Router Teldat

Interfaz Túnel IP (TNIP)

Doc. *DM519* Rev. *8.30*

Marzo, 2000

ÍNDICE

Capítulo 1
Interfaz túnel IP (TNIP)

1. Descripción

1.1. Introducción

Se denomina “Procesado Túnel” (Tunneling) al procedimiento mediante el cual paquetes de diversos protocolos son encapsulados dentro de otro protocolo. Dicha funcionalidad es implementada mediante un interfaz virtual con lo que su configuración se reduce a la de un simple interfaz que se denominara: “Interfaz Túnel”. El Interfaz Túnel no está ligado de antemano a ningún protocolo de transporte, de encapsulado e interno fijo sino que es una arquitectura que proporciona los servicios necesarios para implementar cualquier esquema estándar de encapsulación. Como los túneles son enlaces punto a punto, se deben configurar túneles independientes para cada enlace.

El “Procesado Túnel” posee tres componentes:

- Protocolo Interno, protocolo viajero o protocolo de carga (Payload Protocol): Es el protocolo que está siendo encapsulado (IP o SRT).
- Protocolo Encapsulador (Carrier Protocol): Es el protocolo que se encarga de encapsular .
  - ◊ Generic Routing Encapsulation (GRE)
- Protocolo de transporte, protocolo externo (Delivery Protocol): Es el protocolo que se encarga de transportar el protocolo interno ya encapsulado. (Sólo IP)

1.2. Ventajas del tunneling

Existen diversas situaciones en las que encapsular tráfico de un protocolo en otro es útil:

- Para interconectar redes locales multiprotocolo a través de un “backbone” con un sólo protocolo.
- Para resolver el problema de interconexión de redes que contienen protocolos con un número limitado de saltos y que sin este procedimiento no podrían llegar a conectarse.
- Para conectar dos subredes discontinuas.
- Para permitir Redes Privadas Virtuales a lo largo de redes WAN.

1.3. Consideraciones especiales

Los siguientes puntos describen consideraciones y precauciones que deben observarse a la hora de configurar túneles:

- El encapsulado y desencapsulado que se produce en los extremos del túnel son operaciones lentas.
- Hay que tener cuidado en las configuraciones y tener en cuenta los posibles problemas de seguridad y topología. Por ejemplo, se podría configurar un túnel cuyo origen y destino no estén restringidos por Firewalls.

- Hay que elegir correctamente los medios a través de los cuales irá el túnel. Podría darse el caso de que atravesara redes “Fast FDDI” y enlaces lentos de 9600 baudios. Algunos protocolos internos se comportan incorrectamente en redes compuestas de medios mixtos.
- Muchos túneles punto a punto podrían llegar a saturar un enlace con la información de encaminamiento.
- Aquellos protocolos de encaminamiento que deciden el mejor camino basándose únicamente en el número de saltos preferirán el túnel aunque exista un camino mejor sin pasar por él. El túnel siempre aparenta ser un salto aunque realmente su coste sea mayor.
- Un problema aún peor podría ocurrir si la información de encaminamiento de las redes conectadas por el túnel se llegara a mezclar con la de las redes que transportan dicha información. En esos casos, el mejor camino hacia el “destino del túnel” sería a través del túnel. A este tipo de ruta se le denomina “ruta recursiva” y provoca que el túnel se caiga temporalmente. Para impedir el problema de las rutas recursivas hay que mantener las informaciones de encaminamiento independientes;
    - ◊ Usando un número AS o TAG distinto.
    - ◊ Usando un protocolo de encaminamiento distinto.
    - ◊ Usando rutas estáticas para el primer salto (pero teniendo cuidado con los bucles de rutas).

2. Estructura de la trama encapsulada

En el caso del Túnel IP el protocolo de transporte o externo es IP por tanto la estructura de trama encapsulada sería la siguiente.

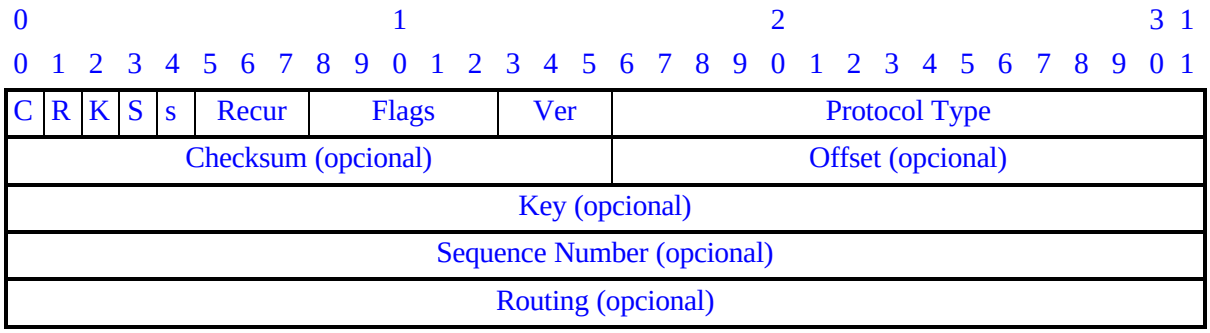
Cabecera del protocolo externo: IP
Cabecera del protocolo encapsulador
Paquete del protocolo interno

2.1. IP sobre IP con GRE

En este caso, el protocolo encargado del encapsulado es GRE. Y el protocolo interno o protocolo que está siendo encapsulado es IP. El protocolo de encapsulado GRE (Generic Routing Encapsulation) está descrito en la RFC1701 y el caso particular de IP sobre IP con GRE en la RFC1702.

Cabecera del protocolo externo: IP
Cabecera del protocolo encapsulador: GRE
Protocolo interno: IP

La cabecera IP está fuera de los límites de este documento, no así la cabecera GRE. La cabecera GRE posee la forma:



Checksum Present (bit 0) (C)

Si está puesto a 1, entonces el campo Checksum está presente y contiene información válida. Si el bit de Checksum o de Routing está presente tanto el campo offset como el campo Checksum estarán presentes en el paquete.

Routing Present (bit 1) (R)

No usado.

Key Present (bit 2)

Si está a 1, entonces el campo key (o identificador) está presente en el paquete y tiene valor válido.

Sequence Number Present (bit 3)

Si está a 1, entonces el campo Número de Secuencia (Sequence Number) está presente y contiene un valor válido.

Strict Source Route Present (bit 4)

No usado.

Recursion Control (bits 5-7)

Contiene un entero positivo de 3 bits que indica el número de encapsulaciones adicionales que están permitidas. Siempre 0.

Número de versión (bits 13-15)

Siempre 0.

Tipo de protocolo (2 octetos)

Contiene el tipo de protocolo del paquete interno.

Offset (2 octetos)

Indica el desplazamiento en octetos desde el inicio del campo Routing hasta la primera ruta que debe ser examinada.

Checksum (2 octetos)

Contiene el checksum IP de la cabecera GRE y el paquete interno.

Key (4 octetos)

Identificador del túnel.

Número de secuencia (4 octetos)

Número usado por el receptor para asegurar el correcto orden de llegada de los paquetes.

Routing (longitud variable)

No existirá.

Cuando IP se encapsula en IP usando GRE el TOS y las opciones de seguridad IP son copiadas de la cabecera del protocolo interno (payload protocol) en la cabecera del protocolo externo (delivery protocol). EL TTL sin embargo no se copia sino que se establece al valor por defecto usado para IP con el fin de evitar que los paquetes RIP que viajen a través del túnel expiren antes de llegar al destino.

2.2. Adaptación IP sobre IP Internet

Para más información acerca de la adaptación IP sobre IP Internet ver el capítulo 6.

2.3. IP sobre SRT con GRE

De nuevo el protocolo encargado del encapsulado es GRE. En este caso el protocolo interno o protocolo que está siendo encapsulado es SRT.

Los campos de la cabecera GRE se rellenan e interpretan de la misma manera.

El TTL, TOS y las opciones de seguridad en la cabecera del protocolo externo (delivery protocol) son las usadas por defecto en IP.

3. Referencias

RFC-1701: Generic Routing Encapsulation (GRE), S. Hanks, Octubre-1994
RFC-1702: Generic Routing Encapsulation over IPv4 networks, S. Hanks, Octubre-1994

Capítulo 2
Configuración del Interfaz túnel IP (TNIP)

1. Creación del Interfaz túnel IP (TNIP)

Para crear un interfaz de tipo Túnel IP se debe introducir:

```
Config>ADD DEVICE TNIP
Added TNIP interface with num: 2

TNIP tunnel encapsulated type:[GRE]?
Config>
```

Para entrar posteriormente en configuración basta con teclear:

```
Config>NETWORK 2
```

El protocolo que es soportado sobre el interfaz TNIP es el IP. Es necesario para activar el IP sobre el interfaz TNIP asignar una dirección IP al citado interfaz o configurarlo como interfaz de tipo no numerado. Para ello es necesario entrar en configuración del protocolo IP y asignar una dirección al citado interfaz o configurarlo como no numerado.

Ejemplo con dirección IP conocida:

```
*P 4
Config>PROTOCOL IP
Internet protocol user configuration
Conf IP>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 5.5.5.1
Address mask[255.0.0.0]? 255.255.255.0
Conf IP>LIST ADDRESS
IP addresses for each interface:
...
intf  2   5.5.5.1      255.255.255.0    NETWORK broadcast,    fill 0
...
Conf IP>EXIT
```

Ejemplo como interfaz no numerado:

```
*P 4
Config>PROTOCOL IP
Internet protocol user configuration
Conf IP>ADD ADDRESS
Which net is this address for [0]? 2
New address[0.0.0.0]? 0.0.0.2
Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0   ...           IP disabled on this interface
   intf  1   ...           IP disabled on this interface
   intf  2   0.0.0.2       255.255.255.0 NETWORK broadcast, fill 0
Conf IP>EXIT
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
```

2. Configuración del interfaz Túnel IP (TNIP)

En este apartado se describen los comandos de configuración del interfaz TNIP. Para acceder al entorno de configuración de TNIP, se deben introducir los siguientes comandos:

```
Config>NETWORK 2

-- IP Tunnel Net Config --
TNIP config>
```

Comando	Función
? (AYUDA)	Lista los comandos u opciones disponibles.
SET	Configura el tipo de túnel, origen y destino del mismo.
ENABLE	Habilita el túnel o alguna de las opciones que afectan a su funcionamiento.
DISABLE	Deshabilita el túnel o alguna de la opciones del mismo.
LIST	Muestra la configuración actual del túnel IP.
EXIT	Sale del proceso de configuración de TNIP.

Las letras en **negrita** son el número mínimo de caracteres que hay que teclear para que el comando sea efectivo.

2.1. ? (AYUDA)

Utilizar el comando **?** (AYUDA) para listar los comandos disponibles en el prompt en el que se esté trabajando. También se puede usar este comando a continuación de un comando específico para listar opciones disponibles.

Sintaxis:

```
TNIP config>?
```

Ejemplo:

```
TNIP config>?
SET
ENABLE
DISABLE
LIST
EXIT
TNIP config>
```

2.2. SET

Se utiliza para configurar el origen y el destino de túnel, y para entrar en la configuración del protocolo de encapsulado usado.

Sintaxis:

```
TNIP config>SET ?
PROTOCOL
SOURCE
DESTINATION
```

a) SET PROTOCOL

Sirve para entrar en la configuración del protocolo de encapsulado. Por defecto es GRE ya que actualmente es el único que se soporta

Ejemplo:

```
TNIP config>SET PROTOCOL

-- GRE Config --
GRE config>
```

El interfaz TNIP soportará varios tipos de encapsulado. Mediante este comando se especificará el tipo de encaspulado a usar.

b) SET SOURCE

Mediante este comando se configura la dirección IP del origen del túnel IP. Debe coincidir con la dirección IP de uno de los interfaces configurados en el router excepto la del propio túnel (Ethernet, FRAME RELAY, interno, etc.) y con la dirección IP configurada como destino en el equipo que sea el otro extremo del túnel.

Si la dirección IP origen no coincide con ninguno de los interfaces del router los paquetes destinados a esta dirección IP no serán tomados por el router como propios y los intentará encaminar hacia otro equipo.

Si la dirección IP configurada como origen no coincide con la configurada como destino en el otro extremo del router, no existirá nunca enlace.

Ejemplo:

```
TNIP config>SET SOURCE
Tunnel Source address  [0.0.0.0]?1.1.6.1
TNIP config>
```

c) SET DESTINATION

Mediante este comando se configura la dirección IP del destino del túnel IP. Debe coincidir con la dirección IP configurada como origen en el router del otro extremo.

Si la dirección IP destino no coincide con la configurada como origen en el otro extremo del router, los paquete que se envíen a dicho router serán descartados por no pertenecer al túnel.

Es necesario que exista ruta hacia dicho destino pues si no los paquetes del túnel no podrán ser encaminados. Como precaución dicha ruta debe ser una ruta estática para evitar el problema de recursividad en la tabla de rutas explicado en el capítulo 1.

Ejemplo:

```
TNIP config>SET DESTINATION
Tunnel destination address  [0.0.0.0]?2.2.6.1
TNIP config>
```

2.3. ENABLE

Se utiliza para habilitar el túnel.

Sintaxis:

```
TNIP config>ENABLE ?
TUNNEL
```

a) ENABLE TUNNEL

Por defecto, el interfaz túnel no está activo. Para activarlo en configuración se usa dicho comando.

Ejemplo:

```
TNIP config>ENABLE TUNNEL
TNIP config>
```

2.4. DISABLE

Se utiliza para deshabilitar el túnel.

Sintaxis:

```
TNIP config>DISABLE ?
TUNNEL
```

a) DISABLE TUNNEL

Por defecto, el interfaz túnel no está activo. Para desactivarlo en configuración se usa dicho comando.

Ejemplo:

```
TNIP config>DISABLE TUNNEL
TNIP config>
```

2.5. LIST

Se utiliza para listar la configuración del túnel.

Sintaxis:

```
TNIP config>LIST ?
STATE
TUNNEL_MODE
ADDRESSES
ALL
```

a) LIST STATE

Muestra el estado configurado del túnel. Los posibles estados son habilitado o deshabilitado.

Ejemplo:

```
TNIP config>LIST STATE
Tunneling IP:   enable
TNIP config>
```

b) LIST TUNNEL MODE

Mediante este comando se muestra el tipo de encapsulado usado. Por ahora sólo se soporta GRE.

Ejemplo:

```
TNIP config>LIST TUNNEL_MODE
Tunnel Mode: GRE
TNIP config>
```

c) LIST ADDRESSES

Mediante este comando se muestra la dirección IP origen y destino del túnel.

Ejemplo:

```
TNIP config>LIST ADDRESSES
Tunnel Addresses
Source:  1.1.6.1
Destination: 2.2.6.1
TNIP config>
```

d) LIST ALL

Mediante este comando se muestra el estado configurado del túnel, el tipo de encapsulado usado, y las direcciones IP origen y destino del túnel.

Ejemplo:

```
TNIP config>LIST ALL
Tunnel Mode: GRE
Tunnel Addresses
Source:  1.1.6.1
Destination: 2.2.6.1
Tunneling IP:   enabled
TNIP config>
```

2.6. EXIT

Utilizar el comando **EXIT** para volver al nivel prompt en el que se estaba anteriormente.

Sintaxis:

```
TNIP config>EXIT
```

Ejemplo:

```
TNIP config>EXIT
Config>
```

3. Configuración del protocolo de encapsulado GRE

En este apartado se describen los comandos de configuración del protocolo de encapsulado. Como se ha comentado anteriormente por el momento sólo se soporta GRE por lo que este apartado corresponde a la configuración del protocolo GRE. Para acceder al entorno de configuración de GRE, como vimos en el apartado 2.2.a "SET PROTOCOL" se deben introducir los siguientes comandos:

```
Config>NETWORK 2

-- IP Tunnel Net Config --
TNIP config>SET PROTOCOL

-- GRE Config --
GRE config>
```

Comando	Función
? (AYUDA)	Lista los comandos u opciones disponibles.
SET	Configura el cifrado.
ENABLE	Habilita alguna de las opciones que permite el protocolo de encapsulado y que afectan al funcionamiento del túnel.
DISABLE	Deshabilita alguna de la opciones.
LIST	Muestra la configuración actual.
EXIT	Sale del proceso de configuración de GRE.

Las letras en **negrita** son el número mínimo de caracteres que hay que teclear para que el comando sea efectivo.

3.1. ? (AYUDA)

Utilizar el comando **? (AYUDA)** para listar los comandos disponibles en el prompt en el que se esté trabajando. También se puede usar este comando a continuación de un comando específico para listar opciones disponibles.

Sintaxis:

```
GRE config>?
```

Ejemplo:

```
GRE config>?
SET
ENABLE
DISABLE
LIST
EXIT
GRE config>
```

3.2. SET

Se utiliza para configurar el protocolo de encapsulado GRE.

Sintaxis:

```
GRE config>SET ?
CIPHER KEY
```

a) SET CIPHER KEY

El protocolo GRE soporta la posibilidad de cifrar los datos mediante el protocolo RC4. Mediante este comando se configura la clave de sesión del interfaz túnel. Dicha clave admite un máximo de 32 caracteres alfanuméricos. En caso de habilitar cifrado y no configurar explícitamente la clave, se utiliza una clave por defecto.

Ejemplo:

```
GRE config>SET  CIPHER KEY
Cipher key :        ****************
Rewrite key:        ****************
New cipher key set
GRE config>
```

3.3. ENABLE

Se utiliza para habilitar las opciones que permite el protocolo GRE y que rigen el funcionamiento del túnel.

Sintaxis:

```
TNIP config>ENABLE ?
CHECKSUM
CIPHER
KEY
PROP_SEQ
SEQUENCE
```

a) ENABLE CHECKSUM

Se utiliza para habilitar la opción de envío de checksum. Por defecto, el túnel no garantiza la integridad de los paquetes. Habilitando dicha opción el router envía los paquetes con campo checksum. Si llega un paquete con checksum el equipo siempre comprueba el checksum descartando aquellos paquetes que lo tengan inválido, aunque el equipo tenga deshabilitada la opción.

Ejemplo:

```
GRE config>ENABLE CHECKSUM
GRE config>
```

b) ENABLE CIPHER

El protocolo GRE soporta la posibilidad de cifrar los datos mediante el protocolo RC4. Mediante este comando se activa el cifrado de este interfaz túnel.

Ejemplo:

```
GRE config>ENABLE CIPHER
 GRE config>
```

c) ENABLE KEY

Se utiliza para habilitar la opción de comprobación del identificador del túnel. Al habilitarse dicha opción el equipo solicita un identificador para el túnel en cuestión. Dicho identificador de túnel ha de ser igual en ambos extremos del túnel. Por defecto, el túnel tiene deshabilitada la opción.

Habilitando dicha opción el router descarta aquellos paquetes que posean un identificador distinto al configurado.

Ejemplo:

```
GRE config>ENABLE KEY
Tunnel key : [0]?12345
GRE config>
```

d) ENABLE PROPIETARY SEQUENCE

Se utiliza para habilitar el uso de número de secuencia propietario. Al habilitar esta opción, en caso de desincronización de los extremos del túnel (se reciben paquetes con número de secuencia menor al esperado), el reenganche es más rápido ya que incluye el número de secuencia esperado por parte del otro extremo del túnel. Por defecto el túnel tiene deshabilitada esta opción. Se recomienda su uso cuando los extremos del túnel sean Routers Teldat.

Ejemplo:

```
GRE config>ENABLE PROP_SEQ
GRE config>
```

e) ENABLE SEQUENCE

Se utiliza para habilitar la opción de asegurar orden en datagramas entrantes. Por defecto, el túnel tiene deshabilitada la opción.

Habilitando dicha opción el router descarta aquellos paquetes que lleguen fuera de orden.

Ejemplo:

```
GRE config>ENABLE SEQUENCE
GRE config>
```

3.4. DISABLE

Se utiliza para deshabilitar las opciones que permite el protocolo GRE y que rigen el funcionamiento del túnel.

Sintaxis:

```
TNIP config>DISABLE ?
CHECKSUM
CIPHER
KEY
PROP_SEQ
SEQUENCE
```

a) DISABLE CHECKSUM

Se utiliza para deshabilitar la opción de envío de checksum. Por defecto, el túnel no garantiza la integridad de los paquetes. Deshabilitando dicha opción el router envía los paquetes sin campo checksum. Si llega un paquete con checksum el equipo siempre comprueba el checksum descartando aquellos paquetes que lo tengan inválido.

Ejemplo:

```
GRE config>DISABLE CHECKSUM
GRE config>
```

b) DISABLE CIPHER

El protocolo GRE soporta la posibilidad de cifrar los datos mediante el protocolo RC4. Mediante este comando se desactiva el cifrado de este interfaz túnel

Ejemplo:

```
GRE config>DISABLE CIPHER
GRE config>
```

c) DISABLE KEY

Se utiliza para deshabilitar la opción de comprobación del identificador del túnel. Por defecto, el túnel tiene deshabilitada la opción.

Deshabilitando dicha opción el router descarta aquellos paquetes que posean un identificador.

Ejemplo:

```
GRE config>DISABLE  KEY
GRE config>
```

d) DISABLE PROPIETARY SEQUENCE

Se utiliza para deshabilitar el uso de número de secuencia propietario Por defecto, el túnel tiene deshabilitada la opción.

Ejemplo:

```
GRE config>DISABLE PROP_SEQ
GRE config>
```

e) DISABLE SEQUENCE

Se utiliza para deshabilitar la opción de asegurar orden en datagramas entrantes. Por defecto, el túnel tiene deshabilitada la opción.

Deshabilitando dicha opción el router no descarta aquellos paquetes que lleguen fuera de orden.

Ejemplo:

```
GRE config>DISABLE SEQUENCE
GRE config>
```

3.5. LIST

Se utiliza para listar la configuración del protocolo GRE para el interfaz TNIP.

Sintaxis:

```
TNIP config>LIST ?
STATE
OPTIONS
ALL
```

a) LIST STATE

Muestra el estado configurado del cifrado. Los posibles estados son habilitado o deshabilitado.

Ejemplo:

```
GRE config>LIST STATE
Cipher:         enable
GRE config>
```

b) LIST OPTIONS

Muestra el estado (habilitado/deshabilitado) de las opciones que rigen el funcionamiento del túnel.

Ejemplo:

```
GRE config>LIST OPTIONS
GRE Options GRE
End-to-End Checksumming:     disabled
Tunnel identification key:   enabled
--------------------> key:   12345
Drop Out-of-Order Datagrams: disabled
Proprietary sequence number: disabled
GRE config>
```

c) LIST ALL

Muestra el estado configurado del cifrado y el estado de las opciones que rigen el funcionamiento del túnel.

Ejemplo:

```
GRE config>LIST ALL
Cipher:         enable
GRE Options GRE
End-to-End Checksumming:     disabled
Tunnel identification key:   enabled
--------------------> key:   12345
Drop Out-of-Order Datagrams: disabled
Proprietary sequence number: disabled
GRE config>
```

3.6. EXIT

Utilizar el comando **EXIT** para volver al nivel prompt en el que se estaba anteriormente.

Sintaxis:

```
GRE config>EXIT ?
```

Ejemplo:

```
GRE config>EXIT
TNP Config>
```

Capítulo 3
Monitorización del Interfaz túnel IP (TNIP)

1. Estadísticos del interfaz Túnel IP (TNIP)

1.1. Introducción

- Visualización del prompt de monitorización del interfaz Túnel IP: corresponde a la parte de túneles dinámicos por lo que se verá en el apartado 6.1 del capítulo 6 “Túneles Dinámicos (Internet)”.

- Comandos de monitorización del interfaz Túnel IP: corresponde a la parte de túneles dinámicos por lo que se verá en el apartado 6.2 del capítulo 6 “Túneles Dinámicos (Internet)”.

1.2. Interfaces TNIP y el comando DEVICE del proceso MONITOR

Al ejecutar el comando **DEVICE** desde el prompt del proceso MONITOR (+) se mostrarán todos los estadísticos del interfaz TNIP:

```
+DEVICE 2
Auto-test   Auto-test     Maintenance
Ifc  Interface     CSR    Vect      valids    failures        failures
2    TNIP/0          0       0           2           0               0
Input Stats
-----------
  Frames ok    0
  Frames error 0
  ---> Invalid encapsulated     0
  ---> Out-of-Order frames      0
  ---> Checksum errors          0
  ---> Key errors               0
  ---> Unknown payload protocol 0
  ---> Error in cipher          0
  ---> Internal errors          0
Output Stats
------------
  Frames ok    0
  Frames error 0
  ---> Invalid encapsulation    0
  ---> Unknow internal protocol 0
+
```

Capítulo 4
Ejemplos de configuración de Túnel IP

1. Pasos a seguir. Túnel IP sobre IP

1.1. Pasos a seguir en cada extremo del túnel

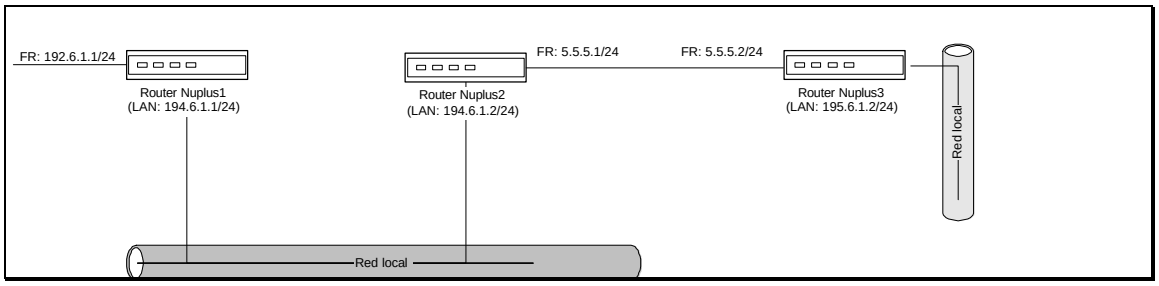
- Crear el interfaz túnel IP, guardar y reiniciar.
- Asignar una dirección IP al interfaz túnel o configurarlo como no numerado.
- Configurar el origen del túnel, que será una dirección IP de un interfaz existente en el equipo excepto la propia del túnel.
- Configurar el destino del túnel. Agregar la ruta IP necesaria para llegar a dicho destino.
- Configurar el protocolo de encapsulado que irá en el túnel (o tipo de túnel).
- Habilitar las opciones deseadas (checksum, número de secuencia o/y identificador).
- Agregar las rutas IP de aquellas redes que tengan que ser accesibles a través del túnel IP poniendo como siguiente salto la dirección del interfaz del túnel del otro extremo (en caso de que no se haya configurado como no numerado) o el interfaz de túnel (en caso de que se haya configurado como no numerado.
- Habilitar el túnel, guardar y reiniciar.

1.2. Pasos a seguir en los equipos que atraviesa el túnel

- Agregar las rutas necesarias para que origen y destino del túnel sean accesibles.

1.3. Ejemplo 1: IP sobre IP con GRE

Configuración de un túnel con origen Nuplus1 y destino Nuplus3, en el que se puedan comunicar las redes 193.6.1.0/24 y 195.6.1.0/24.



a) Configuración Nuplus1

Agregamos el interfaz Frame Relay y el túnel IP

```
*P 4
Config>SET HOSTNAME
What is the new router name?[]?Nuplus1
Config>LIST DEVICE

Con    Ifc Type of interface                    CSR     CSR2  int
---      1 Router->Node                           0             0
---      2 Node->Router                           0             0
LAN      0 Ethernet                         9000000            1C
WAN1     3 X25                              F001600  F000C00   9E
WAN2     4 X25                              F001620  F000D00   9D
ISDN 1   5 channel D: X.25                  A000000            1B
ISDN 1   7 channel B: X.25                  F001640  F000E00   9C
ISDN 2   6 channel D: X.25                  A200000            1B
ISDN 2   8 channel B: X.25                  F001660  F000F00   9B
Config>SET DATA FR
which port will be changed[1]?
Config>ADD DEVICE TNIP
Added TNIP interface with num: 2

TNIP tunnel encapsulated type:[GRE]?
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuramos las direcciones de los interfaces

```
Nuplus1 *P 4
Nuplus1 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus1 Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0                                  IP disabled on this interface
   intf  1                                  IP disabled on this interface
   intf  2                                  IP disabled on this interface
   intf  3                                  IP disabled on this interface
Nuplus1 Conf IP>ADD ADDRESS
Which net is this address for[0]?
New address [0.0.0.0]? 194.6.1.1
Address mask [255.255.255.0]? 255.255.255.0
Nuplus1 Conf IP>ADD ADDRESS
Which net is this address for[0]? 1
New address[0.0.0.0]? 193.6.1.1
Address mask [255.255.255.0]? 255.255.255.0
Nuplus1 Conf IP>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 0.0.0.2
Nuplus1 Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0   194.6.1.1        255.255.255.0    NETWORK broadcast,    fill 0
   intf  1   193.6.1.1        255.255.255.0    NETWORK broadcast,    fill 0
   intf  2   0.0.0.2          0.0.0.0          NETWORK broadcast,    fill 0
   intf  3                                    IP disabled on this interface
Nuplus1 Conf IP>EXIT
```

A continuación configuramos el túnel

```
Nuplus1 Config>NETWORK 2

-- IP Tunnel Net Config --
Nuplus1 TNIP config>LIST ALL
Tunnel Mode: GRE
Tunnel Addresses
Source:      0.0.0.0
Destination: 0.0.0.0
Tunneling IP:   disabled
TNIP config>
Nuplus1 TNIP config>SET SOURCE

Tunnel Source address [0.0.0.0]? 194.6.1.1
Nuplus1 TNIP config>SET DESTINATION

Tunnel Destination address [0.0.0.0]? 5.5.5.2
Nuplus1 TNIP config>ENABLE TUNNEL
Nuplus1 TNIP config>SET PROTOCOL

-- GRE Config --
Nuplus1 GRE config>LIST ALL
Cipher:         disabled
GRE Options GRE
End-to-End Checksumming:      disabled
Tunnel identification key:    disabled
Drop Out-of-Order Datagrams:  disabled
Proprietary sequence number:  disabled
Nuplus1 GRE config>
Nuplus1 GRE config>ENABLE CHECKSUM
Nuplus1 GRE config>ENABLE KEY

Tunnel key: [0]? 1234
Nuplus1 GRE config>ENABLE SEQUENCE
Nuplus1 GRE config>EXIT
Nuplus1 TNIP config>EXIT
```

Agregamos las rutas necesarias

```
Nuplus1 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus1 Conf IP>LIST ROUTE

Nuplus1 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 5.5.5.2
Address mask [0.0.0.0]? 255.255.255.255
Via gateway at [0.0.0.0]? 194.6.1.2
Cost[1]?
Nuplus1 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 195.6.1.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 0.0.0.2
Cost[1]?
Nuplus1 Conf IP>EXIT
Nuplus1 Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Nuplus1 Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

```
Nuplus1 *P 3
Console Operator
Nuplus1 +PROTOCOL IP
Nuplus1 IP>INTERFACE
Interface  IP Address(es)        Mask(s)
   Eth/0     194.6.1.1         255.255.255.0
    FR/0     193.6.1.1         255.255.255.0
  TNIP/0     0.0.0.0           0.0.0.0
Nuplus1 IP>DUMP
Type   Dest net           Mask   Cost  Age  Next hop(s)

 Est*  5.5.5.2          FFFFFFFF  1     0    194.6.1.2
 Dir*  193.6.1.0        FFFFFF00  1     0    FR/0
 Dir*  194.6.1.0        FFFFFF00  1     0    Eth/0
 Est*  195.6.1.0        FFFFFF00  1     0    TNIP/0

Routing table size: 768 nets (49152 bytes), 4 nets known
Nuplus1 IP>
```

b) Configuración Nuplus2

Agregamos el interfaz Frame Relay

```
*P 4
Config>SET HOSTNAME
What is the new router name?[]?Nuplus2
Config>SET DATA FR
which port will be changed[1]?
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuramos el interfaz Frame Relay

```
nuplus2 *P 4
nuplus2 Config>NETWORK 1

-- Frame Relay user configuration --
nuplus2 FR config>DISABLE LMI
nuplus2 FR config>SET FRAME-SIZE
Interface MTU in bytes [2048]? 1500
nuplus2 FR config>ADD PVC
Circuit number[16]?
Committed Information Rate (CIR) in bps[16000]? 64000
Committed Burst Size (Bc) in bits[16000]?
Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)?
Assign circuit name[]?
nuplus2 FR config>ADD PROTOCOL-ADDRESS
IP Address [0.0.0.0]? 5.5.5.2
Circuit number[16]?
nuplus2 FR config>EXIT
```

Configuramos las direcciones de los interfaces

```
nuplus2 Config>PROTOCOL IP
Internet protocol user configuration
nuplus2 Conf IP>ADD ADDRESS
Which net is this address for[0]?
New address [0.0.0.0]? 194.6.1.2
Address mask [255.255.255.0]? 255.255.255.0
nuplus2 Conf IP>ADD ADDRESS
Which net is this address for[0]? 1
New address [0.0.0.0]? 5.5.5.1
Address mask [255.255.255.0]? 255.255.255.0
nuplus2 Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0   194.6.1.2        255.255.255.0    NETWORK broadcast,    fill 0
   intf  1   5.5.5.1          255.255.255.0    NETWORK broadcast,    fill 0
   intf  2                                     IP disabled on this interface
nuplus2 Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

```
nuplus2 *P 3
Console Operator
nuplus2 +PROTOCOL IP
nuplus2 IP>INTERFACE
Interface  IP Address(es)        Mask(s)
  Eth/0     194.6.1.2        255.255.255.0
   FR/0     5.5.5.1          255.255.255.0
nuplus2 IP>
```

c) Configuración Nuplus3

Agregamos el interfaz Frame Relay y el túnel IP

```
*P 4
Config>SET HOSTNAME
What is the new router name?[]?Nuplus3
Config>SET DATA FR
which port will be changed[1]?
Config>ADD DEVICE TNIP
Added TNIP interface with num: 2

TNIP tunnel encapsulated type:[GRE]?
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuramos las direcciones de los interfaces

```
Nuplus3 *P 4
Nuplus3 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus1 Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0                                  IP disabled on this interface
   intf  1                                  IP disabled on this interface
   intf  2                                  IP disabled on this interface
   intf  3                                  IP disabled on this interface
Nuplus3 Conf IP>ADD ADDRESS
Which net is this address for[0]?
New address [0.0.0.0]? 195.6.1.1
Address mask [255.255.255.0]? 255.255.255.0
Nuplus3 Conf IP>ADD ADDRESS
Which net is this address for[0]? 1
New address[0.0.0.0]? 5.5.5.2
Address mask [255.255.255.0]? 255.255.255.0
Nuplus3 Conf IP>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 0.0.0.2
Nuplus3 Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0   195.6.1.1        255.255.255.0    NETWORK broadcast,    fill 0
   intf  1   5.5.5.2          255.255.255.0    NETWORK broadcast,    fill 0
   intf  2   0.0.0.2          0.0.0.0          NETWORK broadcast,    fill 0
   intf  3                                     IP disabled on this interface
Nuplus3 Conf IP>EXIT
```

Configuramos el interfaz Frame Relay

```
Nuplus3 *P 4
Nuplus3 Config>NETWORK 1

-- Frame Relay user configuration --
Nuplus3 FR config>DISABLE LMI
Nuplus3 FR config>SET FRAME-SIZE
Interface MTU in bytes [2048]? 1500
Nuplus3 FR config>ADD PVC
Circuit number[16]?
Committed Information Rate (CIR) in bps[16000]? 64000
Committed Burst Size (Bc) in bits[16000]?
Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)?
Assign circuit name[]?
Nuplus3 FR config>ADD PROTOCOL-ADDRESS
IP Address [0.0.0.0]? 5.5.5.1
Circuit number[16]?
Nuplus3 FR config>EXIT
```

A continuación configuramos el túnel

```
Nuplus3 Config>NETWORK 2

-- IP Tunnel Net Config --
Nuplus3 TNIP config>SET SOURCE

Tunnel Source address [0.0.0.0]? 5.5.5.2
Nuplus3 TNIP config>SET DESTINATION

Tunnel Destination address [0.0.0.0]? 194.6.1.1
Nuplus3 TNIP config>ENABLE TUNNEL
Nuplus3 TNIP config>SET PROTOCOL

-- GRE Config --
Nuplus3 GRE config>ENABLE CHECKSUM
Nuplus3 GRE config>ENABLE KEY

Tunnel key: [0]? 1234
Nuplus3 GRE config>ENABLE SEQUENCE
Nuplus3 GRE config>EXIT
Nuplus3 TNIP config>EXIT
```

Agregamos las rutas necesarias

```
Nuplus3 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus3 Conf IP>LIST ROUTE

Nuplus3 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 194.6.1.1
Address mask [0.0.0.0]? 255.255.255.255
Via gateway at [0.0.0.0]? 5.5.5.1
Cost[1]?
Nuplus3 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 193.6.1.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 0.0.0.2
Cost[1]?
Nuplus3 Conf IP>EXIT
Nuplus3 Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Nuplus3 Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

```
Nuplus3 *P 3
Console Operator
Nuplus3 +PROTOCOL IP
Nuplus3 IP>INTERFACE
Interface  IP Address(es)        Mask(s)
   Eth/0     195.6.1.1        255.255.255.0
    FR/0     5.5.5.2          255.255.255.0
  TNIP/0     0.0.0.0          0.0.0.0
Nuplus3 IP>DUMP
Type   Dest net           Mask  Cost  Age  Next hop(s)

 Dir*  5.5.5.0          FFFFFF00  1    0    FR/0
 Est*  193.6.1.0        FFFFFFFF  1    0    TNIP/0
 Est*  194.6.1.1        FFFFFFFF  1    0    5.5.5.1
 Dir*  195.6.1.0        FFFFFF00  1    0    Eth/0

Routing table size: 768 nets (49152 bytes), 4 nets known
Nuplus3 IP>
```

2. Pasos a seguir. Túnel IP sobre SRT

2.1. Pasos a seguir en cada extremo del túnel

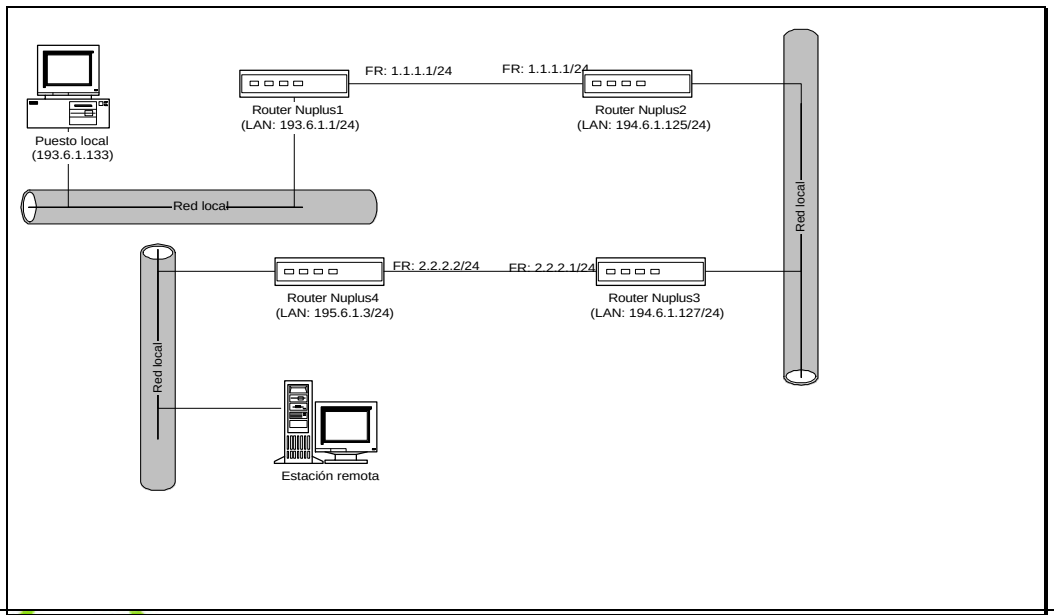
- Crear el interfaz túnel ip, guardar y reiniciar.
- Habilitar el bridge.
- Agregar un puerto en el bridge para el interfaz del túnel.
- Configurar el origen del túnel, que será una dirección IP de un interfaz existente en el equipo excepto la propia del túnel.
- Configurar el destino del túnel. Agregar la ruta IP necesaria para llegar a dicho destino.
- Configurar el protocolo de encapsulado que irá en el túnel (o tipo de túnel).
- Habilitar las opciones deseadas (checksum, número de secuencia o/y identificador).
- Habilitar el túnel, guardar y reiniciar.

2.2. Pasos a seguir en los equipos que atraviesa el túnel

- Agregar las rutas necesarias para que origen y destino del túnel sean accesibles.

2.3. Ejemplo: IP sobre SRT con GRE

Configuración de un túnel con origen Nuplus1 y destino Nuplus4, en el que se puedan comunicar las redes 193.6.1.0/24 y 195.6.1.0/24 mediante tráfico NetBEUI. Para ello estableceremos un túnel IP sobre SRT entre ambas.



a) Configuración Nuplus1

Al igual que en el ejemplo anterior, se añade el interfaz FR y el interfaz túnel IP (TNIP)

```
*P 4
Config>SET HOSTNAME
What is the new router name?[]?Nuplus1
Config>SET DATA FR
which port will be changed[1]?
Config>ADD DEVICE TNIP
Added TNIP interface with num: 2

TNIP tunnel encapsulated type:[GRE]?
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuramos las direcciones de los interfaces

```
Nuplus1 *P 4
Nuplus1 Config>PROTOCOL IP
Internet protocol user configuration
Which net is this address for[0]?
New address [0.0.0.0]? 193.6.1.133
Address mask [255.255.255.0]? 255.255.255.0
Nuplus1 Conf IP>ADD ADDRESS
Which net is this address for[0]? 1
New address[0.0.0.0]? 1.1.1.1
Address mask [255.255.255.0]? 255.255.255.0
Nuplus1 Conf IP>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 0.0.0.2
Nuplus1 Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0   193.6.1.133      255.255.255.0    NETWORK broadcast,    fill 0
   intf  1   1.1.1.1          255.255.255.0    NETWORK broadcast,    fill 0
   intf  2   0.0.0.2          0.0.0.0          NETWORK broadcast,    fill 0
   intf  3                                     IP disabled on this interface
Nuplus1 Conf IP>ex
```

A continuación configuramos el túnel

```
Nuplus1 Config>NETWORK 2

-- IP Tunnel Net Config --
Nuplus1 TNIP config>SET SOURCE

Tunnel Source address [0.0.0.0]? 1.1.1.1
Nuplus1 TNIP config>SET DESTINATION

Tunnel Destination address [0.0.0.0]? 2.2.2.2
Nuplus1 TNIP config>ENABLE TUNNEL
Nuplus1 TNIP config>SET PROTOCOL

-- GRE Config --
Nuplus1 GRE config>ENABLE CHECKSUM
Nuplus1 GRE config>ENABLE KEY

Tunnel key: [0]? 1234
Nuplus1 GRE config>ENABLE SEQUENCE
Nuplus1 GRE config>ENABLE PROP_SEQ
Nuplus1 GRE config>EXIT
Nuplus1 TNIP config>EXIT
```

Configuramos el interfaz Frame Relay

```
Nuplus1 Config>NETWORK 1

-- Frame Relay user configuration --
Nuplus1 FR config>DISABLE LMI
Nuplus1 FR config>SET FRAME-SIZE
Interface MTU in bytes [2048]? 1500
Nuplus1 FR config>ADD PVC
Circuit number[16]?
Committed Information Rate (CIR) in bps[16000]? 64000
Committed Burst Size (Bc) in bits[16000]?
Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)?
Assign circuit name[]?
Nuplus1 FR config>ADD PROTOCOL-ADDRESS
IP Address [0.0.0.0]? 1.1.1.2
Circuit number[16]?
Nuplus1 FR config>EXIT
```

Agregamos las rutas necesarias

```
Nuplus1 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus1 Conf IP>LIST ROUTE

Nuplus1 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 2.2.2.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 1.1.1.2
Cost[1]?
Nuplus1 Conf IP>EXIT
Nuplus1 Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Nuplus1 Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Por último configuramos el bridge.

```
*P 4

Nuplus1 Config>PROTOCOL ASRT

-- ASRT Bridge user configuration --
Nuplus1 ASRT config>ENABLE BRIDGE
Nuplus1 ASRT config>ADD PORT
Interface Number[0]? 2
Port Number[2]?
Nuplus1 ASRT config>DISABLE STP
Nuplus1 ASRT config>LIST BRIDGE
Source Routing Transparent Bridge Configuration
              ==================================================

Bridge:    Enabled                              Bridge behavior: STB
                   +-----------------------------------------+
-------------------|       SOURCE ROUTING INFORMATION        |-----------------
                   +-----------------------------------------+
Bridge Number:           00                     Segments:          0
Max ARE Hop Cnt:         00                     Max STE Hop cnt:  00
1:N SRB:                 Not Active             Internal Segment:  0x000
LF-bit interpret:        Extended
                   +-----------------------------------------+
-------------------|             SR-TB INFORMATION           |-----------------
                   +-----------------------------------------+
SR-TB Conversion:        Disabled
TB-Virtual Segment:      0x000                  MTU of TB-Domain:  0
                   +-----------------------------------------+
-------------------|    SPANNING TREE PROTOCOL INFORMATION   |------------------

                   +-----------------------------------------+
Bridge Address:          Default                Bridge Priority:   32768/0x8000

STP Participation:       Disabled
                   +-----------------------------------------+
-------------------|        TRANSLATION INFORMATION          |------------------

                   +-----------------------------------------+
FA<=>GA Conversion:      Enabled                UB-Encapsulation:  Disabled
DLS for the bridge:      Disabled
                   +-----------------------------------------+
-------------------|            PORT INFORMATION             |------------------

                   +-----------------------------------------+
Number of ports added: 2
Port:   1      Interface:       0      Behavior:    STB Only   STP: Enabled

Port:   2      Interface:       2      Behavior:    STB Only   STP: Enabled


Nuplus1 ASRT config>EXIT
Nuplus1 Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Nuplus1 Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

b) Configuración Nuplus2

Agregamos el interfaz Frame Relay y lo configuramos de manera análoga al anterior.

Configuramos las direcciones de los interfaces.

Añadimos la ruta necesaria para que el origen y el destino del túnel sean accesibles

```
Nuplus2 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus2 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 2.2.2.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 194.6.1.127
Cost[1]?
Nuplus2 Conf IP>
```

c) Configuración Nuplus3

Agregamos el interfaz Frame Relay y lo configuramos de manera análoga al anterior.

Configuramos las direcciones de los interfaces.

Añadimos la ruta necesaria para que el origen y el destino del túnel sean accesibles

```
Nuplus3 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus3 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 1.1.1.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 194.6.1.125
Cost[1]?
Nuplus3 Conf IP>
```

d) Configuración Nuplus4

Al igual que para Nuplus1, se añade el interfaz Frame Relay y el interfaz túnel IP (TNIP)

```
*P 4
Config>SET HOSTNAME
What is the new router name?[]?Nuplus4
Config>SET DATA FR
which port will be changed[1]?
Config>ADD DEVICE TNIP
Added TNIP interface with num: 2

TNIP tunnel encapsulated type:[GRE]?
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuramos las direcciones de los interfaces

```
Nuplus4 *P 4
Nuplus4 Config>PROTOCOL IP
Internet protocol user configuration
Which net is this address for[0]?
New address [0.0.0.0]? 195.6.1.3
Address mask [255.255.255.0]? 255.255.255.0
Nuplus4 Conf IP>ADD ADDRESS
Which net is this address for[0]? 1
New address[0.0.0.0]? 2.2.2.2
Address mask [255.255.255.0]? 255.255.255.0
Nuplus4 Conf IP>ADD ADDRESS
Which net is this address for[0]? 2
New address [0.0.0.0]? 0.0.0.2
Nuplus4 Conf IP>LIST ADDRESS
IP addresses for each interface:
   intf  0   195.6.1. 3       255.255.255.0    NETWORK broadcast,    fill 0
   intf  1   2.2.2.2          255.255.255.0    NETWORK broadcast,    fill 0
   intf  2   0.0.0.2          0.0.0.0          NETWORK broadcast,    fill 0
   intf  3                                     IP disabled on this interface
Nuplus4 Conf IP>EXIT
```

A continuación configuramos el túnel

```
Nuplus4 Config>NETWORK 2

-- IP Tunnel Net Config --
Nuplus4 TNIP config>SET SOURCE

Tunnel Source address [0.0.0.0]? 2.2.2.2
Nuplus4 TNIP config>SET DESTINATION

Tunnel Destination address [0.0.0.0]? 1.1.1.1
Nuplus4 TNIP config>ENABLE TUNNEL
Nuplus4 TNIP config>SET PROTOCOL

-- GRE Config --
Nuplus4 GRE config>ENABLE CHECKSUM
Nuplus4 GRE config>ENABLE KEY

Tunnel key: [0]? 1234
Nuplus4 GRE config>ENABLE SEQUENCE
Nuplus4 GRE config>ENABLE PROP_SEQ
Nuplus4 GRE config>EXIT
Nuplus4 TNIP config>EXIT
```

Configuramos el interfaz Frame Relay

```
Nuplus4 Config>NETWORK 1

-- Frame Relay user configuration --
Nuplus4 FR config>DISABLE LMI
Nuplus4 FR config>SET FRAME-SIZE
Interface MTU in bytes [2048]? 1500
Nuplus4 FR config>ADD PVC
Circuit number[16]?
Committed Information Rate (CIR) in bps[16000]? 64000
Committed Burst Size (Bc) in bits[16000]?
Excess Burst Size (Be) in bits[0]?
Encrypt information? [No]:(Yes/No)?
Assign circuit name[]?
Nuplus4 FR config>ADD PROTOCOL-ADDRESS
IP Address [0.0.0.0]? 2.2.2.1
Circuit number[16]?
Nuplus4 FR config>EXIT
```

Agregamos las rutas necesarias

```
Nuplus4 Config>PROTOCOL IP
Internet protocol user configuration
Nuplus4 Conf IP>LIST ROUTE

Nuplus4 Conf IP>ADD ROUTE
IP destination [0.0.0.0]? 1.1.1.0
Address mask [0.0.0.0]? 255.255.255.0
Via gateway at [0.0.0.0]? 2.2.2.1
Cost[1]?
Nuplus4 Conf IP>EXIT
Nuplus4 Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Nuplus4 Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Por último configuramos el bridge.

```
*P 4

Nuplus4 Config>PROTOCOL ASRT

-- ASRT Bridge user configuration --
Nuplus4 ASRT config>ENABLE BRIDGE
Nuplus4 ASRT config>ADD PORT
Interface Number[0]? 2
Port Number[2]?
Nuplus4 ASRT config>DISABLE STP
Nuplus4 ASRT config>EXIT
Nuplus4 Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Nuplus4 Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Capítulo 5
Eventos del interfaz Túnel IP (TNIP)

1. Monitorización de eventos del interfaz Túnel IP (TNIP)

Permiten monitorizar en tiempo real los eventos que suceden sobre uno o varios interfaces TNIP cuando esta habilitado el sistema de eventos para ese protocolo.

La forma en que se habilitan desde el menú de configuración es la siguiente:

```
*P 4

-- ELS Config --
ELS Config>
ELS Config>ENABLE TRACE SUBSYSTEM TNIP ALL
ELS Config>EXIT
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Así mismo pueden ser habilitados desde el menú de monitorización en cualquier momento sin necesidad de que este almacenada en la configuración de la siguiente forma:

```
*P 3

+EVENT

-- ELS Monitor --
ELS>ENABLE TRACE SUBSYSTEM TNIP ALL
ELS>EXIT
```

El listado de eventos disponibles para el protocolo TNIP es el siguiente (Excepto los eventos específicos de los túneles dinámicos, definidos en el capítulo 6):

TNIP.001

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.001 Pack rec *str_protocolo_enc*, ext prt 0x*num_protocolo_externo*, (*dirección_ip_origen- >dirección_ip_destino*), int *interfaz ID*

Sintaxis Larga:

TNIP.001 Packet received with encapsulation *str_protocolo_enc*, external protocol 0x*num_protocolo_externo*, (source *dirección_ip_origen* destination *dirección_ip_destino*), on interface *interfaz ID*

Descripción:

Se ha recibido un paquete con un protocolo de encapsulado dado, que viajaba en un protocolo externo con numero dado, y el origen y destino del mismo es el dado. El interfaz encargado de su desencapsulado es el dado.

TNIP.002

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.002 Pack rec *str_protocolo_enc*, ext prt 0x*num_protocolo_externo*, (*dirección_ip_origen->dirección_ip_destino*), no tunnel

Sintaxis Larga:

TNIP.002 Received packet with encapsulation *str_protocolo_enc*, external protocol 0x*num_protocolo_externo*, (source *dirección_ip_origen* destination *dirección_ip_destino*) There is no tunnel for it.

Descripción:

Se ha recibido un paquete con un protocolo de encapsulado dado. El protocolo externo es el dado. Con el origen y destino dados no se ha encontrado túnel que se pueda encargar de su desencapsulado.

Causa:

Un dispositivo externo esta enviando paquetes hacia el router pero no se aceptan por no tener el origen y destino configurados en los interfaces túnel

Acción:

Cambiar configuración de túneles para aceptar dichos paquetes si así se desea. Identificar el dispositivo externo y configurarlo para que no mande dichos paquetes.

TNIP.003

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.003 Incom pack disc no act int, int *interfaz ID*

Sintaxis Larga:

TNIP.003 Incoming packet discarded. The interface is down. Interface *interfaz ID*

Descripción:

La función de entrada del interfaz de túnel ha descartado el paquete por estar dicho interfaz inactivo.

TNIP.004

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.004 Incom pack disc no conf int, int *interfaz ID*

Sintaxis Larga:

TNIP.004 Incoming packet discarded. The interface has no configuration. Interface *interfaz ID*

Descripción:

La función de entrada del interfaz de túnel ha descartado el paquete por estar dicho interfaz desconfigurado.

TNIP.005

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.005 Incom pack disc encapsul prot reject,int *interfaz ID*

Sintaxis Larga:

TNIP.005 Incoming packet has been discarded because the interface configuration has a different encapsulation protocol, interface *interfaz ID*

Descripción:

La función de entrada del interfaz de túnel ha descartado el paquete por estar dicho interfaz configurado con un modo (tipo de protocolo de encapsulado esperado) distinto al que ha llegado.

Causa:

Interfaz mal configurado en alguno de los extremos del túnel.

Acción:

Configurar el mismo modo de funcionamiento en ambos extremos del túnel.

TNIP.006

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.006 Err GRE header flag routing act, int *interfaz ID*

Sintaxis Larga:

TNIP.006 Error in GRE header. Flags have the routing option , interface *interfaz ID*

Descripción:

La función de desencapsulado GRE ha descartado el paquete por tener la opción de routing activa.

Causa:

El otro extremo del túnel esta enviando paquetes GRE con campo routing. Por ahora no se aceptan este tipo de paquete.

Acción:

Configurar dicho extremo sin routing GRE.

TNIP.007

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.007 Err GRE header chksm 0x*checksum* (exp 0x*checksum_esperado*), int *int ID*

Sintaxis Larga:

TNIP.007 Error in GRE header, checksum 0x*checksum* (expected 0x*checksum_esperado*), interface *interfaz ID*

Descripción:

Este mensaje se genera cuando un paquete tiene un checksum invalido. El checksum recibido se muestra junto con el correcto

Causa:

Lo más probable es que sea un paquete dañado. Puede ser que un nodo esté construyendo una cabecera errónea.

Acción:

Si el problema persiste, examinar una traza para determinar donde se daña el paquete.

TNIP.008

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP. Dsc GRE pack key *key* (exp *key_esperado*), int *interfaz ID*

Sintaxis Larga:

TNIP.008 Packet GRE discarded, key *key* (expected *key_esperado*), interface *interfaz ID*

Descripción:

Este mensaje se genera cuando un paquete tiene un key invalido. El key recibido se muestra junto con el correcto

Causa:

Puede ser que un nodo esté configurado con un key erróneo.

Acción:

Configurar el key correctamente.

TNIP.009

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.009 Dsc GRE pack with no key(exp *key_esperado*), int *interfaz ID*

Sintaxis Larga:

TNIP.009 Packet GRE with no key discarded (expected *key_esperado*), interface *interfaz ID*

Descripción:

Este mensaje se genera cuando un paquete no tiene key y el túnel estaba configurado con comprobación de identificación de key.

Causa:

Puede ser que un nodo esté mal configurado.

Acción:

Configurar el key correctamente.

TNIP.010

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.010 Dsc GRE pack with key (exp sin key), int *interfaz ID*

Sintaxis Larga:

TNIP.010 Packet GRE with key discarded, key *key*(not expected key), interface *interfaz ID*

Descripción:

Este mensaje se genera cuando un paquete tiene key y el túnel esta configurado sin comprobación de identificación de key.

Causa:

Puede ser que un nodo esté mal configurado.

Acción:

Configurar el key correctamente.

TNIP.011

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.011 Dsc GRE pack seq *num_sec* less exp *num_sec_esperado*, int *interfaz ID*

Sintaxis Larga:

TNIP.011 Packet GRE discarded, sequence number *num_sec* less than expected *num_sec_esperado*, interface *interfaz ID*

Descripción:

Este mensaje se genera cuando un paquete llega con un numero de secuencia invalido. El numero de secuencia recibido se muestra junto con el correcto

Causa:

Los extremos están desincronizados.

Acción:

Esperar a que se sincronicen. Si números de secuencia muy dispares y el tiempo de sincronización se prevé largo se puede optar por reiniciar los equipos.

TNIP.012

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.012 Err GRE header flag recurs act, int *interfaz ID*

Sintaxis Larga:

TNIP.012 Error in GRE header. Recursion option active, interface *interfaz ID*

Descripción:

La función de desencapsulado GRE ha descartado el paquete por tener la opción de recursión activa. No aceptamos encapsulado múltiple.

Causa:

El otro extremo del túnel esta enviando paquetes GRE con encapsulado múltiple.

Acción:

Cambiar configuración para evitar que paquetes GRE entren en el túnel.

TNIP.013

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.013 Err GRE header wrong vrsn *versión*, int *interfaz ID*

Sintaxis Larga:

TNIP.013 Error in GRE header, invalid encapsulation version *versión*, interface *interfaz ID*

Descripción:

La función de desencapsulado GRE ha descartado el paquete por tener una versión no conocida.

Causa:

El otro extremo del túnel esta enviando paquetes GRE con versión posterior. O esta construyendo mal la cabecera.

Acción:

Cambiar versión de GRE.

TNIP.014

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.014 Desencap pack GRE , inter prt 0x*num_protocolo*, (*dirección_ip_origen->dirección_ip_destino*), int *interfaz ID*, seq *num_sec*

Sintaxis Larga:

TNIP.014 Desencapsulated GRE packet with success, internal protocol 0x*num_protocolo* (source *dirección_ip_origen* and destination *dirección_ip_destino*), interface *interfaz ID*, sequence number *num_sec*

Descripción:

Se ha procesado el desencapsulado de un paquete GRE con éxito. Se especifica el protocolo que viajaba en el interior del paquete GRE (el origen y el destino) y el interfaz encargado de su desencapsulado.

TNIP.015

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.015 Desencap pack GRE, inter prt 0x*num_protocolo*, unknown, int *interfaz ID*

Sintaxis Larga:

TNIP.015 Error in desencapsulated GRE packet, unknown internal protocol 0x*num_protocolo*, , interface *interfaz ID*

Descripción:

Se ha procesado el desencapsulado de un paquete GRE y el protocolo que viajaba en el interior del paquete GRE es desconocido.

TNIP.016

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.016 Dsc out pack int no act, int *interfaz ID*

Sintaxis Larga:

TNIP.016 The interface is down so the outgoing packet has been discarded, interface *interfaz ID*

Descripción:

La función de salida del interfaz de túnel ha descartado el paquete por estar dicho interfaz inactivo.

TNIP.017

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.017 Dsc out pack int no conf, int *interfaz ID*

Sintaxis Larga:

TNIP.017 The interface is no configured so the outgoing packet has been discarded, interface *interfaz ID*

Descripción:

La función de salida del interfaz de túnel ha descartado el paquete por estar dicho interfaz desconfigurado.

TNIP.018

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.018 Dsc out pack invalid inter prt 0x*num_protocolo*, int *interfaz ID*

Sintaxis Larga:

TNIP.018 The internal protocol 0x*num_protocolo* has been rejected so the outgoing packet has been discarded, interface *interfaz ID*

Descripción:

La función de salida del interfaz de túnel ha descartado el paquete por no aceptarse el protocolo interno (protocolo payload) para ser encapsulado.

TNIP.019

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.019 Encap GRE pack, inter prt 0x*num_protocolo*, (*dirección_ip_origen->dirección_ip_destino*), int *interfaz ID*

Sintaxis Larga:

TNIP.019 Successful encapsulated GRE packet, internal protocol 0x*num_protocolo*, (source *dirección_ip_origen* and destination *dirección_ip_destino*), interface *interfaz ID*

Descripción:

La función de salida del interfaz de túnel ha encapsulado un paquete GRE con éxito. Se especifica el protocolo del paquete que ha sido encapsulado así como el origen y el destino del mismo.

TNIP.020

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.020 Snd pack *str_protocolo_enc*, ext prt 0x*num_protocolo_externo*, (*dirección_ip_origen->dirección_ip_destino*), int *interfaz ID*, seq *num_sec*

Sintaxis Larga:

TNIP.020 Sending packet *str_protocolo_enc*, ext prt 0x*num_protocolo_externo*, (source *dirección_ip_origen* and destination *dirección_ip_destino*), interface *interfaz ID*, sequence number *num_sec*

Descripción:

Se ha enviado un paquete con un protocolo de encapsulado dado, el protocolo externo (delivery

protocol) es el dado, también se especifica dirección origen y destino así como el interfaz que se encargó de su encapsulado.

TNIP.025

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.025 Pack GRE ciph, inter prt 0x*num_protocolo_interno*, (*dirección_ip_origen->dirección_ip_destino*), int *interfaz ID*

Sintaxis Larga:

TNIP.025 Successful ciphered GRE packet, internal protocol 0x*num_protocolo_interno*, (source *dirección_ip_origen->* destination *dirección_ip_destino*), interface *interfaz ID*

Descripción:

Se ha cifrado un paquete GRE con un protocolo de encapsulado dado, entre las direcciones especificadas

TNIP.026

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.026 Pack GRE desciph, inter prt 0x*num_protocolo_interno*, (*dirección_ip_origen->dirección_ip_destino*), int *interfaz ID*

Sintaxis Larga:

TNIP.026 Successful deciphered GRE packet, internal protocol 0x*num_protocolo_interno*, (source *dirección_ip_origen->* destination *dirección_ip_destino*), interface *interfaz ID*

Descripción:

Se ha descifrado con éxito el payload de un paquete GRE. Se especifica el protocolo que viajaba en el interior del paquete GRE (el origen y el destino) y el interfaz encargado de su desencapsulado.

TNIP.027

Nivel: Error interno anormal, ERROR-AI/UI-ERROR

Sintaxis Corta:

TNIP.027 Err desciph GRE, int *interfaz ID*

Sintaxis Larga:

Error deciphering GRE, interface *interfaz ID*

args %3"interfaz ID"

Descripción:

Este mensaje se genera cuando un paquete se descifra y da un checksum de cifrado inválido, o el protocolo no era cifrado. Lo más probable es que la clave de cifrado esté mal, o que el paquete no esté cifrado.

TNIP.028

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.028 Desencap pack GRE , inter prt 0x*num_protocolo*, int *interfaz ID*, sec *num_sec*

Sintaxis Larga:

TNIP.028 Desencapsulated GRE packet with success, internal protocol 0x*num_protocolo* interface *interfaz ID*, sequence number *num_sec*

Descripción:

Se ha procesado el desencapsulado de un paquete GRE con éxito. Se especifica el protocolo que viajaba en el interior del paquete GRE y el interfaz encargado de su desencapsulado.

TNIP.029

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.029 Pack GRE ciph, inter prt 0x*num_protocolo_interno*, int *interfaz ID*

Sintaxis Larga:

TNIP.029 Successful ciphered GRE packet, internal protocol 0x*num_protocolo_interno* interface *interfaz ID*

Descripción:

Se ha cifrado un paquete GRE con un protocolo de encapsulado dado

TNIP.030

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.030 Encap GRE pack, inter prt 0x*num_protocolo*, int *interfaz ID*

Sintaxis Larga:

TNIP.030 Successful encapsulated GRE packet, internal protocol 0x*num_protocolo* interface *interfaz ID*

Descripción:

Se ha procesado el encapsulado de un paquete GRE con éxito. Se especifica el protocolo del paquete que ha sido encapsulado.

TNIP.031

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.031 Desencap pack GRE , inter prt 0x*num_protocolo*, (*dirección_mac_origen->dirección_mac_destino*), int *interfaz ID*, sec *num_sec*

Sintaxis Larga:

TNIP.031 Desencapsulated GRE packet with success, internal protocol 0x*num_protocolo* (source *dirección_mac_origen* and destination *dirección_mac_destino*), interface *interfaz ID*, sequence number *num_sec*

Descripción:

Se ha procesado el desencapsulado de un paquete GRE con éxito. Se especifica el protocolo que viajaba en el interior del paquete GRE (el origen y el destino mac) y el interfaz encargado de su desencapsulado.

TNIP.032

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.032 Pack GRE ciph, inter prt 0x*num_protocolo_interno*, (*dirección_mac_origen->dirección_mac_destino*), int *interfaz ID*

Sintaxis Larga:

TNIP.032 Successful ciphered GRE packet, internal protocol 0x*num_protocolo_interno*, (source *dirección_mac_origen->* destination *dirección_mac_destino*), interface *interfaz ID*

Descripción:

Se ha cifrado un paquete GRE con un protocolo de encapsulado dado, entre las direcciones mac especificadas

TNIP.033

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.033 Encap GRE pack, inter prt 0x*num_protocolo*, (*dirección_mac_origen->dirección_mac_destino*), int *interfaz ID*

Sintaxis Larga:

TNIP.033 Successful encapsulated GRE packet, internal protocol 0x*num_protocolo*, (source *dirección_mac_origen* and destination *dirección_mac_destino*), interface *interfaz ID*

Descripción:

La función de salida del interfaz de túnel ha encapsulado un paquete GRE con éxito. Se especifica el protocolo del paquete que ha sido encapsulado así como el origen y el destino mac del mismo.

Capítulo 6
Túneles Dinámicos (Internet)

1. Descripción

1.1. Introducción

Si aplicamos la técnica de los túneles a las redes públicas Internet será posible la interconexión de redes locales dispersas de una forma barata y eficaz. A partir de la técnica de túneles vista en los capítulos anteriores podría realizarse, pero nos encontraríamos con algunas dificultades que trataremos en este capítulo, entre ellas las siguientes:

- Para establecer un túnel entre dos puntos, es imprescindible que ambos conozcan la dirección IP del extremo, por lo que sólo sería realizable con accesos autentificados e IP fijas (lo que es un recurso limitado y caro en Internet).
- La conexión de *n* redes locales requeriría configurar y establecer en cada uno de ellos *n-1* túneles.

La solución a estos problemas pasa por un equipo central (con una dirección IP fija y conocida) que soporta *n* túneles, y que gestiona el tráfico inter-túnel por lo que el segundo problema queda solucionado automáticamente mientras que la solución al primero consiste en dotar a este equipo de la capacidad de adaptar la configuración de sus túneles para permitir conexiones de equipos cuya IP es distinta cada vez que se conectan. **Esta reconfiguración dinámica del túnel cada nueva conexión es el motivo de que estos túneles reciban el nombre de túneles "dinámicos".**

En adelante denominaremos al equipo central como el router de "ISP" *(CENTRIX-ISP)***, puesto que su ubicación normal será en un Internet Server Provider, mientras que los routers que se conectan a él los denominaremos los routers "clientes".**

1.2. Escenarios/Problemática presentada

- **Escenario 4:** Acceso de los equipos de una red local a Internet para servicios de la red (html, ftp,…) mediante un router (típicamente con E-NAT).
- **Escenario 5**: Interconexión de redes locales remotas con la red local del ISP, mediante routers con túneles.
- **Escenario 6:** Interconexión de redes locales remotas entre sí, y con la red local del ISP, mediante routers con túneles.

Si el objetivo es el escenario 5/6, la configuración del los routers "clientes" es sencilla puesto que podemos predecir que cualquier dirección IP que no sea local es accesible mediante el túnel, pero si la intención es permitir simultáneamente el escenario 4, los routers "clientes" deben distinguir si una determinada dirección destino es accesible por el túnel o fuera de él (dirección de Internet). Esto obliga a que los "clientes" conozcan las redes alcanzables a través del túnel. La solución pasa por configurar todas las rutas posibles en todos los clientes, o configurarlas en el router central "ISP", y que éste informe a los clientes mediante un protocolo de routing (RIP).

Además el equipo del "ISP" debe conocer las redes accesibles a través de routers "clientes" junto a un mecanismo para "despertar" a éstos si son requeridos. Este mecanismo consiste en una tabla que debe asociar las direcciones de las redes locales de los "clientes" con su número RDSI. Cuando se desee establecer una comunicación con un "cliente" no conectado, el equipo de "ISP" lanzará una llamada hasta él, con la única finalidad de indicarle que debe realizar la conexión, por lo que el cliente rechazará la llamada y procederá a la conexión normal a Internet.

NOTA 1: Esta primera llamada no se tarifica, puesto que no llega a conectarse.

NOTA 2: El protocolo RIP sobre el túnel no provocará llamadas RDSI, ni se tendrá en cuenta para liberar llamadas RDSI en ausencia de datos.

NOTA 3: Si no se requiere el escenario 4, y queremos que la ruta por defecto sea el túnel, debe deshabilitarse la opción *Cambiar ruta por defecto* en el enlace PPP.

1.3. Tipos de túneles

Realizaremos la siguiente clasificación de túneles con el objetivo de analizar los distintos comportamientos en cada caso:

- **Estáticos**: Llamaremos así a los túneles, donde las direcciones origen y destino son fijas, (vistos en el capítulo 4). Estos túneles no serán tratados por tanto en este capítulo.
- **Dinámicos**: Cuando una de las direcciones (origen o destino) del túnel es desconocida antes de efectuarse la conexión, y el equipo que se conectará es desconocido.
- **Semidinámicos**: Se trata de un caso especial de túnel dinámico en el que a pesar de no conocer la dirección del equipo que se conectará, conocemos a este, pues el identificador de túnel (campo key de GRE) es único.

(Los túneles dinámicos y semidinámicos son el caso normal en Internet cuando la dirección obtenida por el equipo remoto no está preasignada).

a) Túneles "dinámicos"

Son los túneles más fáciles de configurar y a la vez los más flexibles, por lo que se recomienda su uso frente a los otros tipos.

El equipo de "ISP" ofrece *n* túneles a los "clientes", que éstos utilizan a medida que se conectan; cuando un cliente deja de enviar información, el túnel que estaba haciendo servir este cliente queda disponible para una nueva conexión.

La potencia de esta configuración radica en el uso de RIP para que el "cliente" informe al "ISP" de las redes accesibles a través de él y viceversa.

Es usual configurar un conjunto de túneles para dar servicio a una determinada entidad con el mismo "key", de forma que en la configuración de grupos IP se asigne a todos estos interfaces una misma tabla de routing.

b) Túneles semidinámicos

Son una extensión de los túneles dinámicos, en los que discriminamos los equipos remotos que permitimos que se conecten en cada túnel del ISP. Para ello configuraremos un "identificador" único en el túnel que debe coincidir con el configurado en el equipo remoto (campo Key de GRE). Realmente es como configurar un único túnel dinámico para cada equipo remoto.

Estos túneles añaden dos funcionalidades:

- Identificación del equipo remoto.
- Como sabemos a priori el "cliente" que se conecta a cada túnel, podemos agregar rutas, y por tanto deshabilitar RIP.

Por lo tanto estos túneles se recomiendan únicamente cuando se quiera prescindir de RIP o la seguridad y el control de acceso sea indispensable, pues requieren mayor esfuerzo de configuración, al tener que relacionar identificadores con equipos remotos.

NOTA 1: Debido a que no sabemos que "cliente" se conectará a un túnel dinámico, es imprescindible el uso de RIP en éstos.
NOTA 2: Siempre que se precise "despertar" un router cliente, es necesario mantener RIP desde el cliente hacia el ISP.

1.4. Importancia del RIP

Uno de los aspectos más delicados de este tipo de túneles es el control del estado de los mismos; a partir de un estado en el que están "a la espera" pasa a un estado "conectado" con el equipo remoto *cliente* que lo solicite. Mientras el túnel permanece en uso se mantiene en este estado, pero cuando deja de ser utilizado debe volver al estado inicial, en espera de futuros usos.

Uno de los aspectos más críticos cuando se establecen túneles dinámicos es la decisión de si el túnel permanece en uso o no, pues el equipo remoto puede haberse desconectado o apagado sin previo aviso, por lo que es necesario un* diálogo *entre los routers que sostienen los túneles, para lo que se utiliza el protocolo estándar RIP.

Si queremos evitar la "reutilización" de un túnel, reservándolo exclusivamente para dar servicio a un equipo "cliente", identificaremos éste con un "key" único.

Otra cuestión de gran importancia es el acceso a clientes que no tienen establecida una conexión con Internet, cuya solución pasa por configurar en el equipo de *ISP* una tabla con la(s) dirección(es), red(es) o subred(es) accesible(s) a través de cada cliente junto al número del acceso RDSI del mismo, siendo el funcionamiento el siguiente: Cuando el equipo de *ISP* reciba información **cuyo destino exista en la tabla y no esté conectado por ningún túnel**, realizará una llamada RDSI al equipo *cliente*, quien la rechazará con objeto de que no sea tarificada, realizando a continuación la conexión a Internet.

Por tanto cuando el cliente realiza la conexión debe informar de red(es) o subred(es) accesible(s) a través del mismo, para que el equipo de ISP no realice más llamadas, y en lugar de ello entregué al router* cliente *el tráfico dirigido a esos destinos, para lo que también se hace servir RIP.

Resumen de facilidades que aporta RIP:

a) Control de "desconexión" para reutilización de túneles.

b) Control de “conexión” cuando se ha de “despertar” a los *clientes*.

c) Informar de red(es) accesibles.

Problemas que puede presentar el RIP:

Cuando las direcciones IP de los extremos de un túnel son de redes distintas, puede darse el caso de que un router reciba información de accesibilidad de la red destino del túnel a través del propio interfaz túnel, por lo que se perdería el acceso al extremo remoto. Esto no se dará nunca en Internet cuando la dirección que adquiera el cliente pertenezca a la red del equipo de ISP, pero sí en el resto de casos.

Para solucionarlo bastaría con añadir una ruta estática para acceder al destino, siempre que podamos conocerlo a priori.

En cualquier caso esta situación es detectada por los routers, que a su vez informan con eventos y estadísticos.

2. Escenarios de utilización

Es fundamental definir la utilización del router antes de configurar túneles en el mismo, pues el aprovechamiento óptimo de router y línea de comunicaciones está en función de que la configuración encaje al máximo con las necesidades.

La decisión más importante radica en la configuración de rutas estáticas, o delegar esta cuestión en un protocolo de routing, que facilitará la configuración pero disminuirá el rendimiento al utilizar parte del ancho de banda de la línea en intercambiar mensajes entre routers.

Aunque no existe una norma general, si podemos basarnos en unas directrices que ayudarán a tomar la decisión más conveniente, para lo cual es imprescindible definir el escenario en el que trabajará el router, por lo que se deberá tener en el equipo de acceso:

- **Escenario 5/6 (túnel):** Todas las direcciones no locales son accesibles a través del túnel, por lo que hay suficiente con configurar éste como ruta por defecto (excepto la dirección del extremo remoto del túnel, que debe configurarse de forma estática).
- **Túnel por Internet + Navegar por Internet:** Si las redes locales remotas no son del tipo 10.X.X.X no es necesario ninguna configuración de rutas.

Además hay que tener presentes aspectos vistos en capítulos anteriores:

- Cuando se utilicen túneles *dinámicos* es necesario configurar RIP, debido a la reutilización de los mismos.

Igualmente cuando se pretenda *despertar* a un cliente debe configurarse RIP desde éste hacia el ISP.

2.1. Funcionamiento de túneles sin navegar por Internet (Esc. 5/6)

La configuración en los "clientes" se basa en definir el túnel como el camino por defecto hacia cualquier destino (excepto destinos locales o ISP), por tanto podemos inhibir el RIP que llega desde el "ISP", mejorando el rendimiento de la línea pues el tráfico RIP en este sentido es elevado si el "ISP" soporta muchos túneles.

a) Mínimo esfuerzo de configuración a costa de RIP

Se consigue con túneles dinámicos (por tanto reutilizables), siendo imprescindible el uso de RIP en el sentido "cliente"→ "ISP" para conocer las redes accesibles del cliente.

Permite navegar:	No
Tipo de túnel:	Dinámico
Ruta por defecto:	Túnel
RIP:	“Cliente” ⇒ “ISP”
Seguridad:	Baja
Dificultad de configuración	Muy baja
Eficiencia	Alta

b) *Mayor esfuerzo de configuración reduciendo el tráfico RIP*

Mediante túneles dedicados para cada equipo remoto que quiera acceder, pues el cliente queda identificado y no es imprescindible RIP en el sentido “cliente”→”ISP”. Por el contrario deben mantenerse los identificadores al configurar túneles en “ISP” y “clientes”.

Permite navegar:	No
Tipo de túnel:	Semidinámico
Ruta por defecto:	Túnel
RIP:	No (“Cliente” ⇒ “ISP”) Si se debe “despertar”
Seguridad:	Alta
Dificultad de configuración	Media
Eficiencia	Muy Alta

2.2. Túneles y Navegación simultánea (Esc. 4 + 5/6)

En los “clientes” el camino por defecto hacia cualquier destino será la red extensa (Internet), y por tanto, los destinos hacia redes accesibles por el túnel han de ser conocidos, lo que se puede conseguir mediante configuración estática en cada uno de ellos, o puede ser configurado únicamente en el “ISP” y que éste informe a los “clientes” por RIP.

a) *Mayor sobrecarga en la red / Mínimo esfuerzo de configuración*

En casos en los que el número de clientes no sea muy elevado, puede delegarse el mecanismo de routing en el protocolo RIP, eliminando la necesidad de configurar rutas estáticas en los “clientes”.

Permite navegar:	No
Tipo de túnel:	Dinámico
Ruta por defecto:	Internet
RIP:	”Clientes” ⇔“ISP”
Seguridad:	Baja
Dificultad de configuración	Baja
Eficiencia	Baja si hay muchos túneles

Esto no excluye algún caso concreto en el que no sea conveniente utilizar RIP con alguna delegación en particular, pudiendo dedicarle un "key" único.

Este escenario es muy útil cuando el objetivo es la interconexión de unas pocas redes locales remotas entre si.

b) Mínima sobrecarga en la red / Mayor esfuerzo de configuración

Cuando el número de rutas conocidas por el equipo del ISP comienza a ser importante (ya sea porque el número de túneles es elevado o porque las redes locales remotas son complejas), el tráfico RIP puede llegar a afectar seriamente al rendimiento de los túneles, por lo que se debe evaluar la posibilidad de prescindir del protocolo de routing en el sentido ISP→Clientes, lo que obliga a configurar estáticamente en los clientes las redes a las que será posible llegar a través del túnel.

Permite navegar:	Si
Tipo de túnel:	Dinámico
Ruta por defecto:	Internet
RIP:	"Clientes" ⇒ "ISP"
Seguridad:	Media
Dificultad de configuración	Media
Eficiencia	Alta

Al igual que en los casos anteriores, cabe la posibilidad de eliminar RIP en el sentido Cliente→ISP, dedicándole un "key" único.

Este escenario es muy útil cuando el objetivo es el acceso de las redes locales remotas desde el ISP, y no la interconexión de redes locales remotas entre si, por ejemplo, cuando una entidad posea ISP propio y desee dar acceso a las delegaciones al mismo.

c) Sobrecarga nula en la red/Mayor esfuerzo de configuración/Control de clientes

Este escenario se basa totalmente en la utilización de "keys" distintos, de forma que cada interfaz túnel queda perfectamente definido, es decir, sabemos quien es el cliente que se conectará a él, y las redes alcanzables a través del mismo.

Permite navegar:	Si
Tipo de túnel:	Semidinámico
Ruta por defecto:	Internet
RIP:	No (“Cliente” ⇒ “ISP”) Si se debe “despertar”
Seguridad:	Alta
Dificultad de configuración	Alta
Eficiencia	Máxima

Esto reduce a cero la sobrecarga, pues se elimina totalmente el tráfico RIP a costa de configurar explícitamente todas las rutas alcanzables (Excepto si se pretende “despertar”).

Debido al mayor control de los clientes en este escenario, se hace apropiado cuando el ISP ofrece servicios de interconexión de redes a terceros.

Nota1: Es posible utilizar el campo “identificador” para distinguir entre clientes cuando se ofrece el servicio a terceros, ya sea mediante un identificador dedicado para cada punto remoto, o un identificador compartido entre un número máximo de túneles simultáneos contratados por un cliente dado.

Nota2: Cuando se ofrece el servicio a terceros, se ha deben evitar la duplicidad de direcciones entre las instalaciones de los clientes. Puede ser oportuno obligar a los clientes a utilizar unas determinadas redes o subredes para asegurarlo, a la vez que facilitar la configuración, **o bien separar los distintos clientes mediante la opción de grupos IP**.

3. Seguridad

Cuando se trata de conectar redes locales a través de una red pública, los aspectos relativos a la seguridad cobran gran importancia. Deben existir mecanismos para autenticar las conexiones, y mecanismos para evitar el tráfico inter-túnel no deseado.

El primer mecanismo de autenticación sería la utilización de direcciones fijas, aunque este es un recursos costoso en Internet. Por tanto cuando no pueda ser utilizado se debe recurrir a otro mecanismo, como pueden ser el identificador del protocolo GRE (key), que ha de ser conocido por ambos extremos (como se vio en el capítulo 1 dicho campo se compone de 32 bits, lo que supone más de 400 millones de posibles combinaciones).

Debido a que el tráfico inter-túnel es realizado por el equipo de "ISP", tenemos total control sobre el mismo, y mediante la unión de los identificadores de GRE y los grupos IP podemos aislar totalmente el tráfico entre túneles de distintos clientes, además de permitir y gestionar sin problemas la duplicidad de direcciones entre distintos clientes .

4. Configuración

Las posibilidades de configuración son numerosas, por lo que nos centraremos en las más comunes, escenarios 5 y 6 con túneles dinámicos (reutilizables) y RIP.

4.1. Claves para configurar túneles dinámicos

Debido la particularidades de estas conexiones, según se ha visto en el capítulo 1, se deben tener en cuenta los siguientes aspectos :

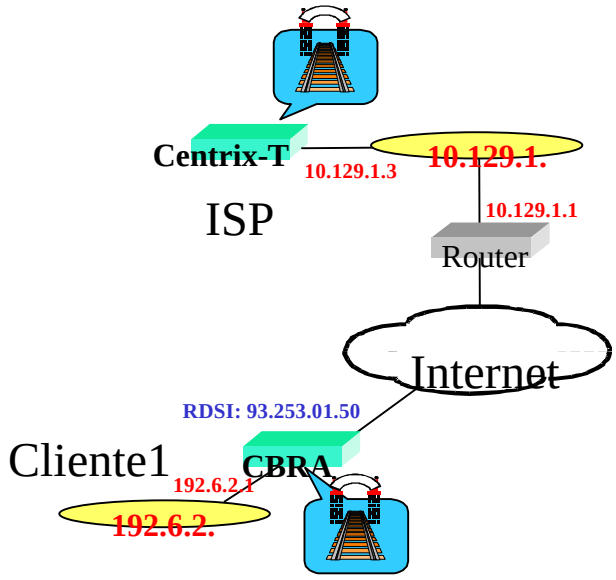
- **En el lado ISP** se configurarán túneles dinámicos con las siguientes características :
  a) Los interfaces de un mismo cliente estarán agrupados en un mismo Grupo IP
  b) La dirección IP origen del túnel será una dirección del equipo válida en la red pública, y accesible por los clientes.
  c) La dirección IP destino del túnel se debe dejar como 0.0.0.0, pues se refiere a la dirección del equipo de acceso del cliente, la cual no es conocida a priori, y será distinta cada vez que el cliente inicie un túnel.
  d) Se configurará el "key" asignado al cliente.
  e) Habilitar RIP sobre el túnel si es preciso.

  Además se configurará la tabla de redes remotas ⇔ Nº RDSI.

- **En el lado cliente** se configurará un único túnel, con las siguientes particularidades:
  a) La dirección destino será la dirección configurada como origen en el equipo del ISP.
  b) La dirección origen no es conocida a priori, por lo que la configuramos como 0.0.0.0.
  c) Se configurará el "key" asignado al cliente.
  d) Habilitar RIP sobre el túnel si es preciso.

- **Decisión de la Ruta por defecto,** en el caso de que la ruta por defecto sea el túnel en lugar del enlace WAN preconfigurado en el router, debe deshabilitarse la opción de "*Cambiar Ruta por Defecto*" en el encapsulador PPP correspondiente.

4.2. Ejemplo 1: Interconexión de Redes y acceso simultáneo por Internet (Esc. 4 + 5)



A partir de un ISP existente, es posible añadir un equipo que termine los túneles en el extremo proveedor sin modificar en absoluto la estructura existente; la única condición es que tal equipo (en nuestro ejemplo "Centrix-T") tenga asignada una dirección de la red pública accesible por los clientes. (En nuestro ejemplo el ISP tiene asignadas 256 direcciones Internet, del tipo 10.129.1.X, y se ha asignado la dirección 10.129.1.3 a "Centrix-T").

Además se configurará el nº RDSI de la oficina remota "CBRA" para poder "*despertarlo*".

Si se trata de crear un ISP en lugar de incorporar túneles en un ISP existente, se podría utilizar "Centrix-T" simultáneamente como extremo de túneles y Router de acceso, simplemente configurando de forma adecuada una línea Frame-Relay hacia la red pública.

a) Configuración Centrix-T (Equipo de ISP)

Configuración del nombre del equipo y creación de interfaces:

```
*P 4

Config>SET HOSTNAME CENTRIX
Config>ADD DEVICE TNIP
Added TNIP interface with num: 1

TNIP tunnel encapsulated type:[GRE]?
Config>ADD DEVICE PPP
Type basic access ISDN [2]?1
If you are going to config more than two DIAL interfaces, you must config what t
hey have CSR:F011640 and CSR:F011660 over the ISDN 2 connector
Ifc number to delete: [0]?8
Added PPP-DIAL interface with num: 3
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuración del interfaz túnel:

```
Centrix *P 4
Centrix Config>NETWORK 1
-- IP Tunnel Net Config --
Centrix TNIP config>ENABLE TUNNEL
Centrix TNIP config>SET SOURCE 10.129.1.3
```

Configuración del protocolo IP:

```
Centrix TNIP config>EXIT
Centrix Config>PROTOCOL IP
Internet protocol user configuration
Centrix Conf IP>ADD ADDRESS 0 10.129.1.3 255.255.255.0
Centrix Conf IP>ADD ADDRESS 1 0.0.0.1
Centrix Conf IP>ADD ISDN 192.6.2.0 255.255.255.0 *
ISDN Number[]? 932530150
Cost[1]? 5
Centrix Conf IP>ADD ROUTE 192.6.1.0 255.255.255.0 * 10.219.1.2 2
Centrix Conf IP>SET DEFAULT NETWORK-GATEWAY * 10.129.1.1 1
```

Configuración del protocolo RIP:

```
Centrix Conf IP>EXIT
Centrix Config>PROTOCOL RIP
RIP protocol user configuration
Centrix Conf RIP>ENABLE RIP
Centrix Conf RIP>SET COMPATIBILITY 10.129.1.3 * 1 4
```

Listado de interfaces:

```
Centrix Config>LIST DEVICES
Con    Ifc Type of interface                  CSR     CSR2  int
---      1 IP Tunnel                            0             0
---      4 Router->Node                         0             0
---      5 Node->Router                         0             0
LAN      0 Ethernet                       9000000            1C
WAN1     6 X25                            F001600  F000C00   9E
WAN2     7 X25                            F001620  F000D00   9D
ISDN 1   2 ISDN                           F001640  F000E00   9C
ISDN 1   3 channel B: PPP                        0             0
ISDN 1   8 channel D: X.25                A000000            1B
ISDN 2   9 channel D: X.25                A200000            1B
ISDN 2  10 channel B: X.25                F001660  F000F00   9B
```

Listado del interfaz túnel:

```
Centrix Config>NETWORK 1

-- IP Tunnel Net Config --
Centrix TNIP config>LIST ALL
Tunnel Mode: GRE
Tunnel Addresses
Source:      10.129.1.3
Destination: 0.0.0.0
Tunneling IP:   enable
Centrix TNIP config>SET PROTOCOL

-- GRE Config --
Centrix GRE config>LIST ALL
Cipher:         disabled
GRE Options GRE
End-to-End Checksumming:      disabled
Tunnel identification key:    disabled
Drop Out-of-Order Datagrams:  disabled
Proprietary sequence number:  disabled
Centrix GRE config>
```

Listado del protocolo IP:

```
Centrix Config>PROTOCOL IP
Internet protocol user configuration
Centrix Conf IP>LIST ALL
Interface addresses
IP addresses for each interface:
   intf  0  (       *) 10.129.1.3    255.255.255.0    NETWORK broadcast,   fill 0
   intf  1  (       *) 0.0.0.1       0.0.0.0          NETWORK broadcast,   fill 0
   intf  2                                            IP disabled on this interface
   intf  3                                            IP disabled on this interface
```

```
   intf  4                                          IP disabled on this interface
Routing
route to 192.6.1.0,255.255.255.0 via 10.219.1.2, cost 2 group *
route to 0.0.0.0,0.0.0.0 via 10.129.1.1, cost 1 group *
route to 192.6.2.0,255.255.255.0 via ISDN 932530150 cost 5 group *
Protocols
Directed broadcasts: enabled
RIP: enabled
OSPF: disabled
Per-packet-multipath: disabled
Ip classless: disabled
```

Listado del protocolo RIP:

```
Centrix Config>PROTOCOL RIP
RIP protocol user configuration
Centrix Conf RIP>LIST ALL
RIP: enable
RIP default origination: disabled
Options per interface address:
Interface:  0
    Address: 10.129.1.3
        RIP sending disabled on this interface.
        RIP receiving disabled on this interface.
        Authentication:..................No.
        Aggregation type:................Do not aggregate.
        Allow disconnected subnetted networks:..Yes
        Per interface additional cost: 0
Interface:  1
    Address: 0.0.0.1
        Send network routes:.............Yes
        Send subnetwork routes:..........Yes
        Send static routes:..............No
        Send direct routes:..............Yes
        Send default routes:.............No
        Poison reverse enabled:..........Yes
        Autonomous system label:.........0
        Sending compatibility:...........RIP2 Broadcast.
        Receive network routes:..........Yes
        Receive subnetwork routes:.......Yes
        Overwrite default routes:........No
        Overwrite static routes:.........No
        Receiving compatibility:.........RIP1 or RIP2.
        Authentication:..................No.
        Aggregation type:................Do not aggregate.
        Allow disconnected subnetted networks:..Yes
        Per interface additional cost: 0
Accept RIP updates always for:
[NONE]

RIP timers:
Periodic sending timer: 30
Route expire timer: 180
Route garbage timer: 120
Limit RIP: disabled.
```

b) Configuración CBRA (Equipo de Cliente)

Partimos de un CBRA correctamente configurado para conectarse a Internet, lo que se puede hacer fácilmente con el programa configurador en entornos Windows, y a partir de ahí construimos el resto de la configuración.

Creación del interfaz túnel:

```
*P 4
Config>ADD DEVICE TNIP
Added TNIP interface with num: 7

TNIP tunnel encapsulated type:[GRE]?
Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Config>
*RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuración del interfaz túnel:

```
*P 4

Config>NETWORK 7
-- IP Tunnel Net Config --
TNIP config>ENABLE TUNNEL
TNIP config>SET DESTINATION 10.129.1.3
```

Configuración del protocolo IP:

```
TNIP config>EXIT
Config>PROTOCOL IP
Internet protocol user configuration
Conf IP>ADD ADDRESS 7 0.0.0.7
Conf IP>ADD ROUTE 192.6.4.0 255.255.255.0 192.6.2.2 0
Conf IP>SET DEFAULT NETWORK-ROUTER 0.0.0.7 0
Conf IP>DELETE ACCESS-CONTROL 1
                                          Beg End  Beg   End   Beg  End
Type        Source           Destination  Pro Pro  SPrt  SPrt  DPrt DPrt
1 E         0.0.0.0/0          0.0.0.0/0  17  17     0 65535   520   520
Are you sure this is the record you want to delete(Yes/No)? y
Deleted
C_TUNNEL IP config>
```

Configuración del protocolo RIP:

```
Conf IP>EXIT
Config>PROTOCOL RIP
RIP protocol user configuration
Conf RIP>ENABLE RIP
Conf RIP>SET COMPATIBILITY 192.6.2.1 1 4
Conf RIP>SET COMPATIBILITY 192.168.253.1 1 4
Conf RIP>SET COMPATIBILITY 192.168.254.1 1 4
```

Configuración para callback por Internet (Excluyente con callback por Internet):

```
Config>NETWORK 5
Circuit Config
Circuit Config>ENCAPSULATOR

-- Interface PPP. Configuration --
PPP Config>ENABLE CALLBACK
PPP Config>EXIT
Circuit Config>EXIT
```

Configuración para callback por Internet (Excluyente con callback por Internet):

```
Config>NETWORK 3
ISDN Config
Config ISDN>SET LOCAL-ADDRESS
Local destination[]?Ninguna
Config ISDN>EXIT
Config>net 6
Circuit Config
Circuit Config>ENABLE INCOMING
Circuit Config>ENCAPSULATOR

-- Interface PPP. Configuration --
PPP Config>ENABLE CALLBACK
PPP Config>EXIT
Circuit Config>EXIT
```

Listado de interfaces:

```
Config>LIST DEVICES
Con    Ifc Type of interface                  CSR     CSR2  int
---      7 IP Tunnel                            0             0
LAN      0 Quicc Ethernet                F001600  F000C00   9E
WAN1     1 AT COM                        F001620  F000D00   9D
WAN1     2 PPP AT COM                           0             0
ISDN 1   3 ISDN                          F001640  F000E00   9C
ISDN 1   5 Channel B: PPP                       0             0
ISDN 2   4 ISDN                          F001660  F000F00   9B
ISDN 2   6 Channel B: PPP                       0             0
```

Listado del interfaz túnel:

```
TNIP config>LIST ALL
-- IP Tunnel Net Config --

Tunnel Mode: GRE
Tunnel Addresses
Source:       0.0.0.0
Destination: 10.129.1.3
Tunneling IP:   enable
TNIP config>SET PROTOCOL

-- GRE Config --
GRE config>LIST ALL
Cipher:         disabled
GRE Options GRE
End-to-End Checksumming:      disabled
Tunnel identification key:    disabled
Drop Out-of-Order Datagrams:  disabled
Proprietary sequence number:  disabled
GRE config>
```

Listado del protocolo IP:

```
Conf IP>LIST ALL
Interface addresses
IP addresses for each interface:
   intf  0   192.6.2.1        255.255.255.0    NETWORK broadcast,    fill 0
   intf  1                                     IP disabled on this interface
   intf  2                                     IP disabled on this interface
   intf  3                                     IP disabled on this interface
   intf  4                                     IP disabled on this interface
   intf  5   192.168.253.1    255.255.255.0    NETWORK broadcast,    fill 0
   intf  6                                     IP disabled on this interface
   intf  7   0.0.0.7          0.0.0.0          NETWORK broadcast,    fill 0
Routing
route to 10.0.0.0,255.0.0.0 via 192.168.253.2, cost 0
route to 192.6.4.0,255.255.255.0 via 192.6.2.2, cost 2
route to 0.0.0.0,0.0.0.0 via 0.0.0.7, cost 0
Protocols
Directed broadcasts: disabled
RIP: enabled
OSPF: disabled
Per-packet-multipath: disabled
Ip classless: disabled
```

Listado de los controles de acceso:

```
Conf IP>LIST ACCESS-CONTROL
Access Control is: enabled
List of access control records:
                                          Beg End  Beg   End   Beg  End
Type        Source           Destination  Pro Pro  SPrt  SPrt  DPrt DPrt
1 I         0.0.0.0/0          0.0.0.0/0   0 255     0 65535     0 65535
```

Listado del protocolo RIP:

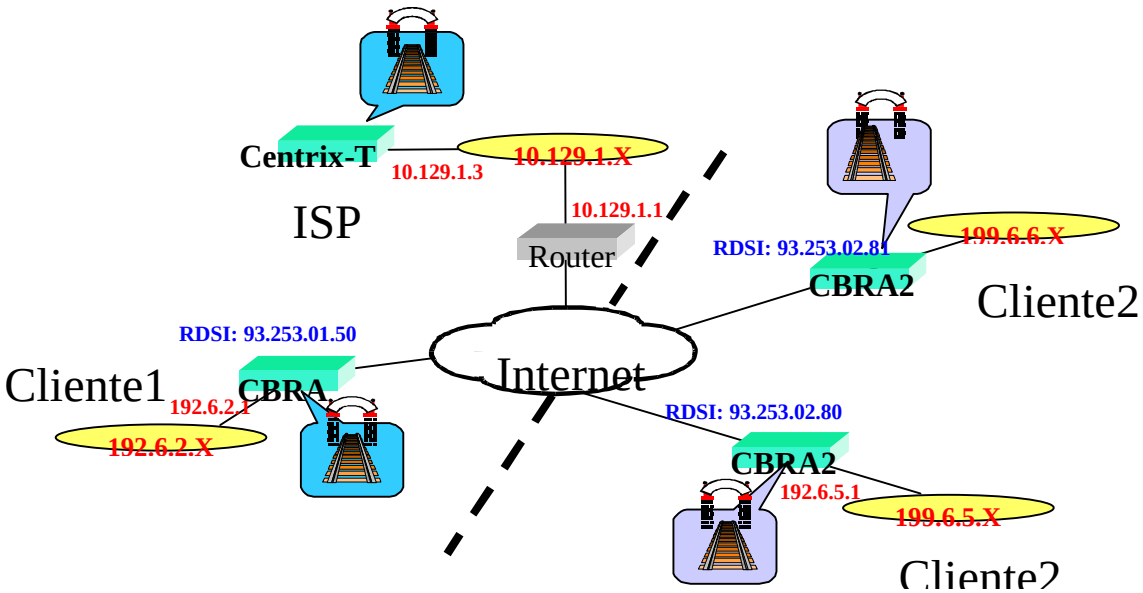
```
Config>PROTOCOL RIP
RIP protocol user configuration
RIP config>LIST ALL
RIP: enabled
RIP default origination: disabled
Options per interface address:
Interface:  0
    Address: 192.6.2.1
        RIP sending disabled on this interface.
        RIP receiving disabled on this interface.
        Authentication:.................No.
        Aggregation type:...............Do not aggregate.
        Allow disconnected subnetted networks:..Yes
        Per interface additional cost: 0
Interface:  5
    Address: 192.168.253.1
        RIP sending disabled on this interface.
        RIP receiving disabled on this interface.
        Authentication:.................No.
        Aggregation type:...............Do not aggregate.
        Allow disconnected subnetted networks:..Yes
        Per interface additional cost: 0
```

```
Interface:  7
    Address: 0.0.0.7
        Send network routes:.............Yes
        Send subnetwork routes:..........Yes
        Send static routes:..............No
        Send direct routes:..............Yes
        Send default routes:.............No
        Poison reverse enabled:..........Yes
        Autonomous system label:.........0
        Sending compatibility:...........RIP2 Broadcast.
        Receive network routes:..........Yes
        Receive subnetwork routes:.......Yes
        Overwrite default routes:........No
        Overwrite static routes:.........No
        Receiving compatibility:.........RIP1 or RIP2.
        Authentication:..................No.
        Aggregation type:................Do not aggregate.
        Allow disconnected subnetted networks:..Yes
        Per interface additional cost: 0
Accept RIP updates always for:
[NONE]

RIP timers:
Periodic sending timer: 30
Route expire timer: 180
Route garbage timer: 120
Limit RIP: disabled.
```

4.3. Ejemplo 2: Escenario 6 (Por Internet)

Partiendo del ejemplo anterior conectaremos mediante túneles dos redes locales de un tercera entidad, aislando totalmente este nuevo tráfico con el existente, es decir, estos nuevos túneles se verán entre ellos, pero no con los túneles antiguos ni la red del ISP.



a) Modificaciones necesarias en Centrix-T (Equipo de ISP)

Creación de los nuevos interfaces túnel:

```
Centrix *P 4

Centrix Config>ADD DEVICE TNIP
Added TNIP interface with num: 2
Centrix Config>ADD DEVICE TNIP
Added TNIP interface with num: 3

TNIP tunnel encapsulated type:[GRE]?
Centrix Config>SAVE
Save configuration [n]? y
Saving configuration...OK
Centrix Config>^p
Centrix *RESTART
Are you sure to restart the system?(Yes/No)? y
```

Configuración de los interfaces túnel:

```
Centrix *P 4

Centrix Config>NETWORK 2
-- IP Tunnel Net Config --
Centrix TNIP config>SET SOURCE 10.129.1.3
Centrix TNIP config>ENABLE TUNNEL
Centrix TNIP config>SET PROTOCOL

-- GRE Config --
Centrix GRE config>ENABLE KEY

Tunnel key: [0]? 333
Centrix GRE config>EXIT
Centrix TNIP config>EXIT
Centrix Config>NETWORK 3
-- IP Tunnel Net Config --
Centrix TNIP config>SET SOURCE 10.129.1.3
Centrix TNIP config>ENABLE TUNNEL
Centrix TNIP config>SET PROTOCOL

-- GRE Config --
Centrix GRE config>ENABLE KEY

Tunnel key: [0]? 333
Centrix GRE config>EXIT
Centrix TNIP config>EXIT
```

Configuración del protocolo IP:

```
Centrix TNIP config>EXIT
Centrix Config>PROTOCOL IP
Internet protocol user configuration
Centrix Conf IP>ADD ADDRESS 2 0.0.0.2
Centrix Conf IP>ADD ADDRESS 3 0.0.0.3

Centrix Conf IP>GROUP
Centrix GIP>ADD Client1 2
Centrix GIP>ADD Client1 3
Centrix GIP>EXIT

Centrix Conf IP>ADD ISDN 199.6.5.0 255.255.255.0 Client1
ISDN Number[]? 932530280
Cost[1]? 2
Centrix Conf IP>ADD ISDN 199.6.6.0 255.255.255.0 Client1
ISDN Number[]?932530281
Cost[1]? 2
```

Listado de interfaces:

```
Centrix Config>LIST DEVICE
Con    Ifc Type of interface                CSR     CSR2  int
---     1 Tunel IP                            0             0
---     2 Tunel IP                            0             0
---     3 Tunel IP                            0             0
---     4 Router->Node                        0             0
---     5 Node->Router                        0             0
LAN     0 Ethernet                      9000000             1C
WAN1    6 X25                           F001600  F000C00    9E
WAN2    7 X25                           F001620  F000D00    9D
ISDN 1  8 channel D: X.25               A000000             1B
ISDN 1 10 channel B: X.25               F001640  F000E00    9C
ISDN 2  9 channel D: X.25               A200000             1B
ISDN 2 11 channel B: X.25               F001660  F000F00    9B
```

Listado de los interfaces túnel:

```
Centrix Config>NETWORK 2

-- IP Tunnel Net Config --
Centrix TNIP config>LIST ALL
Tunnel Mode: GRE
Tunnel Addresses
Source: 10.129.1.3
Destination: 0.0.0.0
Tunneling IP:   enabled
Centrix TNIP config>SET PROTOCOL

-- GRE Config --
Centrix GRE config>LIST ALL
Cipher:         disabled
GRE Options GRE
End-to-End Checksumming:      disabled
Tunnel identification key:    enabled
--------------------> key:    333
Drop Out-of-Order Datagrams:  disabled
Proprietary sequence number:  disabled
Centrix GRE config>EXIT
```

```
Centrix TNIP config>EXIT
Centrix Config>net 3
-- IP Tunnel Net Config --
Centrix TNIP config>LIST ALL
Tunnel Mode: GRE
Tunnel Addresses
Source: 10.129.1.3
Destination: 0.0.0.0
Tunneling IP:   enabled
Centrix TNIP config>SET PROTOCOL
-- GRE Config --
Centrix GRE config>LIST ALL
Cipher:         disabled
GRE Options GRE
End-to-End Checksumming:      disabled
Tunnel identification key:    enabled
--------------------> key:    333
Drop Out-of-Order Datagrams:  disabled
Proprietary sequence number:  disabled
```

Listado del protocolo IP:

```
Centrix Conf IP>LIST ALL
Interface addresses
IP addresses for each interface:
   intf  0 (       *)  10.129.1.3     255.255.255.0   NETWORK broadcast,    fill 0
   intf  1 (       *)     0.0.0.1           0.0.0.0   NETWORK broadcast,    fill 0
   intf  2 (Cliente1)     0.0.0.2           0.0.0.0   NETWORK broadcast,    fill 0
   intf  3 (Cliente1)     0.0.0.3           0.0.0.0   NETWORK broadcast,    fill 0
   intf  4                                            IP disabled on this interface
Routing
route to 192.6.1.0,255.255.255.0 via 10.219.1.2, cost 1 *
route to 0.0.0.0,0.0.0.0 via 10.129.1.1, cost 0 *
route to 199.6.5.0,255.255.255.0 via ISDN 932530150 cost 2 Client1
route to 199.6.6.0,255.255.255.0 via ISDN 932530280 cost 2 Client1
Protocols
Directed broadcasts: enabled
RIP: enabled
OSPF: disabled
Per-packet-multipath: disabled
Ip classless: disabled
```

b) Configuración necesaria en CBRAs (Equipo de Cliente1)

La configuración de los equipos de los clientes no sufren variaciones importantes por el hecho de trabajar en escenario 5 o 6, y debido a que el camino por defecto es el túnel no es necesaria ninguna configuración adicional excepto el Key. Por tanto la configuración de los equipos para este nuevo cliente es la expuesta en el apartado 4.2.b más el identificador GRE:

```
*P 4

Config>NETWORK 2
-- IP Tunnel Net Config --
TNIP config>SET PROTOCOL

-- GRE Config --
GRE config>ENABLE KEY 333
```

5. Eventos

Debido a la reutilización de los túneles dinámicos y el hecho de "despertar" al cliente, se han añadido los siguientes eventos:

El listado de eventos añadidos para el protocolo TNIP es el siguiente:

TNIP.021

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.021 Set up tn int *num_interfaz* typ *interfaz_id* (*dirección_ip_origen->dirección_ip_destino*)

Sintaxis Larga:

TNIP.021 Interface *num_interfaz* sets up a tunnel type *interfaz_id* source address *dirección_ip_origen* and destination *dirección_ip_destino*

Descripción:

Se ha usado uno de los túneles dinámicos libres para crear un nuevo túnel.

TNIP.022

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.022 Err tn with no routes rel, int *num_interfaz* type *interfaz_id*

Sintaxis Larga:

TNIP.022 Error tunnel with no routes release, interface *num_interfaz* type *interfaz_id*

Descripción:

En un túnel dinámico establecido no se han recibido rutas por RIP ni tiene ninguna ruta estática por lo que se libera para poder ser utilizado de nuevo.

TNIP.023

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

TNIP.023 Rele tn int *num_interfaz* typ *interfaz_id* Rx idem IP *dirección_ip*

Sintaxis Larga:

TNIP.023 Release tunnel interface *num_interfaz* type *interfaz_id* set up another tunnel with the same address IP *dirección_ip*

Descripción:

TNIP.023 Se ha creado un nuevo túnel con una dirección IP de un túnel que ya existía y aun no se habían dado las condiciones de liberación y ahora es el momento de liberarlo

TNIP.024

Nivel: Error externo anormal, ERROR-AE/UE-ERROR

Sintaxis Corta:

TNIP.024 Err loop in tunnel, int *num_interfaz* tipo *interfaz_id*

Sintaxis Larga:

TNIP.024 Error loop in tunnel, interface *num_interfaz* type *interfaz_id*

Descripción:

TNIP.024 Se ha detectado en un túnel que se intenta encapsular un paquete que volverá al túnel provocando un bucle infinito.

El listado de eventos añadidos para el protocolo RIP es el siguiente:

RIP.029

Nivel: Traza por paquete, TRAZA-P/P-TRACE

Sintaxis Corta:

RIP.029 Tn nt int *num_interfaz* no routes.

Sintaxis Larga:

RIP.029 Tunnel interface *num_interfaz* released, no routes.

Descripción:

RIP.029 Cuando se borran rutas aprendidas por RIP se comprueban si estas eran de un túnel y si no quedan rutas a donde ir por el túnel se libera.

6. Monitorización

Además de los estadísticos de los túneles no dinámicos vistos en el capítulo 3, existen estadísticos concretos para los túneles dinámicos:

6.1. Visualización del prompt de monitorización

En este apartado se describen los comandos de monitorización del interfaz TNIP. Para acceder al entorno de monitorización de TNIP, se deben seguir los siguientes pasos:

1. En el prompt GESTCON (*), teclee **PROCESS 3** o (**P 3**).

2. En el prompt MONITOR (+), teclee **NETWORK #,** donde # es un número de interfaz correspondiente a un túnel IP.

3. En el prompt de monitorización de Túnel IP (TNIP>) teclee los comandos de control deseado.

Ejemplo:

```
*P 3
+NETWORK 2
TNIP protocol monitor
TNIP>
```

6.2. Comandos de Monitorización

Para visualizar los estadísticos del interfaz teclear desde el menú de consola:

Comando	Función
? (AYUDA)	Lista los comandos u opciones disponibles
LIST	Muestra los estadísticos del interfaz túnel IP
EXIT	Sale del proceso de monitorización de TNIP

Las letras en **negrita** son el número mínimo de caracteres que hay que teclear para que el comando sea efectivo

a) ? (AYUDA)

Utilizar el comando **?** (AYUDA) para listar los comandos disponibles en el prompt en el que se esté trabajando. También se puede usar este comando a continuación de un comando específico para listar opciones disponibles.

Sintaxis:

```
TNIP>?
```

Ejemplo:

```
TNIP >?
LIST
EXIT
TNIP config>
```

b) LIST

Se utiliza para listar los estadísticos del interfaz túnel IP.

Sintaxis:

```
TNIP>LIST ?
STATE
```

STATE

Muestra el estado de los estadísticos del túnel. Estos estadísticos son para túneles dinámicos.

Ejemplo:

```
TNIP>LIST STATE

Int Source IP      Dest. IP        Start Time  Connections Discon.err  Loop
--- ---------      ----------      ----------  ----------  ----------  ----
 1 195.80.0.2      195.78.0.3         09:10        113            1       0
 2 195.80.0.2      192.0.56.1         13:15         28            0       0
 3 10.125.0.2      10.4.123.3         12:10         36            0       0
```

Start Time: hora de inicio de la última conexión.
Connections: número de conexiones desde el último arranque del router.
Discon.err: numero de desconexiones por no recibir rutas a través de dicho túnel.
Loop: informa si ha habido un bucle.