

out El conjunto de reglas de filtrado afecta al tráfico de paquetes saliente para la interfaz previamente definida.

7.2.3. Acción por defecto

```
1234@irouter>firewalls>firewall1$ default-action <value>
```

Define la acción por defecto en caso de que no exista ninguna regla de filtrado definida para un determinado tráfico de paquetes. Básicamente se pueden seleccionar dos acciones por defecto, aceptar los paquetes (opción Permit) o bien rechazarlos (opción Drop).

drop La acción por defecto es rechazar los paquetes para los que no exista ninguna regla de filtrado.

permit La acción por defecto es aceptar los paquetes para los que no exista ninguna regla de filtrado.

7.2.4. Reglas

```
1234@irouter>firewalls>firewall1$ add rule <value>
```

Añade una nueva regla de filtrado no nula al firewall. La evaluación de las reglas es descendente.

Nombre

Se trata del nombre que deseemos asignar a una determinada regla de filtrado. A continuación podremos configurar los diferentes atributos que defininán el comportamiento de la regla de filtrado. Se recomienda un nombre explicativo que permita identificar claramente el tipo de filtrado que realiza.

7.3. Configuración de Regla

```
1234@irouter>firewalls>firewall1$ rule <value>
```

Permite la configuración de la regla de filtrado definida por dicho nombre. La configuración de dicha regla consistirá en definir los siguientes atributos: protocolo, tipo de acción, tipo de rechazo, tipo de ICMP, dirección IP actual, máscara origen, puerto inicial de origen, puerto de origen final, dirección ip destino, máscara destino, puerto inicial de destino, puerto final de destino y si se desea habilitar dicha regla.

7.3.1. Regla de configuración

```
1234@irouter>firewalls>firewall1>rule1$ set-rule protocol <value> action <value>
     reject-type <value>
```

Protocolo

Define el protocolo que se verá afectado por la regla de filtrado definida. La regla de filtrado puede afectar a Any (afecta a todos), ICMP (Internet Control Message Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol) y TCP-UDP.

any La regla definida afecta a todos los protocolos

icmp La regla definida afecta al protocolo ICMP

tcp La regla definida afecta al protocolo TCP

udp La regla definida afecta al protocolo UDP

tcp-udp La regla definida afecta al protocolo TCP-UDP

Acción

Permite definir la acción que llevará a cabo la regla de filtrado sobre el tráfico de paquetes objetivo. La regla de filtrado puede permitir dicho flujo de paquetes (PERMIT), rechazarlo (REJECT), o bien descartarlo (DROP).

drop El valor Drop establece que la acción de la regla de filtrado consiste en descartar el flujo de paquetes definido en la regla.

permit El valor Permit establece que la acción de la regla de filtrado es permitir el flujo de paquetes definido en la regla.

reject El valor Reject establece que la acción de la regla de filtrado consiste en rechazar el flujo de paquetes definidos en la regla. A diferencia de la opción Drop, esta opción permite establecer un tipo de rechazo: icmp-net-unreachable, icmp-host-unreachable, icmp-proto-unreachable, icmp-port-unreachable, icmp-net-prohibited, icmp-host-prohibited y tcp-reset

Tipo de rechazo

Permite seleccionar el tipo de rechazo que sufre el flujo de paquetes objetivo cuando la acción de la regla de filtrado se trata de Reject. Los tipos de rechazo posibles son los siguientes: icmp-net-unreachable (red inaccesible), icmp-host-unreachable (host inaccesible), icmp-proto-unreachable (protocolo inaccesible), icmp-port-unreachable (puerto inaccesible), icmp-net-prohibited, icmp-host-prohibited y tcp-reset

icmp-net-unreachable Envía un icmp de red inalcanzable.

icmp-host-unreachable Envía un icmp de host inalcanzable.

icmp-proto-unreachable Envía un icmp de protocolo inalcanzable.

icmp-port-unreachable Envía un icmp de puerto inalcanzable.

icmp-net-prohibited Envía un icmp de red prohibida.

icmp-host-prohibited Envía un icmp de host prohibido.

tcp-reset Envía un RST de tcp.

7.3.2. Tipo de ICMP

```
1234@irouter>firewalls>firewall1>rule1$ icmp-type <value>
```

Establece el tipo de ICMP. El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado. El sistema permite seleccionar los siguientes tipos de ICMP: any, echo-reply, destination-unreachable, network-unreachable, host-unreachable, protocol-unreachable, port-unreachable, fragmentation-needed, source-route-failed, network-unknown, host-unknown, network prohibited, host-prohibited, TOS-network-unreachable, TOS-host-unreachable, comunication-prohibited, host-precedence-violation, precedence-cutoff, source-quench, redirect, network-redirect, host-redirect, TOS-network-redirect, TOS-Host-redirect, echo-request, router-advertisement, router-solicitation, time-exceeded, ttl-zero-during-transit, ttl-zero-during-reassembly, parameter-problem, ip-header-bad, required-option-missing, timestamp-request, timestamp-reply, address-mask-request y address-mask-reply.

any Establece como tipo de ICMP cualquiera.

echo-reply Establece como tipo de ICMP echo-reply. Echo Reply (Respuesta de Eco) en el protocolo ICMP suele ser un mensaje generado como contestación a un mensaje Echo Request (petición de Eco).

destination-unreachable Establece como tipo de ICMP destination-unreachable. El mensaje significa que el router considera inalcanzable el destino.

network-unreachable Establece como tipo de ICMP network-unreachable. El mensaje significa que la red actualmente es inalcanzable.

host-unreachable Establece como tipo de ICMP host-unreachable. El mensaje significa que el host es actualmente inalcanzable.

protocol-unreachable Establece como tipo de ICMP protocol-unreachable. El mensaje significa que el protocolo utilizado (tcp, udp...) es inalcanzable.

port-unreachable Establece como tipo de ICMP port-unreachable. El mensaje significa que el puerto es actualmente inalcanzable.

fragmentation-needed Establece como tipo de ICMP fragmentation-needed. El mensaje significa que el paquete necesita ser fragmentado, pero el bit de -No fragmentar- se encuentra activo.

source-route-failed Establece como tipo de ICMP source-route-failed. Ha fallado el encaminamiento exigido en origen: se ha especificado el camino/enrutado que deben seguir los paquetes y uno de los puntos de la ruta no está disponible

network-unknown Establece como tipo de ICMP network-unknown. Dirección de destino desconocida. El mensaje significa que no existe una ruta para una determinada red.

host-unknown Establece como tipo de ICMP host-unknown. Host de destino desconocido El mensaje significa que no existe una ruta para un determinado host.

network-prohibited Establece como tipo de ICMP network-prohibited. El mensaje significa que no dispone de permiso para el envío de paquetes a la red.

host-prohibited Establece como tipo de ICMP host-prohibited. El mensaje significa que no dispone de permiso para el envío de paquetes al host.

TOS-network-unreachable Establece como tipo de ICMP TOS-network-unreachable. El mensaje significa que la red fue inalcanzable debido a una mala configuración del TOS en el paquete. Los bits del campo de tipo de servicio (TOS) son un conjunto de cuatro indicadores de un bit de la cabecera de IP. Si uno de estos indicadores de bit vale 1, un encaminador puede manipular el datagrama de forma diferente del caso en el que ningún indicador valiera 1. Cada uno de los cuatro bits tiene un propósito diferente y sólo uno de los bits de TOS puede valer 1 al mismo tiempo, es decir, las combinaciones no están permitidas. Estos indicadores de bit se denominan de tipo de servicio porque permiten que la aplicación que transmite los datos informe a la red del tipo de servicio de red que requiere. Las clases de servicios de red disponibles son: Demora mínima, Rendimiento máximo, Fiabilidad máxima y Coste mínimo

TOS-host-unreachable Establece como tipo de ICMP TOS-host-unreachable. El mensaje significa que el host fue inalcanzable debido al TOS en el paquete.

communication-prohibited Establece como tipo de ICMP communication-prohibited. El mensaje significa que la comunicación se encuentra prohibida debido al filtrado (firewall).

host-precedence-violation Establece como tipo de ICMP host-precedence-violation. El mensaje significa que el valor de precedencia en el campo Tipo de servicio no está permitido.

precedence-cutoff Establece como tipo de ICMP precedence-cutoff. El mensaje significa que valor de precedencia (prioridad) es más bajo que el mínimo permitirdo en la red.

source-quench Establece como tipo de ICMP source-quench. El router realiza una petición al emisor para que reduzca la tasa de envío de paquetes.

redirect Establece como tipo de ICMP redirect. Significa que se reenvíe el paquete en una ruta alternativa . Permite enviar información sobre enrutado.

network-redirect Establece como tipo de ICMP networl-redirect. Significa que se reenvíe el paquete en una ruta alternativa para alcanzar la red..

host-redirect Establece como tipo de ICMP host-redirect. Significa que se reenvíe el paquete en una ruta alternativa par alcanzar el host..

TOS-network-redirect Establece como tipo de ICMP TOS-network-redirect. Significa que se reenvíe el paquete en una ruta alternativa para alcanzar la red y con otro TOS al establecido.

TOS-host-redirect Establece como tipo de ICMP TOS-host-redirect. Significa que se reenvíe el paquete en una ruta alternativa para alcanzar el host debido y con otro TOS al establecido.

echo-request Establece como tipo de ICMP echo-request. El Echo Request (Petición eco) es un mensaje de control que se envía a un host con la expectativa de recibir de él un Echo Reply (Respuesta eco).

router-advertisement Establece como tipo de ICMP router-advertisement. Se trata de un mensaje que avisa sobre la existencia del enrutador

router-solicitation Establece como tipo de ICMP router-solicitation. Se trata de una solicitud de existencia del enrutador

time-exceeded Establece como tipo de ICMP time-exceeded. Indica que el tiempo se ha excedido.

ttl-zero-during-transit Establece como tipo de ICMP ttl-zero-during-transit. TTL igual a 0 durante el tránsito, por lo que al paquete se le ha acabado su tiempo de vida antes de alcanzar su destino

ttl-zero-during-reassembly Establece como tipo de ICMP ttl-zero-during-reassembly. TTL igual a 0 durante el reensamblado. Si un paquete ha sido fragmentado y durante su reensamblaje el TTL llega a 0, se genera este error

parameter-problem Establece como tipo de ICMP parameter-problem. Indica que existen problemas en los parámetros.

ip-header-bad Establece como tipo de ICMP ip-header-bad. Significa que la cabecera IP se encuentra errónea.

required-option-missing Establece como tipo de ICMP required-option-missing. Faltan opciones requeridas

timestamp-request Establece como tipo de ICMP timestamp-request. Realiza una petición de la hora en origen.

timestamp-reply Establece como tipo de ICMP timestamp-reply. Se trata de la respuesta a la petición de hora

address-mask-request Establece como tipo de ICMP address-mask-request. Petición de máscara de red. Efectúa una petición para saber qué máscara de red debe utilizar

address-mask-reply Establece como tipo de ICMP address-mask-reply. Respuesta a la petición de máscara de red.

7.3.3. IP origen

```
1234@irouter>firewalls>firewall1>rule1$ source-ip address <value> mask <value>
```

Dirección IP actual

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como característica discriminatoria la dirección IP origen introducida.

Máscara origen

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como características discriminatorias la dirección IP origen y la máscara origen.

7.3.4. Puerto origen

```
1234@irouter>firewalls>firewall1>rule1$ source-port start <value> end <value>
```

Puerto inicial de origen

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como característica discriminatoria el puerto inicial de origen.

Puerto de origen final

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como característica discriminatoria el puerto de origen final.

7.3.5. IP destino

```
1234@irouter>firewalls>firewall1>rule1$ destination-ip address <value> mask
     <value>
```

Dirección IP destino

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como característica discriminatoria la dirección IP destino introducida.

Máscara destino

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como características discriminatorias la dirección IP destino y la máscara destino introducidas.

7.3.6. Puerto destino

```
1234@irouter>firewalls>firewall1>rule1$ destination-port start <value> end
     <value>
```

Puerto inicial de destino

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como característica discriminatoria el puerto inicial de destino introducido.

Puerto final de destino

Establece que el tráfico de paquetes que se verá afectado por la regla de filtrado tiene como característica discriminatoria el puerto final de destino introducido.

7.3.7. Habilitar

```
1234@irouter>firewalls>firewall1>rule1$ enable
```

Permite habilitar o deshabilitar la regla de filtrado definida.

Capítulo 8

Gestión

8.1. Configuración de Gestión

```
1234@irouter>$ management
```

Permite realizar la configuración de gestión.

8.1.1. Contraseña

```
1234@irouter>management$ password <value>
```

Define la contraseña de la gestión del router.

8.2. Configuración de Parámetros del TR069

```
1234@irouter>management$ tr69
```

Muestra los diferentes parámetros configurables relativos al estántar TR069 (Technical Report 069). Mediante este estándar se permite el mantenimiento remoto de dispositivos del usuario final.

8.2.1. URL

```
1234@irouter>management>tr69$ url <value>
```

Permite definir la URL.

8.2.2. Nombre de usuario

```
1234@irouter>management>tr69$ user <value>
```

Permite definir el nombre de usuario.

8.2.3. Contraseña

```
1234@irouter>management>tr69$ password <value>
```

Permite definir la contraseña.

8.2.4. Nombre del usuario para la conexión

```
1234@irouter>management>tr69$ connection user <value>
```

Permite definir el nombre de usuario para la conexión

8.2.5. Contraseña de conexión

```
1234@irouter>management>tr69$ connection password <value>
```

Permite definir la contraseña para la conexión.

8.2.6. Actualizaciones gestionadas

```
1234@irouter>management>tr69$ upgradesmanaged
```

Permite habilitar las actualizaciones gestionadas.

8.3. Configuración de Información periódica

```
1234@irouter>management>tr69$ periodic-inform
```

Permite configurar la información periódica.

8.3.1. Intervalo de información periódica

```
1234@irouter>management>tr69>periodic-inform$ interval <value>
```

Define el intervalo de la información periódica.

8.3.2. Referencia de hora

```
1234@irouter>management>tr69>periodic-inform$ reference <value>
```

Permite definir la referencia de hora.

8.3.3. Habilitar

```
1234@irouter>management>tr69>periodic-inform$ enable
```

Habilita la configuración de información periódica.

8.4. Configuración de STUN

```
1234@irouter>management>tr69$ stun
```

Permite la configuración del STUN.

8.4.1. Dirección del servidor STUN

```
1234@irouter>management>tr69>stun$ server-address <value>
```

Dirección del servidor STUN

8.4.2. Puerto del servidor STUN

```
1234@irouter>management>tr69>stun$ server-port <value>
```

Puerto del servidor STUN

8.4.3. Periodo mínimo del keepalive para el STUN binding

```
1234@irouter>management>tr69>stun$ minimum-keepalive-period <value>
```

Periodo mínimo del keepalive para el STUN binding (segundos).

8.4.4. Periodo máximo del keepalive para el STUN binding

```
1234@irouter>management>tr69>stun$ maximum-keepalive-period <value>
```

Periodo máximo del keepalive para el STUN binding (segundos).

8.4.5. Habilitar

```
1234@irouter>management>tr69>stun$ enable
```

Permite habilitar la configuración del STUN introducida.

Capítulo 9

Hora

9.1. Configuración de Hora

```
1234@irouter>$ time
```

Permite la configuración de la hora en función de la zona horaria local y los servidores NTP. Además permite visualizar la hora actual

9.1.1. Zona de hora local

```
1234@irouter>time$ timezone <value>
```

Permite establecer la zona horaria local. Se muestra un listado de las diferentes zonas horarias que se pueden seleccionar.

9.1.2. Primer servidor NTP

```
1234@irouter>time$ ntpserver1 <value>
```

Permite seleccionar el primer servidor NTP. Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

9.1.3. Segundo servidor NTP

```
1234@irouter>time$ ntpserver2 <value>
```

Permite seleccionar un segundo servidor NTP.

9.1.4. Habilitar

```
1234@irouter>time$ enable
```

Permite habilitar o deshabilitar la nueva configuración horaria definida.

Capítulo 10

Almacenamiento

10.1. Configuración de Almacenamiento

```
1234@irouter>$ storage
```

Permite configurar las diferentes opciones de compartición de ficheros del sistema.

10.1.1. Grupo de trabajo

```
1234@irouter>storage$ workgroup <value>
```

Define el nombre del Grupo de trabajo.

10.1.2. Habilitar servicio CIFS

```
1234@irouter>storage$ enable-cifs
```

Permite habilitar la compartición de ficheros. Se trata de una implementación del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS). Permite que el sistema se reconozca como un servidor de contenidos en redes de Windows.

10.1.3. Actualizar el contenido del USB

```
1234@irouter>storage$ scan
```

Permite actualizar el contenido de los dispositivos USB conectados al router.

10.1.4. Desmontar todos los dispositivos de almacenamiento

```
1234@irouter>storage$ umount-all
```

Permite desmontar todos los dispositivos de almacenamiento.

10.1.5. Carpetas compartidas

```
1234@irouter>storage$ share device <value> directory <value> name <value>
     permissions <value>
```

Muestra un listado de las carpetas que están siendo compartidas actualmente. Concretamente ofrece información sobre el nombre del dispositivo, la carpeta de compartición, el nombre asignado a dicho contenido y el tipo de permiso asignado al contenido. Además permite compartir nuevas carpetas.

Dispositivo

Establece el nombre del dispositivo del que se desee compartir contenidos. Si se selecciona TODOS se compartirán automáticamente todas las unidades conectadas.

Directorio

Define la ruta del directorio que se desee compartir. Si se deja vacío se compartirá la raíz del dispositivo.

Etiqueta

Define el nombre del contenido a compartir.

Permisos

Define el tipo de permiso del contenido que se encuentra compartido. Puede ser de dos tipos: solo lectura o lectura/escritura.

read-only Especifica que el sistema de ficheros es de solo lectura.

writable Especifica explícitamente que se puede escribir dentro del sistema de ficheros.

10.1.6. Usuarios de almacenamiento

```
1234@irouter>storage$ user name <value> password <value>
```

Permite definir los usuarios con acceso a los elementos compartidos. Se requiere establecer previamente los usuarios, con sus respectivas contraseñas, que podrán tener acceso a los elementos compartidos. Un aspecto importante es que si no se introduce ningún usuario, no se podrá tener acceso a los directorios compartidos.

Nombre de usuario

Define el nombre de usuario que tendrá acceso a los elementos compartidos.

Contraseña

Define la contraseña que dispondrá el usuario para acceder a los elementos compartidos.

Capítulo 11

Impresión

11.1. Configuración de Impresión

```
1234@irouter>$ printing
```

Permite observar las diferentes impresoras conectadas, ofreciendo características como el fabricante, modelo y puerto. Además permite habilitar o deshabilitar el servidor de impresora

11.1.1. Habilitar servidor de impresora

```
1234@irouter>printing$ enable
```

Permite habilitar o deshabilitar el servidor de la impresora

Capítulo 12

Servidor DNS

12.1. Configuración de Servidor DNS

```
1234@irouter>$ dns-server
```

Permite la configuración del Servidor de DNS. DNS es una abreviatura para Sistema de Nombres de Dominio (Domain Name System). Básicamente se trata de un sistema para asignar nombres a equipos y servicios de red que se organizan en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP. La mayoría de los usuarios prefieren un nombre descriptivo, fácil de utilizar, como -MiEquipo- para localizar un equipo (como un servidor Web o de correo electrónico) en la red. Un nombre descriptivo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante direcciones numéricas. Para facilitar el uso de los recursos de red, los sistemas de nombres como DNS proporcionan una forma de asignar estos nombres descriptivos de los equipos o servicios a sus direcciones numéricas. Básicamente el servicio DNS se encarga de asociar una determinada dirección URL a una dirección IP. Básicamente cuando se realice una consulta al DNS, se traducirá la dirección URL en una terminada IP, que es realmente la que permite identificar al servidor con el que se desea contactar.

12.1.1. Habilitar servidor DNS

```
1234@irouter>dns-server$ enable
```

Permite habilitar el servidor de DNS

12.1.2. Hosts DNS

```
1234@irouter>dns-server$ host name <value> address <value>
```

Tabla con información referente al DNS. Muestra las diferentes traduciones que se llevarán a cabo en el sistema.

Nombre

Define el nombre del host que se desea traducir.

Dirección

Establece la traducción que se desea asignar al nombe del host previamente introducido, es decir el nombre del host introducido se traducirá por la dirección IP ante una consulta DNS.

Capítulo 13

QoS

13.1. Configuración de QoS

```
1234@irouter>$ qos
```

Permite la configuración de la calidad del servicio QoS. El térmico Calidad del Servicio (Quality of Service QoS) hace referencia a los mecanismos de control que permiten la reserva de recursos para ciertos flujos de datos. Básicamente trata de establecer prioridades para las diferentes aplicaciones, usuarios, flujos de datos o garantizar un cierto nivel de rendimiento para un flujo de datos determinado. Existen ciertas aplicaciones que podrían requerir requisitos estrictos en cuanto a la tasa binaria, retraso, jitter, probabilidad de pérdida de paquete y/o tasa de error máxima. La QoS es especialmente importante para aplicaciones como la voz sobre IP, IP-TV... ya que frecuentemete requieren una tasa binaria fija y son muy sensibles a los retrasos. QoS permite que el tráfico como voz, vídeo y tráfico en tiempo real se puedan asignar a una cola de alta prioridad, mientras que a otros tráficos se les puede asignar una cola de prioridad inferior.

13.1.1. Cola por defecto

```
1234@irouter>qos$ default-queue <value>
```

Permite seleccionar la cola por defecto para el tráfico que no se encuentra asociado a los clasificadores previamente definidos.

13.1.2. Cola multicast por defecto

```
1234@irouter>qos$ default-multicast-queue <value>
```

Permite seleccionar la cola por defecto para el tráfico multicast que no se encuentra asociado a los clasificadores previamente definidos.

13.1.3. Habilitar

```
1234@irouter>qos$ enable
```

Habilita las colas por defecto tanto para el tráfico unicast como multicast.

13.2. Configuración de Colas

```
1234@irouter>qos$ queues
```

Permite la definición de colas con diferentes prioridades y con distintos algoritmos de planificación, concretamente se debe elegir entre Strict Priority, Weighted Fair Queuing (WFQ) Y Weighted Round Robin (WRR). Se deben tener en cuenta tres consideraciones importantes a la hora de definir nuevas colas: las colas con algoritmo de planificación Strict Priority (SP) obligatoriamente deben tener una mayor prioridad que las colas definidas con un algoritmo de planificación WFQ o WRR. La segunda consideración a tener en cuenta es que no pueden existir conjuntamente colas WFQ y WRR. El usuario deberá elegir entre utilizar colas con algoritmo de planificación WFQ o WRR. La tercera consideración es que el conjunto de colas definidas como WFQ o WRR deben tener la misma prioridad, no pudiéndose definir colas WFQ o WRR con distintas prioridades.

13.2.1. Colas

```
1234@irouter>qos>queues$ add queue priority <value> scheduler <value> name
    <value>
```

Permite añadir una nueva entrada dentro de la tabla de colas.

Prioridad

Establece la prioridad de la cola, siendo 1 la mayor prioridad.

Planificador

Establece el algoritmo de planificación. Básicamente se pueden elegir tres opciones: SP (Strict Priority), WFQ (Weighted Fair Queuing) y WRR (Weighted Round Robin).

sp Establece como algoritmo de planificación Strict Priority (SP). SP garantiza que las aplicaciones en las que el tiempo es vital se envíen por una ruta rápida. La prioridad estricta permite que los administradores de red den prioridad al tráfico donde el tiempo es vital y la tarea es crítica respecto a las aplicaciones en las que el tiempo es menos importante. Por ejemplo, en prioridad estricta, el tráfico de voz sobre IP se envía antes que el tráfico de correo electrónico (SMTP) o FTP. La cola de prioridad estricta se vacía antes de que se envíe el tráfico de las colas restantes. Básicamente mientras haya paquetes en una cola de alta prioridad, las demás colas (de menor prioridad) deben esperar. Nota: Podría existir un problema de hambruna en colas de baja proridad, al no ser atendidas en mucho tiempo.

wfq Establece como algoritmo de planificación Encolamiento Justo por Pesos (Weighted Fair Queuing WFQ). La tasa de salida es proporcional al peso asignado a cada flujo. Los paquetes son enviados en el orden de sus tiempos de finalización. Para calcular dichos tiempos WFQ tiene en cuenta el número de turno actual (refleja la cantidad de tráfico a enviar en cada cola), tiempo de finalización (información del estado del paquete) y la asignación de pesos. El paquete será enviado por el algoritmo WFQ únicamente cuando el tiempo de finalización sea menor en comparación con los tiempos calculados en las otras colas. WFQ suele dar mayor prioridad a flujos de tráfico cuyos paquetes sean más pequeños.

wrr Establece como algoritmo de planificación Weighted Round Robin (WRR). A cada flujo se le asigna un peso que corresponde a un porcentaje del ancho de banda del enlace que utilizará. El número de paquetes a enviar en cada turno se calcula con base en el peso del flujo y en la capacidad del enlace. WRR funciona bien para el envío de paquetes de tamaño fijo, pero presenta problemas de desempeño cuando los paquetes son de longitud variable, ya que en el caso de paquetes de tamaño mayor utiliza más ancho de banda del asignado, lo cual hace que el desempeño en el envío de paquetes de las otras colas disminuya.

Nombre

Establece el nombre deseado para la cola. Deberá tratarse de un nombre lo suficientemente aclarativo que permita reconocer el tráfico que está encolando.

13.3. Configuración de Cola

```
1234@irouter>qos>queues$ queue <value>
```

Permite la configuración de los diferentes parámetros de la cola seleccionada.

13.3.1. Nombre

```
1234@irouter>qos>queues>queue1$ name <value>
```

Define el nombre que deseemos asignar a la cola.

13.3.2. Interfaz

```
1234@irouter>qos>queues>queue1$ interface <value>
```

Define la interfaz de salida de la cola. Se puede seleccionar cualquier interfaz previamente definida o bien elegir las opciones WAN (toda la WAN), LAN (toda la LAN) o Any (todas las interfaces).

any Define como interfaz de salida de la cola Any

lan Define como interfaz de salida de la cola la LAN.

wan Define como interfaz de salida de la cola la WAN.

13.3.3. Prioridad

```
1234@irouter>qos>queues>queue1$ priority <value>
```

Establece la prioridad de la cola, siendo 1 la mayor prioridad.

13.3.4. Algoritmo del planificador

```
1234@irouter>qos>queues>queue1$ scheduler <value>
```

Establece el algoritmo de planificación. Básicamente se pueden elegir tres opciones: SP (Strict Priority), WFQ (Weighted Fair Queuing) y WRR (Weighted Round Robin).

sp Establece como algoritmo de planificación Strict Priority (SP).

wfq Establece como algoritmo de planificación Weighted Fair Queuing (WFQ)

wrr Establece como algoritmo de planificación Weighted Round Robin (WRR).

13.3.5. Peso

```
1234@irouter>qos>queues>queue1$ weight <value>
```

Peso de ponderación de la cola en cuestión. Solo tiene sentido para colas con algoritmo de planificación WFQ o WRR. Los valores del campo posibles son 1-255, siendo 1 el valor más bajo y 255 el valor más alto.

13.3.6. Shaping rate

```
1234@irouter>qos>queues>queue1$ rate <value>
```

Define la tasa máxima de envío de ráfaga (KB/sg). Si se introduce el valor -1 indica que no se define.

13.3.7. Etiquetado del tamaño de la ráfaga

```
1234@irouter>qos>queues>queue1$ burst-size <value>
```

Define el tamaño de la ráfaga en bytes

13.3.8. Habilitar

```
1234@irouter>qos>queues>queue1$ enable
```

Permite habilitar o deshabilitar la cola.

13.4. Configuración de Clasificaciones

```
1234@irouter>qos$ classifications
```

Permite definir las diferentes clasificaciones de paquetes necesarias en el sistema. Una clasificación es simplemente un proceso de filtrado de paquetes, donde los que cumplan una serie de requisitos se dirigirán hacia una determinada cola. Básicamente permite configurar el orden de precedencia, el nombre de la clasificación y la cola donde si dirigirá el tráfico que paquetes que se ajuste a la clasificación realizada.

13.4.1. Clasificaciones

```
1234@irouter>qos>classifications$ add classification order <value> name <value>
     class-queue <value>
```

Permite añadir una nueva clasificación dentro la tabla correspondiente.

Orden

Define la posición de la entrada de clasificación en orden de prioridad.

Nombre

Define el nombre que deseemos asignarle a la clasificación de paquetes.

Cola

Nombre de la cola donde se dirigirán los paquetes que cumplan los diferentes requerimientos impuestos en la clasificación. La cola debe definirse previamente.

13.5. Configuración de Clasificación

```
1234@irouter>qos>classifications$ classification <value>
```

Permite configurar los diferentes parámetros, que permitirán identificar el tráfico de paquetes objetivo, de la actual clasificación. Una clasificación es simplemente un proceso de filtrado de paquetes, donde los que cumplan una serie de requisitos se dirigirán hacia una determinada cola.

13.5.1. Orden

```
1234@irouter>qos>classifications>class1$ order <value>
```

Define la posición de la entrada de clasificación en orden de prioridad.

13.5.2. Interfaz

```
1234@irouter>qos>classifications>class1$ interface <value>
```

Define la interfaz de entrada asociada con el proceso de clasificación. Básicamente se trata de la fuente de paquetes que utilizará el proceso de clasificación.

any Define la interfaz Any como entrada asociada al proceso de clasificación.

lan Define la interfaz LAN como entrada asociada al proceso de clasificación.

local Define la interfaz Local como entrada asociada al proceso de clasificación.

wan Define la interfaz WAN como entrada asociada al proceso de clasificación.

13.5.3. Cola

```
1234@irouter>qos>classifications>class1$ class-queue <value>
```

Define el nombre de la cola donde se dirigen los paquetes que entran en la clasificación. La cola se debe haber creado preaviamente.

13.5.4. IP destino

```
1234@irouter>qos>classifications>class1$ destination-ip address <value> mask
     <value>
```

IP destino

Define la dirección IP destino que se empleará en el proceso de clasificación. Si la dirección IP destino del paquete coincide con la introducida, dicho paquete se dirigirá hacia la cola definida. Si el campo se encuentra vació no se utiliza para el proceso de clasificación.

Máscara de destino

Define la máscara de la IP destino que se empleará en el proceso de clasificación. Si la dirección IP destino del paquete se encuentra contenida en la máscara de la IP destino, dicho paquete se dirigirá hacia la cola definida. Si el campo se encuentra vacío se utilizará la IP destino previamente definida.

13.5.5. Excluir IP destino

```
1234@irouter>qos>classifications>class1$ exclude-destination-ip
```

Incluye o excluye en el proceso de clasificación la dirección IP destino.

13.5.6. IP origen

```
1234@irouter>qos>classifications>class1$ source-ip address <value> mask <value>
```

IP origen

Define la dirección IP origen que se empleará en el proceso de clasificación. Si la dirección IP origen del paquete coincide con la introducida, dicho paquete se dirigirá hacia la cola definida. Si el campo se encuentra vació no se utiliza para el proceso de clasificación.

Máscara origen

Define la máscara de la IP origen que se empleará en el proceso de clasificación. Si la dirección IP origen del paquete se encuentra contenida en la máscara de la IP origen, dicho paquete se dirigirá hacia la cola definida. Si el campo se encuentra vacío se utilizará la IP origen previamente definida.

13.5.7. Excluir IP origen

```
1234@irouter>qos>classifications>class1$ exclude-source-ip
```

Incluye o excluye en el proceso de clasificación la dirección IP del origen.

13.5.8. Protocolo

```
1234@irouter>qos>classifications>class1$ protocol <value>
```

Define el tipo de protocolo que se empleará como elemento diferenciador en el proceso de clasificación. Si un paquetes utiliza el mismo protocolo al introducido, dicho paquete se dirigirá hacia la cola definida. Si se introduce el valor -1 no se utiliza para el proceso de clasificación.

13.5.9. Excluir protocolo

```
1234@irouter>qos>classifications>class1$ exclude-protocol
```

Incluye o excluye en el proceso de clasificación el tipo de protocolo.

13.5.10. Puerto destino

```
1234@irouter>qos>classifications>class1$ destination-port port <value> range
     <value>
```

Puerto destino

Define el número de puerto del destino que se empleará en el proceso de clasificación. Si el paquete posee el mismo número de puerto destino que el introducido, el paquete se dirigirá hacia la cola definida. Si se introduce -1, no se utiliza para el proceso de clasificación.

Rango de puerto destino

Define el rango del puerto destino que se utilizará para el proceso de clasificación. Si el paquete posee un número de puerto destino contenido en el rango introducido, el paquete se dirigirá hacia la cola definida Si se introduce el valor -1, no se utiliza para el proceso de clasificación.

13.5.11. Excluir puerto destino

```
1234@irouter>qos>classifications>class1$ exclude-destination-port
```

Incluye o excluye en el proceso de clasificación el puerto destino.

13.5.12. Puerto origen

```
1234@irouter>qos>classifications>class1$ source-port port <value> range <value>
```

Puerto origen

Define el número de puerto del origen que se empleará en el proceso de clasificación. Si el paquete posee el mismo número de puerto origen que el introducido, el paquete se dirigirá hacia la cola definida. Si se introduce -1, no se utiliza para el proceso de clasificación.

Rango de puerto origen

Define el rango del puerto origen que se utilizará para el proceso de clasificación. Si el paquete posee un número de puerto origen contenido en el rango introducido, el paquete se dirigirá hacia la cola definida Si se introduce el valor -1, no se utiliza para el proceso de clasificación.

13.5.13. Excluir puerto origen

```
1234@irouter>qos>classifications>class1$ exclude-source-port
```

Incluye o excluye en el proceso de clasificación el puerto origen.

13.5.14. MAC origen

```
1234@irouter>qos>classifications>class1$ source-mac <value>
```

Define la dirección MAC del origen que se empleará en el proceso de clasificación. Si la dirección MAC origen del paquete coincide con la introducida, el paquete se dirigirá hacia la cola definida. Si el campo se encuentra vacío no se utiliza para el proceso de clasificación.

13.5.15. Excluir MAC origen

```
1234@irouter>qos>classifications>class1$ exclude-source-mac
```

Incluye o excluye en el proceso de clasificación la dirección MAC del origen.

13.5.16. MAC destino

```
1234@irouter>qos>classifications>class1$ destination-mac <value>
```

Define la dirección MAC del destino que se empleará en el proceso de clasificación. Si la dirección MAC destino del paquete coincide con la introducida, el paquete se dirigirá hacia la cola definida. Si el campo se encuentra vacío no se utiliza para el proceso de clasificación.

13.5.17. Excluir MAC destino

```
1234@irouter>qos>classifications>class1$ exclude-destination-mac
```

Incluye o excluye en el proceso de clasificación la dirección MAC destino.

13.5.18. DSCP

```
1234@irouter>qos>classifications>class1$ dscp <value>
```

Define el valor de DSCP que se empleará en el proceso de clasificación. Los paquetes cuyo DSCP sea igual al definido se dirigirán hacia la cola elegida. Si se introduce el valor -1 no se utiliza para el proceso de clasificación. DSCP (Differentiated Services Code Point) hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que requieren los datos que se transportan.

13.5.19. Excluir DSCP

```
1234@irouter>qos>classifications>class1$ exclude-dscp
```

Incluye o excluye en el proceso de clasificación el parámetro DSCP.

13.5.20. Marcado DSCP

```
1234@irouter>qos>classifications>class1$ mark-dscp <value>
```

Etiquetado del byte DSCP para el tráfico de paquetes que entra en esta clasificación. DSCP (de sus siglas en inglés Differentiated Services Code Point) hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan. Existen dos valores con características especiales, concretamente -1 y -2. Si se introduce el valor -1 no se modificarán los paquetes entrantes en la clasificación. El valor -2 realizará un etiquetado automático basado en el valor de prioridad Ethernet del paquete entrante en la clasificación.

13.5.21. Habilitar

```
1234@irouter>qos>classifications>class1$ enable
```

Habilita o deshabilita la clasificación definida.

Capítulo 14

DynDNS

14.1. Configuración de DynDNS

```
1234@irouter>$ dyndns
```

DynDNS (Dynamic Network Services, Inc.) es una compañía de Internet dedicada a ofrecer soluciones de DNS en direcciones IP dinámicas. Ofrece servicios gratuitos de redirección a IP de subdominios de una gran lista de nombres disponibles, ofreciendo a particulares la oportunidad de crear un servidor en Internet gratuitamente con una dirección como -nombrehost.dyndns.com-. El router incluye funciones de actualización de la IP para este servicio, por lo que, una vez configurado el router, la actualización de la IP se convierte en un proceso totalmente transparente para el usuario puesto que es el propio router el que se encarga de actualizar la IP cuando esta cambia. La utilización de este servicio requiere un proceso de registro en http://www.dyndns.com, donde se nos requerirá un nombre de usuario, una contraseña y el nombre de host que deseemos asignar a nuestro sistema.

14.1.1. Nombre de usuario

```
1234@irouter>dyndns$ username <value>
```

Define el nombre de usuario de la cuenta DynDNS. La utilización de este servicio requiere un proceso de registro en http://www.dyndns.com, donde se nos requerirá un nombre de usuario, una contraseña y el nombre de host que deseemos asignar a nuestro sistema.

14.1.2. Contraseña

```
1234@irouter>dyndns$ password <value>
```

Define la contraseña de la cuenta DynDNS.

14.1.3. Host

```
1234@irouter>dyndns$ host <value>
```

Define el nombre de host asociado a la cuenta DynDNS. Un ejemplo del mismo podría ser nombrehost.dyndns.org.

14.1.4. Habilitar DynDNS

```
1234@irouter>dyndns$ enable
```

Permite habilitar el servicio DynDNS.