Router Teldat

Bridge

Doc. *DM517* Rev. *8.40*
Octubre, 2000

ÍNDICE

Capítulo 1 Fundamentos de Bridging 1
1. Relativo a Bridges 2
2. Bridges y Routers 3
2.1. Conexiones Router 3
2.2. Conexiones Bridge 3
2.3. Ventajas del Bridging 3
2.4. Interfaces de Bridging 4
3. Métodos de Bridging 5
4. Cómo funcionan los bridges 6
4.1. Ejemplo 1: Bridge local que conecta dos LANs 6
4.2. Ejemplo 2: Bridging remoto en una conexión en serie 6
4.3. Formatos de la trama MAC del Bridge 7
4.4. Tramas MAC CSMA/CD (Ethernet) 8
4.5. Tramas MAC Token Ring 9
4.6. Tramas Ethernet Pseudo-serie 9
Capítulo 2 Utilizando Bridge Transparente 11
1. Relativo a STB 12
2. Los Routers y STB 13
3. Requisitos de la Red STB 14
4. Habilitar STB 15
5. Cómo Funciona el STB 16
6. Forma del Spanning Tree 17
7. Bridges de Spanning Tree y Traducción del Formato del Paquete Ethernet 20
Capítulo 3 Utilización del Bridging de Encaminamiento de Origen (Source Route Bridging, SRB) 21
1. Relativo a SRB 22
2. Activar SRB 23
3. Cómo funciona el SRB 24
4. Formatos de Trama SRB 25
5. La Opción Explorador Spanning Tree 28
5.1. Simular una Red Spanning Tree 28
6. SRB y Frame Relay 29
Capítulo 4 Utilización de la Conversión de Bridge de Encaminamiento de Origen Transparente (Route-Transparent Bridge, SR-TB) 30
1. Relativo a la Conversión SR-TB 31
2. Activar el SR-TB 32
3. Cómo funciona la Conversión SR-TB 33
4. Operaciones Específicas de Source Routing y Bridging Transparente 34
4.1. Bridging SR-TB: Ejemplos 35
a) Ejemplo 1: Trama enviada desde el equipo final A al equipo final B 36
b) Ejemplo 2: Trama enviada desde el equipo final A al equipo final C 36
c) Ejemplo 3: Trama enviada desde el equipo final C al equipo final D 37
d) Ejemplo 4: Trama enviada desde el equipo final C al equipo final A 37
5. SR-TB y Frame Relay 38
Capítulo 5 Diversas Características de Bridge 39
1. Filtrado del Protocolo 40

2. Característica IBM RT para Tráfico SNA 41
3. Encapsulación UB de Tramas XNS 42
4. Opciones de Protocolo de Spanning Tree Múltiple 43
4.1. Problemas del Protocolo de Spanning Tree Múltiple 43
4.2. Ampliación del STP 43
Capítulo 6 Utilización del Tunneling IP 45
1. Túnel de Bridging IP 46
1.1. Encapsulación y OSPF 47
Capítulo 7 Configuración ASRT 48
1. Visualización de la Configuración ASRT 49
2. Comandos de Configuración ASRT 50
2.1. ? (HELP) 50
2.2. ADD 51
a) ADD ADDRESS addr-value 51
b) ADD MAPPING 55
c) ADD PROT-FILTER 56
d) ADD PORT 58
e) ADD TUNNEL 58
2.3. BAN 59
2.4. CHANGE 59
a) CHANGE BRIDGE 59
b) CHANGE SEGMENT 60
2.5. DELETE 60
a) DELETE ADDRESS 60
b) DELETE MAPPING 60
- DELETE MAPPING DSAP 61
- DELETE MAPPING ETHER 61
- DELETE MAPPING SNAP 61

c) DELETE PROT-FILTER 61
- DELETE PROT-FILTER DSAP 62
- DELETE PROT-FILTER ETHER 62
- DELETE PROT-FILTER SNAP 62

d) DELETE PORT 62
2.6. DISABLE 63
a) DISABLE BRIDGE 63
b) DISABLE DLS 64
c) DISABLE DUPLICATE 64
- DISABLE DUPLICATE STE 64
- DISABLE DUPLICATE TSF 64

d) DISABLE ETHERTYPE-IBMRT-PC 65
e) DISABLE FA-GA-MAPPING 65
f) DISABLE IBM8209_SPANNING_TREE 65
g) DISABLE SOURCE-ROUTING 65
h) DISABLE SR-TB-CONVERSION 66
i) DISABLE STP 66
j) DISABLE SPANNING TREE-EXPLORER 66
k) DISABLE TRANSPARENT 66
l) DISABLE TREE 66
m) DISABLE UB-ENCAPSULATION 67
2.7. ENABLE 67
a) ENABLE BRIDGE 68
b) ENABLE DLS 68
c) ENABLE DUPLICATE 68
- ENABLE DUPLICATE BOTH 69
- ENABLE DUPLICATE STE 69
- ENABLE DUPLICATE TSF 69

- ENABLE DUPLICATE PORT 69

d) ENABLE ETHERTYPE-IBMRT-PC 69
e) ENABLE FA-GA-MAPPING 70
f) ENABLE IBM8209_SPANNING_TREE 70
g) ENABLE SOURCE-ROUTING 70
h) ENABLE SR-TB-CONVERSION 71
i) ENABLE SPANNING-TREE-EXPLORER 71
j) ENABLE STP 71
k) ENABLE TRANSPARENT 72
l) ENABLE TREE 72
m) ENABLE UB-ENCAPSULATION 72

2.8. LIST 72

a) LIST ADDRESS 73
b) LIST BRIDGE 74
c) LIST FILTERING 75
d) LIST MAPPING 76

- LIST MAPPING DSAP 76
- LIST MAPPING ETHER 76
- LIST MAPPING SNAP 76

e) LIST PERMANENT 76
f) LIST PORT 77
g) LIST PROT-FILTER 78
h) LIST PROTOCOL 78
i) LIST RANGE 79

2.9. NETBIOS 80
2.10. NAME-CACHING 80

a) ? AYUDA 81
b) DISABLE 81

- DISABLE ADD-NAME-FILTERING 81
- DISABLE NAME-CACHING 81

c) ENABLE 81

- ENABLE ADD-NAME-FILTERING 82
- ENABLE NAME-CACHING 82

d) LIST 82
e) PORT 82
f) TIMER 83

- TIMER ADD-NAME 83
- TIMER ENTRY 83
- TIMER SERVER-RESPONSE 84

g) EXIT 84

2.11. SET 84

a) SET AGE 85
b) SET BRIDGE 85
c) SET FILTERING 86
d) SET LF-BIT-INTERPRETATION 86

- SET LF-BIT-INTERPRETATION BASIC 86
- SET LF-BIT-INTERPRETATION EXTENDED 86

e) SET MAXIMUM-PACKET-SIZE 87
f) SET PORT 87

- SET PORT BLOCK 87
- SET PORT DISABLE 87

g) SET PROTOCOL 88

- SET PROTOCOL BRIDGE 88
- SET PROTOCOL PORT 88

h) SET ROUTE-DESCRIPTOR-LIMIT 89

- SET ROUTE-DESCRIPTOR-LIMIT ARE 89
- SET ROUTE-DESCRIPTOR-LIMIT STE 89

2.12. EXIT 90
Capítulo 8 Monitorización ASRT 91
1. Visualización de la Monitorización ASRT 92
2. Comandos de Monitorización ASRT 93
2.1. ? (AYUDA) 93
2.2. ADD 94
a) ADD DESTINATION-ADDRESS-FILTER 94
b) ADD STATIC-ENTRY 94
2.3. BAN 94
2.4. CACHE 95
2.5. DELETE 96
2.6. FLIP 96
2.7. LIST 96
a) LIST ADAPTIVE 97
- LIST ADAPTIVE CONFIG 97
- LIST ADAPTIVE COUNTERS 98
- LIST ADAPTIVE DATABASE 98

b) LIST BRIDGE 100
c) LIST CONVERSION 101
- LIST CONVERSION ALL 101
- LIST CONVERSIÓN ETHERTYPE 101
- LIST CONVERSIÓN SAP 102
- LIST CONVERSIÓN SNAP 102

d) LIST DATABASE 102
- LIST DATABASE ALL-PORTS 103
- LIST DATABASE DYNAMIC 104
- LIST DATABASE LOCAL 105
- LIST DATABASE PERMANENT 105
- LIST DATABASE PORT 105
- LIST DATABASE RANGE 106
- LIST DATABASE STATIC 106

e) LIST FILTERING 107
- LIST FILTERING ALL 107
- LIST FILTERING ETHERTYPE 107
- LIST FILTERING SAP 108
- LIST FILTERING SNAP 108

f) LIST PORT 108
g) LIST SOURCE-ROUTING 109
- LIST SOURCE-ROUTING CONFIGURATION 109
- LIST SOURCE ROUTING COUNTERS 110
- LIST SOURCE-ROUTING STATE 112

h) LIST SPANNING-TREE-PROTOCOL 112
- LIST SPANNING-TREE-PROTOCOL CONFIGURATION 113
- LIST SPANNING-TREE-PROTOCOL COUNTERS 113
- LIST SPANNING-TREE-PROTOCOL STATE 113
- LIST SPANNING-TREE-PROTOCOL TREE 114

i) LIST TRANSPARENT 114
- LIST TRANSPARENT CONFIGURATION 114
- LIST TRANSPARENT COUNTERS 114
- LIST TRANSPARENT STATE 115

j) LIST TUNNEL 115
- LIST TUNNEL BRIDGES 115
- LIST TUNNEL CONFIG 116

2.8. NETBIOS 116
2.9. NAME-CACHING 117

a) ? (AYUDA) *117*
b) LIST *117*
- LIST ADD-NAMES 117
- LIST CACHE 118

c) PORT *119*
- LIST 119
- EXIT 120

d) EXIT *120*
2.10. EXIT 120

Capítulo 9 Utilización de NetBIOS 122
1. Relativo a NetBIOS 123
1.1. Nombres NetBIOS 123
1.2. Resolución del Conflicto de Nombre NetBIOS 123
1.3. Procedimiento de Sesión de Sistema NetBIOS 123
2. Reducir el Tráfico NetBIOS 125
2.1. Filtrado del Tipo de Trama 125
2.2. Configuración del Filtrado del Tipo de Trama 126
2.3. Filtrado de Trama Duplicada 126
2.4. Cómo Duplicar Trabajos de Filtrado de Trama 127
2.5. Configurar el Filtrado de Trama Duplicada 128
2.6. Filtrado de trama de respuesta 129
2.7. Filtrado de Trama de Respuesta para DLSw 129
2.8. Name caching y Route caching NetBIOS 130
2.9. Activación del Caching 130
2.10. Tipos de Entradas de Name caching 130
2.11. Añadir Entradas de Name caching 131
2.12. Establecer Parámetro de Cache 131
2.13. Visualización de las Entradas de Cache 132
2.14. Filtrado de Nombre NetBIOS 132
2.15. Filtrado de Byte NetBIOS 133

Capítulo 10 Comandos de Filtrado y de Cache NetBIOS 134
1. Relativo a los comandos de Configuración y Monitorización NetBIOS 135
2. Configuración del Filtrado y Cache NetBIOS 136
2.1. Configuración de NetBIOS para DLSw 136
2.2. Añadir entradas de cache de nombre para vecinos DLSw 136
2.3. Abrir NetBIOS SAPs 136
2.4. Establecer una Prioridad para SNA y Sesiones NetBIOS 137
2.5. Establecer el tamaño máximo de trama NetBIOS 137
2.6. Establecer la distribución de memoria para tramas NetBIOS UI 138
3. Comandos de Configuración NetBIOS 139
3.1. Visualización del prompt de Configuración NetBIOS 139
3.2. ? (AYUDA) 140
3.3. ADD 140
a) ADD CACHE-ENTRY *140*
3.4. DELETE 141
3.5. DISABLE 141
a) DISABLE DUPLICATE-FILTERING *141*
b) DISABLE ROUTE-CACHING *142*
3.6. ENABLE 142
a) ENABLE DUPLICATE-FILTERING *142*
b) ENABLE ROUTE-CACHING *143*
3.7. LIST 143
a) LIST CACHE *143*
- LIST CACHE ALL 143
- LIST CACHE ENTRY-NUMBER 144
- LIST CACHE IP-ADDRESS 144

- LIST CACHE NAME 144

b) LIST FILTERS 145

- LIST FILTERS ALL 145
- LIST FILTERS BRIDGE 146
- LIST FILTERS DLSW 146

c) LIST GENERAL 146

3.8. SET 147

a) SET CACHE-PARMS 147

b) SET FILTERS 149

- SET FILTERS BRIDGE 149
- SET FILTERS BYTE 149
- SET FILTERS DLSW 150
- SET FILTERS NAME 150

c) SET GENERAL 150

3.9. EXIT 152

4. Comandos de Monitorización NetBIOS 153

4.1. Visualización del prompt de Monitorización NetBIOS 153

4.2. ? (AYUDA) 154

4.3. ADD 154

a) ADD CACHE ENTRY 154

4.4. DELETE 155

4.5. DISABLE 155

a) DISABLE DUPLICATE-FILTERING 156

b) DISABLE ROUTE-CACHING 156

4.6. ENABLE 156

a) ENABLE DUPLICATE-FILTERING 156

b) ENABLE ROUTE-CACHING 157

4.7. LIST 157

a) LIST CACHE 157

- LIST CACHE ACTIVE 158
- LIST CACHE CONFIG 158
- LIST CACHE GROUP 158
- LIST CACHE LOCAL 159
- LIST CACHE NAME 159
- LIST CACHE REMOTE 162
- LIST CACHE UNKNOWN 162

b) LIST FILTERS 163

- LIST FILTERS ALL 163
- LIST FILTERS BRIDGE 163
- LIST FILTERS DLSW 164

c) LIST GENERAL 164

d) LIST STATISTICS 165

- LIST STATISTICS CACHE 165
- LIST STATISTICS FRAMES 165
- LIST STATISTICS GENERAL 166

4.8. SET 167

a) SET CACHE-PARMS 167

b) SET FILTERS 168

- SET FILTERS BRIDGE 169
- SET FILTERS BYTE 169
- SET FILTERS DLSW 169
- SET FILTERS NAME 170

c) SET GENERAL 170

4.9. EXIT 171

Capítulo 11 Configuración y Monitorización de Filtrado de Nombre y Byte NetBIOS 172

1. Visualización de los Prompts de Filtrado NetBIOS 173
2. Establecimiento de Filtros de Nombre y Byte NetBIOS 174
3. Comandos de Configuración de Filtros de Nombre y Byte NetBIOS 180
3.1. ? (AYUDA) 180
3.2. CREATE 181
a) CREATE BYTE-FILTER-LIST 181
b) CREATE NAME-FILTER-LIST 181
3.3. DELETE 181
a) DELETE FILTER 182
- DELETE FILTER INPUT 182
- DELETE FILTER OUTPUT 182

b) DELETE BYTE-FILTER-LIST 182
c) DELETE NAME-FILTER-LIST 183
3.4. DISABLE 183
3.5. ENABLE 183
3.6. FILTER-ON 183
a) FILTER-ON INPUT 184
b) FILTER-ON OUTPUT 184
3.7. LIST 185
3.8. UPDATE 186
3.9. EXIT 186
4. Comandos de Monitorización de Filtros de Nombre y Byte NetBIOS 187
4.1. ? (AYUDA) 187
4.2. LIST 187
a) LIST BYTE-FILTER-LISTS 188
b) LIST NAME-FILTER-LISTS 188
c) LIST FILTERS 188
4.3. EXIT 189
5. Comandos de Actualización de la Lista de Filtro de Byte 190
6. Actualizar los Comandos de la Lista de filtro de nombre 193

Capítulo 12 Utilización del Filtrado MAC 197

1. Relativo al Filtrado MAC 198
1.1. Filtrado MAC y Tráfico DLSw 198
2. Utilización de los Parámetros de filtrado MAC 199
2.1. Parámetros de Elemento de filtro 199
2.2. Parámetros de Lista de Filtro 199
2.3 Parámetros de Filtro 200
3. Utilización de las Etiquetas de Filtrado MAC 201

Capítulo 13 Configuración y Monitorización del Filtrado MAC 202

1. Acceso a los Prompts de Filtrado MAC 203
2. Comandos de Configuración de Filtrado MAC 204
2.1. ? (AYUDA) 204
2.2. ATTACH 205
2.3. CREATE 205
a) CREATE LIST 205
b) CREATE FILTER 206
2.4. DEFAULT 206
a) DEFAULT EXCLUDE 206
b) DEFAULT INCLUDE 206
c) DEFAULT TAG 207
2.5. DELETE 207
a) DELETE LIST 207
b) DELETE FILTER 208
2.6. DETACH 208
2.7. DISABLE 208

a) *DISABLE ALL* *208*
b) *DISABLE FILTER* *209*
2.8. ENABLE 209
a) *ENABLE ALL* *209*
b) *ENABLE FILTER* *209*
2.9. LIST 209
a) *LIST ALL* *210*
b) *LIST FILTER* *210*
2.10. MOVE 211
2.11. REINIT 211
2.12. SET-CACHE 212
2.13. UPDATE 212
2.14. EXIT 212
3. Comandos de Monitorización de Filtrado MAC 214
3.1. ? (AYUDA) 214
3.2. CLEAR 214
a) *CLEAR ALL* *215*
b) *CLEAR FILTER* *215*
3.3. DISABLE 215
a) *DISABLE ALL* *215*
b) *DISABLE FILTER* *216*
3.4. ENABLE 216
a) *ENABLE ALL* *216*
b) *ENABLE FILTER* *216*
3.5. LIST 217
a) *LIST ALL* *217*
b) *LIST FILTER* *217*
3.6. REINIT 218
3.7. EXIT 218
4. Comandos de Actualización del Filtrado MAC 219
4.1. ? AYUDA 219
4.2. ADD 220
a) *ADD SOURCE* *220*
b) *ADD DESTINATION* *220*
4.3. DELETE 221
4.4. LIST 221
a) *LIST CANONICAL* *221*
b) *LIST NON-CANONICAL* *222*
4.5. MOVE 222
4.6. SET-ACTION 222
a) *SET-ACTION INCLUDE* *223*
b) *SET-ACTION EXCLUDE* *223*
c) *SET-ACTION TAG* *223*
4.7. EXIT 223

Capítulo 14 Utilización del Threading de Protocolo a través de una Red de Bridge . 224

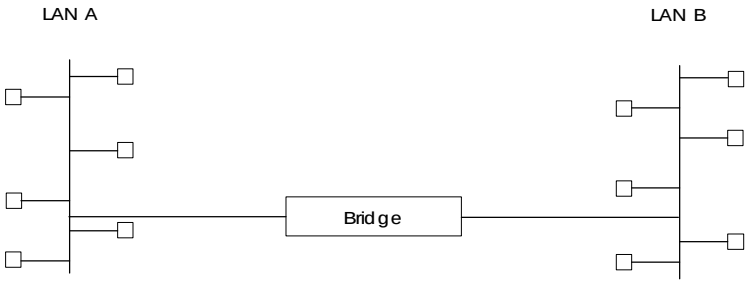
1. Relativo al Threading 225
2. Threading IP con ARP 226
3. Threading DNA 227
4. Threading Apollo 228
5. Threading IPX 229
6. Threading AppleTalk 1 y 2 230

Capítulo 1
Fundamentos de Bridging

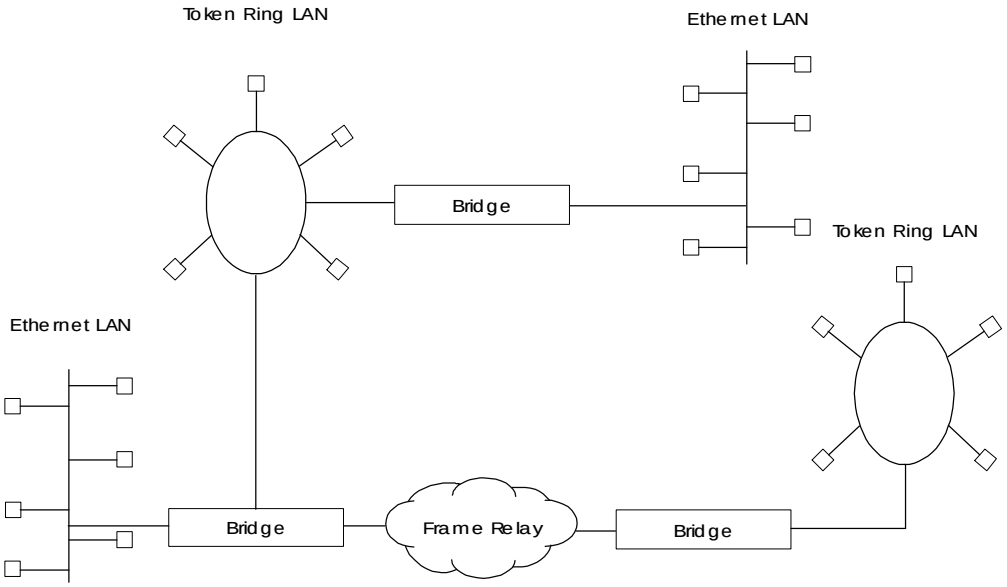
1. Relativo a Bridges

Un bridge es un dispositivo que une dos o más Redes de Área Local (*Local Area Networks, LANs*). El bridge acepta tramas de información de cada red conectada y luego decide si reenviar cada trama basándose en tramas del tipo *Medium Access Control (MAC)*.

Los *bridges* se pueden utilizar para conectar redes homogéneas o heterogéneas. El término homogéneo significa que las redes conectadas utilizan el mismo sistema de *bridging* y los mismos tipos de soporte. El término heterogéneo significa que las redes conectadas mezclan distintos sistemas de *bridging* y tipos de soporte, lo que ofrece más opciones de configuración.



Bridge simple que conecta dos LANs Ethernet Homogeneas



Bridge complejo que conecta LANs Heterogeneas

Figura 1-1. Configuraciones de Bridging homogéneas y heterogéneas

2. Bridges y Routers

Los *bridges* y *routers* conectan segmentos de redes. Sin embargo, cada dispositivo utiliza un sistema diferente para establecer y mantener las conexiones *LAN* a *LAN*. Los *routers* conectan *LANs* en el nivel 3 (nivel de red) del modelo *OSI* mientras que los *bridges* lo hacen en el nivel 2 (nivel de conexión de datos).

2.1. Conexiones Router

Los *routers* conectan *LANs* que estén alejadas y que sean distintas de la forma más inteligente al usar los protocolos de nivel de red. Se recomienda utilizar *routers* para conectar redes extensas debido a que a nivel de red se tiene más información acerca de la topología de red.

Se debe encaminar cuando un protocolo es encaminable. Por ejemplo, se debe encaminar cuando se mezclan *Ethernet* y *Token Ring* con protocolos que usan información *MAC* en los niveles superiores.

2.2. Conexiones Bridge

Los *bridges* conectan *LANs* mediante una conexión física. Esta conexión es prácticamente transparente para el equipo conectado a la red.

Un *bridge* actúa como un repetidor de tramas entre redes en el nivel de conexión de datos. El nivel de conexión de datos mantiene esquemas de direccionamiento físico, disciplina de línea, información de topología, notificación de errores, control de flujo y entrega ordenada de tramas de datos. El principal servicio que proporciona el nivel de enlace al nivel superior es la detección de errores y el control de los mismos. Con un protocolo de nivel de enlace completamente funcional, el nivel inmediatamente superior puede asumir una transmisión prácticamente sin errores en la conexión.

Se debe usar el *bridge* cuando el protocolo es no encaminable, es decir, no lleva nivel de red.

2.3. Ventajas del Bridging

El aislamiento de los protocolos de los niveles superiores es una de las ventajas del *bridging*. Debido a que los *bridges* funcionan en el nivel de conexión de datos, no se ocupan de mirar la información del protocolo de los niveles superiores. Esto proporciona cargas de proceso más bajas y una comunicación rápida del tráfico del protocolo del nivel de red.

Los *bridges* también pueden filtrar tramas teniendo en cuenta los campos del nivel 2. Esto significa que el bridge puede configurarse para aceptar y enviar únicamente tramas de cierto tipo o las que se originen en una red en concreto. Esta capacidad para configurar filtros es muy útil para mantener un flujo de tráfico efectivo.

Los *bridges* tienen muchas ventajas a la hora de dividir redes extensas en segmentos razonables. Las ventajas del *bridging* en redes extensas se pueden resumir en los siguientes puntos:

- El *bridging* permite aislar áreas específicas de la red, dándoles una menor exposición a los problemas de la red mayor.
- El filtrado permite regular la cantidad de tráfico que se envía a determinados segmentos.
- Los bridges permiten la comunicación entre un mayor número de dispositivos de internetworking de los que se mantendrían con una única LAN conectada a un bridge.
- El bridging elimina la limitación de nodos. El tráfico local de la red no se pasa a todas las demás redes conectadas.

- Los bridges prolongan la extensión de conexión de una LAN permitiendo la conexión de estaciones de trabajo que se encuentran alejadas.

2.4. Interfaces de Bridging

Las interfaces que se pueden encontrar en un *bridge* incluyen combinaciones de una o más de las siguientes:

- Ethernet
- Token Ring
- Línea serie (en la que la conexión de datos es serie, PPP y Frame Relay)

Las interfaces Ethernet soportan el *bridging* transparente.

La interfaz Token Ring permite el *source-routing* y el *bridging* transparente.

La línea serie proporciona una conectividad punto a punto al tráfico transparente y al *source-routing*. Es importante señalar que una configuración bridge en una línea serie tiene que ser consistente en ambos extremos. Esto significa que se tienen que configurar ambos extremos de la siguiente manera:

- Transparente a transparente
- *Source-routing* a *source-routing*
- *Source-routing*/transparente a *source-routing*/transparente

Si quiere mezclar tipos de *bridging* lo mejor es configurar la línea serie para ambos métodos de *bridging*. Asegúrese de que los *bridging routers* son consistentes en su método de bridging o en su encaminamiento de ciertos protocolos.

3. Métodos de Bridging

El *bridging* consta de dos protocolos o metodologías puras: Source Transparent Bridging (STB) y Source Route Bridging (SRB).

- STB es un método de *bridging* fundamentalmente para entornos de Ethernet en los que los *bridges* diseñan automáticamente tablas de *bridging* y actualizan dichas tablas en respuesta a una topología cambiante.
- SRB es un método de *bridging* únicamente para entornos Token Ring en los que el equipo origen determina la ruta a seguir por la trama e incluye la información de encaminamiento, o camino que construyen los *routers* que participan en el SRB.

Se puede utilizar el STB y el SRB solos o en combinación dependiendo de sus necesidades sin tener en cuenta el soporte o la topología de red. Estas combinaciones son Source Route Transparent Bridging (SRT), Source Route-Transparent Bridging (SR-TB Conversion) y Adaptive Source Route Transparent Bridging (ASRT).

- El SRT es un método de *bridging* tanto para tramas de *source routing* como para tramas transparentes basadas en el Route Information Indicator (RII). Puede considerarse como dos *bridges* en uno.
- El SR-TB es un método de *bridging* entre dominios SRB y STB. Esto lo consigue mediante un proceso de transformación entre las dos tecnologías de *bridging* (IBM 8209).
- El ASRT es una mejora de TELDAT de la tecnología de *bridging* SRT. Combina la funcionalidad del SRT y del SR-TB. Permite que todos los equipos finales que están en un entorno complejo de *bridge* se comuniquen sin las limitaciones corrientes. Se mantienen tablas para equipos finales SRB y STB de forma que se pueden utilizar *bridges* o transformar según las necesidades.

> ***Nota: Tanto el SRT como el ASRT requieren memorias CAM (Content Adressable Memory) para utilizar* bridges *de forma transparente sobre Token Ring en plataformas CNX.***

La decisión de elegir un método de *bridging* sobre los otros depende de la topología de la red y de las aplicaciones utilizadas en los equipos finales.

4. Cómo funcionan los bridges

Los bridges funcionan en el nivel MAC. De acuerdo con el estándar de LAN IEEE 802, todas las direcciones de equipos se especifican en el nivel MAC. Los siguientes ejemplos muestran como funciona un bridge en el nivel MAC.

4.1. Ejemplo 1: Bridge local que conecta dos LANs

La Figura 1-2 muestran un modelo de *bridge* de dos puertos que conecta equipos finales en dos LANs separados. En este ejemplo el bridge local conecta LANs con niveles LLC y MAC idénticos (por ejemplo dos LANs Token Rings).

El *bridge* captura tramas MAC cuya dirección de destino no está en la LAN local y las envía a la LAN de destino adecuada. Durante este proceso, hay un diálogo entre el par de entidades LLC en los dos equipos finales. Arquitectónicamente el bridge no necesita contener un nivel LLC ya que la función del nivel LLC es únicamente transmitir tramas MAC.

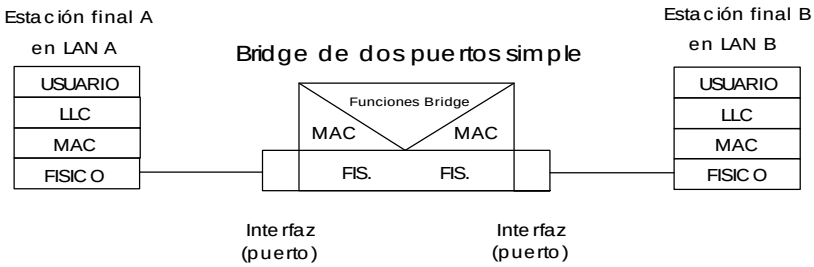


Figura 1-2. Bridge de dos extremos que conectan dos LANs

4.2. Ejemplo 2: Bridging remoto en una conexión en serie

Las Figura 1-3 muestran un par de *bridges* conectados mediante una conexión en serie. Estos *bridges* remotos conectan LANs con niveles LLC y MAC idénticos (por ejemplo dos LANs Token Rings).

El *bridge* A captura una trama MAC cuya dirección de destino no está en la LAN local y después la envía al *bridge* B a través de una línea serie utilizando la encapsulación de la línea serie adecuada para identificar el tipo de trama *bridge*. El *bridge* B remoto desencapsula la cabecera de la línea serie y reenvía la trama a las LANs locales. Durante este proceso hay un diálogo entre las entidades LLC equivalentes de los dos equipos finales.

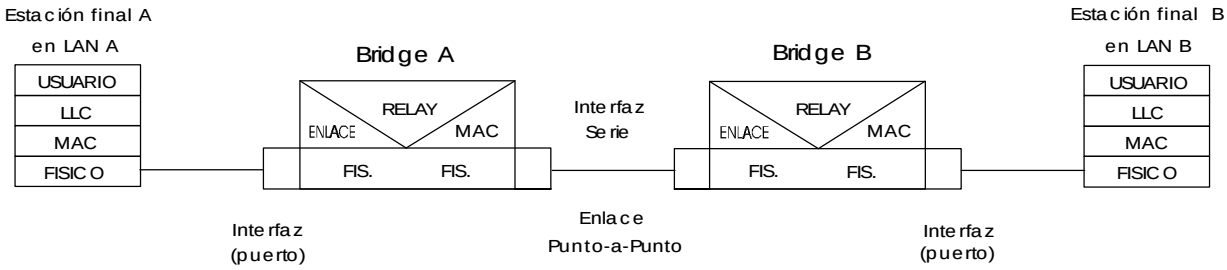


Figura 1-3. *Bridging* en una conexión punto a punto

Los datos se encapsulan mientras los *bridges* comunican los datos en una conexión en serie.

La Figura 1-4 ilustra el proceso de encapsulación.

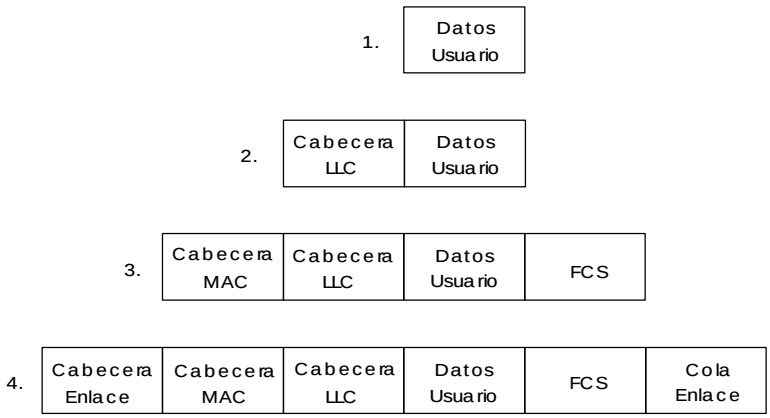


Figura 1-4. Encapsulación de datos en una conexión punto a punto

La encapsulación se desarrolla de la siguiente manera:

1. El equipo final A proporciona datos a su LLC.

2. El LLC añade una cabecera y pasa la unidad de datos resultante al nivel MAC.

3. Después el MAC añade una cabecera y una cola para formar una trama MAC. El *bridge* A captura la trama.

4. El *bridge* A no quita los campos MAC porque su función es transmitir la trama MAC intacta a la LAN de destino. Sin embargo, en la configuración punto a punto el *bridge* añade una cabecera y una cola (por ejemplo HDLC) de nivel de conexión y transmite la trama MAC a través de la conexión.

Cuando la trama de datos alcanza el *bridge* B (bridge objetivo), se quitan los campos de conexión y el *bridge* B transmite la trama MAC *original y sin cambios* a su destino, el equipo final B.

4.3. Formatos de la trama MAC del Bridge

Como ya se ha mencionado, los *bridges* interconectan LANs mediante la transmisión de tramas de datos entre entidades MAC separadas de las LANs unidas por los *bridges*. Las tramas MAC proporcionan la necesaria información de reenvio en forma de direcciones de origen y destino. Esta información es esencial para la transmisión y recepción con éxito de los datos.

IEEE 802 soporta tres tipos de tramas MAC:

- CSMA/CD (802.3)
- Token bus (802.4)
- Token Ring (802.5)

> ***Nota: Un formato de trama separado se utiliza en el nivel LLC. Esta trama se inserta después en la trama MAC apropiada.***

La Figura 1-5 muestra los formatos de las tramas CSMA/CD y Token Ring MAC soportadas por los *bridges*. Las tramas específicas se detallan en la siguiente sección.

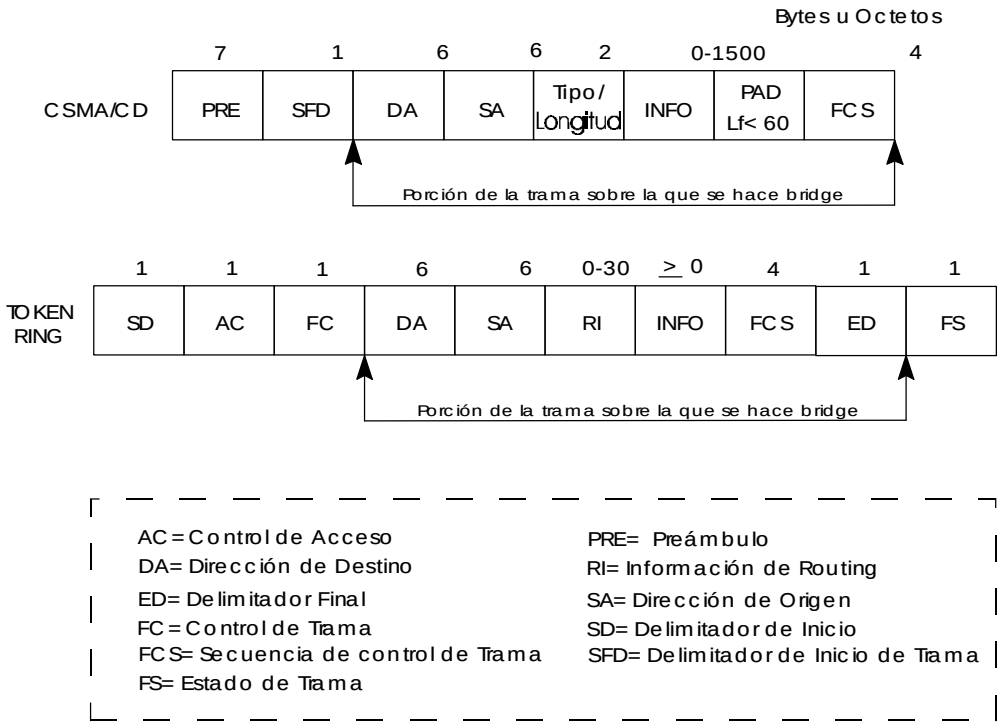


Figura 1-5. Muestras del formato de la trama MAC

4.4. Tramas MAC CSMA/CD (Ethernet)

A continuación se describen cada uno de los campos encontrados en tramas MAC CSMA/CD (Ethernet):

- *Preámbulo* (*Preamble*, PRE). Patrón de 7 bytes utilizado por el equipo final receptor para establecer el sincronismo de bit y después localizar el primer bit de la trama.
- *Delimitador de Inicio de Trama (Start Frame Delimiter* SDF). Indica el inicio de la trama.

La parte de la trama que realmente maneja el *bridge* consiste en los siguientes campos:

- *Dirección de Destino (Destination Address* DA). Especifica el equipo final al que se dirige la trama. Esta dirección puede ser una única dirección física (un destino), una dirección multicast (un grupo de equipos finales como destino). El formato es de 48-bit (6 octetos) y debe ser la misma para todos los equipos en esa LAN en concreto.
- *Dirección de Origen (Source Address* SA). Especifica el equipo final que transmite la trama. La forma tiene que ser la misma que el formato de la dirección de destino. Esta dirección no debe ser nunca una dirección multicast o broadcast.
- *Tipo /Longitud (Type/Length).* Especifica el número de bytes LLC que siguen. Si el valor de este campo es menor que 0x600, entonces el campo es el valor de longitud de los bytes LLC que siguen. Estas se conocen normalmente como tramas IEEE 802.3. El valor mayor o igual a 0x600 identifica el tipo de protocolo. Esta se conoce como trama Ethernet-II.
- *Info* (INFO). Campos insertados creados en el nivel LLC que contienen información del punto de acceso al servicio, información de control y datos de usuario.
- *Relleno (Pad).* Secuencia de bytes que garantizan que la trama es lo suficientemente larga para la correcta operación de detección de colisión (CD). El tamaño mínimo de la trama en Ethernet es 60 bytes, sin incluir FCS.

- *Secuencia de Control de Trama (Frame Check Sequence* FCS). Valor del código cíclico de redundancia (CRC) de 32-bit. Este valor se basa en todos los campos, empezando por la dirección de destino.

4.5. Tramas MAC Token Ring

La siguiente información describe cada uno de los campos que forman las tramas MAC Token Ring:

- *Delimitador Inicial (Starting Delimiter* SD). Patrón único de 8-bit que indica el inicio de la trama.
- *Control de Acceso (Access Control* AC). Campo con el formato PPPTMRRR donde PPP y RRR son variables de prioridad y reserva de 3-bit, M es el bit de monitorización y T indica si es un Token o trama de datos. Si es un Token, el único campo restante es el delimitador final (ending delimiter, ED).
- *Control de Trama (Frame Control,* FC). Indica si esta es una trama de datos LLC. Si no lo es, los bits de este campo controlan la operación del protocolo Token Ring MAC.

La parte de la trama que realmente se transporta en el bridge consta de los siguientes campos:

- *Dirección de Destino (Destination Address* DA). Igual que CSMA/CD y token bus, excepto que el formato de bit es no canónico.
- *Dirección de origen (Source Address, SA*). Identifica el equipo especifico que origina la trama. La extensión del campo puede ser una dirección de 6 octetos. El formato del bit es no canónico.
- *Campo de Información de Encaminamiento (Routing Information Field* RIF). Cuando el RII (el bit más significativo del byte más significativo) en el campo de la dirección origen se fija a 1, este campo aparece después de la dirección origen. Se requiere el RIF para el protocolo de encaminamiento de origen. Consta de un campo de control de encaminamiento de 2-octetos y una serie de campos indicadores de encaminamiento de 2-octetos.
- *Info* (INFO). Campos insertados creados en el nivel LLC que contienen información del punto de acceso al servicio, información de control e datos de usuario.
- *Secuencia de Control de Trama (Frame Check Sequence* FCS). Un valor de control de redundancia cíclica de 32-bit. Este valor se basa es todos los campos, empezando por la dirección de destino.

Por último, el Delimitador Final (*End Delimiter* ED) contiene el bit de detección de error (E) y el bit de trama intermedia (I). El bit I indica que esta es la trama tras la que va la última de una transmisión de trama múltiple. El *Estado de Trama (Frame Status* FS*)* contiene los bits de dirección reconocida (A) y de trama copiada (C).

4.6. Tramas Ethernet Pseudo-serie

Ethernet Pseudo-serie es un modo de operación opcional. Tiene en cuenta la encapsulación de cualquier protocolo encaminado en una línea serie propietaria del router que está haciendo de bridge. De esta forma se puede reenviar dentro de una trama encapsulada de Ethernet. Esto permite al protocolo comunicarse con un bridge puro en el extremo opuesto de la línea serie.

Este modo hace que la línea serie aparezca como una interfaz de Ethernet ante los protocolos de routing configurados. El manejador utiliza encapsulaciones Ethernet (o IEE 802.3, según corresponda). De este modo limita los protocolos al tamaño máximo de trama Ethernet. Estas tramas Ethernet se envían después y se reciben como tramas de *bridge* Ethernet en la línea serie. Cualquier trama que llegue a los puntos de código del protocolo encaminado procedente de una línea serie se ignora, y las tramas Ethernet del *bridge* se pasan al *bridge* o *routing forwarder*, según corresponda.

Normalmente esta encapsulación no es necesaria con los *routers* que hacen de bridge de ambos extremos de la línea serie, ya que ambos se pueden configurar para encaminar el mismo grupo de protocolos en la misma línea serie.

Capítulo 2
Utilizando Bridge Transparente

1. Relativo a STB

El Bridge Transparente también se conoce comúnmente como Spanning Tree Bridge (STB). El término transparente se refiere al hecho de que el bridge envía silenciosamente tráfico no local a LANs relacionadas de una manera que es transparente o invisible para el usuario. Las aplicaciones del equipo final desconocen la presencia del bridge. El bridge sabe de la existencia de los equipos finales mediante la escucha del tráfico que pasa. De este proceso de escucha construye una base de datos de las direcciones de los equipos finales relacionados a sus LANs.

Para cada trama que recibe, el bridge compara las direcciones de destino de las tramas con las de su base de datos. Si el destino está en la misma LAN no envía la trama; si el destino está en otra LAN sí la envía. Si la dirección de destino no aparece en la base de datos, envía la trama a todas las LANs conectadas al bridge exceptuando a la LAN de la que se origina.

Todos los bridges transparentes utilizan un protocolo y algoritmo Spanning Tree. El algoritmo Spanning Tree produce y mantiene una topología sin bucles en una red de bridge que podría contener bucles en su diseño físico. En una topología de malla, donde hay más de un bridge conectado entre dos LANs, los paquetes de datos pueden rebotar de un bridge a otro entre dos bridges paralelos de LANs. Esto produce una redundancia en el tráfico de datos y produce el fenómeno conocido como bucles.

Sin un Spanning Tree, cuando se producen bucles, se deben configurar las LANs locales y/o alejadas para eliminar el bucle físico. Con un Spanning Tree, un algoritmo que se configura por sí sólo permite a un bridge conectarse a cualquier parte de una LAN sin crear bucles. Cuando se añade el nuevo bridge, el Spanning Tree reconfigura de manera transparente todo los bridges de la LAN para formar un Spanning Tree único sin bucles.

El Spanning Tree no tiene nunca más de una ruta de datos activa entre dos equipos finales. De esta forma elimina los bucles de datos. Para cada bridge el algoritmo determina qué puertos de bridge usar para enviar datos y cuáles bloquear para formar una topología sin bucles. Entre sus características el spanning tree proporciona las siguientes:

- *Detección de bucles*. Detecta y elimina los bucles de conexión de datos físicos en configuraciones de LANs prolongadas.
- *Backup automático de rutas de datos*. Configurado especialmente para caminos redundantes. Los bridges conectados a los caminos redundantes dan entrada automáticamente al modo backup. Cuando falla un bridge primario se activa un bridge de backup.
- *Facilidad de configuración por el usuario*. Le permite configurar su topología de red a medida. En ocasiones la configuración por omisión no produce la topología de red deseada. Se puede modificar la prioridad de bridge, la prioridad de puerto y los parámetros de coste de ruta para adaptar el Spanning Tree a su topología de red.
- *Interoperabilidad perfecta*. Permite la interoperabilidad de LAN sin limitaciones de configuración causadas por los distintos entornos de comunicaciones.
- *Bridging de protocolos no encaminables*. Proporciona el bridging de coste eficaz de protocolos no encaminables como el Transporte de Área Local (Local Area Transport, LAT) de la DEC del protocolo de la terminal.

2. Los Routers y STB

Cuando el software de un bridge y un router se ejecutan de forma simultánea en un router equipado con la opción de Spanning Tree ocurre lo siguiente:

- Los paquetes se encaminan si un protocolo de encaminamiento específico está habilitado globalmente.
- Los paquetes se filtran si se configuran filtros de protocolo específicos.
- Los paquetes que no están encaminados o filtrados son candidatos para el bridging dependiendo de la dirección de destino MAC (Medium Access Control).

3. Requisitos de la Red STB

El bridge transparente ejecuta un bridge Spanning Tree que se ajusta al estándar IEEE 802.ID. Todos los bridges transparentes como Ethernet, SL y TKR en la red deben ser bridges Spanning Tree 802.ID. Este protocolo Spanning Tree no es compatible con bridges que hacen efectivo el protocolo propietario Spanning Tree Digital Equipment Corporation.

4. Habilitar STB

La siguiente información explica de manera resumida los pasos iniciales que se requieren para habilitar la opción de bridging transparente que ofrece el bridge ASRT.

> ***Nota: No se soporta el bridging transparente sobre X.25. Se puede trabajar sobre esto mediante la configuración de la opción IP túnel.***

Se utilizan los siguientes comandos para habilitar el bridging transparente:

- ***Enable bridge***. Habilita el bridging transparente en todas las interfaces LAN. Se puede habilitar el bridging en las interfaces WAN (líneas serie) utilizando el comando **ADD PORT**.
- ***Disable transparent*** port #. Hace imposible el bridging transparente en puertos de bridge previamente habilitados. Se tiene que repetir el comando para todos los puertos que se quieran excluir de la configuración de bridging transparente.

Tras completar los pasos arriba descritos, se puede introducir **LIST BRIDGE** para comprobar la configuración.

Para hacer cambios en la configuración, véase el **Capítulo 7 "Configuración ASRT"** de este manual.

Una vez que se hayan hecho los cambios en la configuración se debe reiniciar el router para que la nueva configuración tenga efecto.

5. Cómo Funciona el STB

Durante el inicio todos los bridges que participan en la red intercambian Unidades de Datos de Saludo del Protocolo Bridge (Hello Bridge Protocol Data Units, BPDUs) que proporcionan información de configuración de cada bridge. Los BPDUs incluyen información como el ID del bridge, el ID de la raíz y el coste de la ruta raíz. Dicha información ayuda a los bridges a determinar unánimemente qué bridge es el bridge raíz y qué bridges son los bridges designados para las LANs a las que están conectados.

De la información intercambiada en los mensajes de "Hello", los siguientes parámetros son los más importantes para el cálculo del Spanning Tree:

- *ID del Bridge raíz*. Es el identificador (ID) del bridge raíz, que es el bridge designado para todas las LANs a las cuales está conectado.
- *Coste de la ruta raíz*. La suma de los costes de ruta designados a la raíz a través del puerto raíz de este bridge. Esta información es transmitida tanto por el bridge raíz como por los bridges designados para actualizar todos los bridges en información ruta si cambia la topología.
- *ID de Bridge*. Un identificador (ID) único que usa el algoritmo Spanning Tree para determinar el Spanning Tree. A cada bridge de la red se le asigna un identificador de bridge único.
- *ID de Puerto*. El identificador (ID) del puerto desde el que se transmitió el mensaje de "Hello" actual BPDU.

Con esta información disponible, el Spanning Tree comienza a determinar su forma y dirección y después crea una configuración de ruta lógica según se explica a continuación:

1. Se selecciona un bridge raíz para la red mediante la comparación de los IDs de cada uno de los bridges de la red. Se selecciona el bridge con el menor valor de ID (por ejemplo Prioridad mayor).
2. Después el algoritmo Spanning Tree selecciona un bridge designado para cada LAN. Si más de un bridge está conectado a la misma LAN, se escoge como bridge designado el de menor coste de ruta para la raíz. En el caso de costes de ruta duplicados se escoge como bridge designado el de ID de bridge más bajo.
3. Los bridges no designados en las LANs ponen cada puerto que no ha sido designado en un estado de bloqueo. En el estado de bloqueo un bridge sigue escuchando los mensajes de "Hello" BPDUs de forma que puede actuar sobre los cambios que se realizan en la red (por ej. fallos del bridge designado) y cambiar su estado de estar bloqueado a enviar (por ej. envío de datos).

Mediante este proceso el algoritmo spanning tree reduce una red de bridge LAN de topología arbitraria en un único spanning tree. Con un spanning tree nunca hay más de una ruta de datos activa entre dos equipos finales, eliminando así los bucles de datos.

Esta nueva configuración se delimita por un factor de tiempo. Si un bridge designado falla o es físicamente eliminado, otros bridges en la LAN detectan la situación al no recibir los mensajes de "Hello" BPDUs dentro de un período de tiempo determinado por el tiempo máximo de vida de un bridge. Este hecho puede provocar un nuevo proceso de configuración en el que un nuevo bridge es seleccionado como el bridge designado. También se crea una nueva configuración si el bridge raíz falla.

6. Forma del Spanning Tree

Cuando el Spanning Tree utiliza las configuraciones por omisión, el algoritmo Spanning Tree proporciona resultados aceptables. De todas formas, el algoritmo puede producir en ocasiones un Spanning Tree con un rendmiento de red pobre. En este caso se puede ajustar la prioridad de bridge, la prioridad de puerto y el coste de ruta para adaptar el Spanning Tree a las necesidades de ejecución de la red esperadas. El siguiente ejemplo muestra cómo hacer esto (véase la Figura 2 - 1).

La Figura 2 - 1 muestra tres LANs en red utilizando tres bridges. Cada bridge utiliza la configuración por defecto de prioridad de bridge para la configuración de su Spanning Tree. En este caso se escoge como bridge raíz el bridge con la dirección física más baja, ya que la prioridad de bridge de cada bridge es la misma. En este ejemplo este bridge es el Bridge 2.

El recién configurado Spanning Tree permanece intacto debido a las transmisiones repetidas de mensajes de “Hello” BPDUs desde el bridge raíz durante un intervalo (tiempo de “Hello” del bridge). Durante este proceso, se actualizan los bridges designados con toda la información de configuración. Entonces los bridges designados regeneran la información de los mensajes de “Hello” BPDUs y los distribuyen a las LANs para las que son bridges designados.

Bridge 1	Bridge 2	Bridge 3
Prioridad Bridge: 32768	Prioridad bridge: 32768	Prioridad bridge: 32768
Dirección 00:00.90:00.00:10	Dirección 00:00.90:00.00:01	Dirección 00:00.90:00.00:05
Puerto 1	Puerto 1	Puerto 1
Prioridad: 128	Prioridad: 128	Prioridad: 128
Coste de ruta: 100	Coste de ruta: 100	Coste de ruta: 100
Puerto 2	Puerto 2	Puerto 2
Prioridad: 128	Prioridad: 128	Prioridad: 128
Coste de ruta: 17857	Coste de ruta: 17857	Coste de ruta: 17857
Puerto 3	Puerto 3	Puerto 3
Prioridad: 128	Prioridad: 128	Prioridad: 128
Coste de ruta: 17857	Coste de ruta: 17857	Coste de ruta: 17857

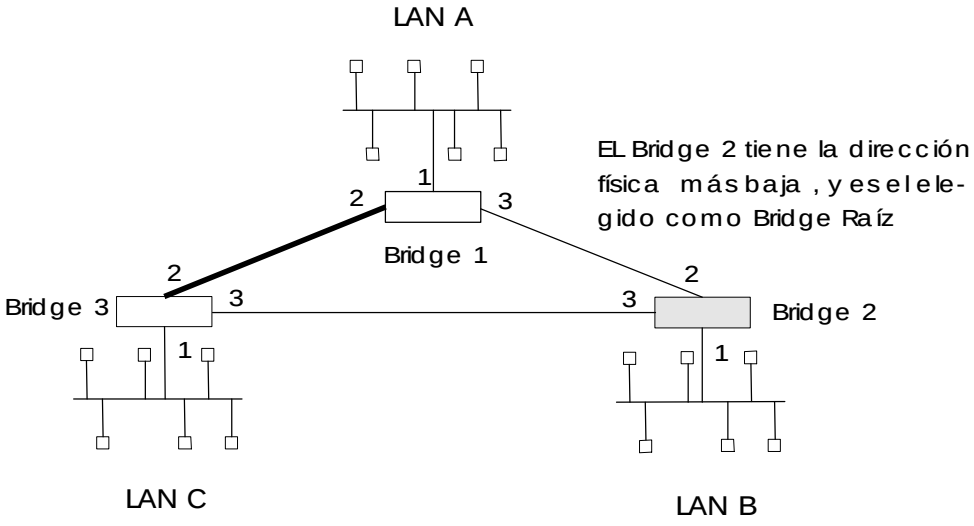


Figura 2-1. LANs de red antes de un spanning tree

El algoritmo Spanning Tree designa el puerto que conecta el Bridge 1 y el Bridge 3 (puerto 2) como un puerto de Backup y lo bloquea de las tramas enviadas que causarían una condición de bucle. El Spanning Tree creado por el algoritmo utiliza los valores por defecto que se muestran en la figura 2-2 con las líneas marcadas de forma más oscura que conectan el Bridge 1 al Bridge 2, y después el Bridge 2 al Bridge 3. El Bridge raíz es el Bridge 2.

Este Spanning Tree tiene como resultado un rendimiento de red pobre porque los equipos en la LAN C sólo pueden acceder al servidor de ficheros en la LAN A indirectamente a través del Bridge 2 en lugar de hacerlo utilizando la conexión directa entre el Bridge 1 y el Bridge 3.

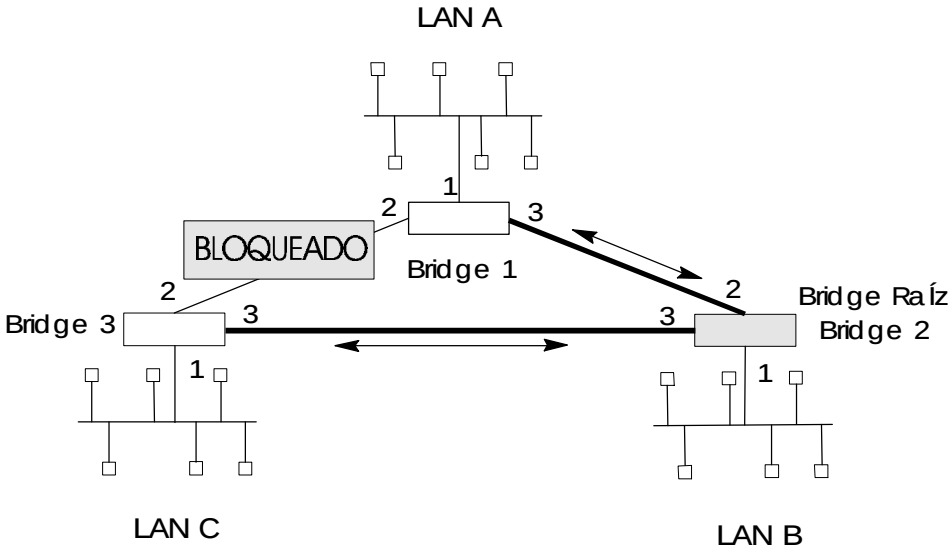


Figura 2-2. Spanning Tree creado con valores por omisión

Por norma general esta red no suele utilizar el puerto entre el Bridge 2 y el Bridge 3. Por lo tanto, se puede mejorar el rendimiento de la red convirtiendo el Bridge 1 en el bridge raíz del Spanning Tree. Esto se puede hacer configurando el Bridge 1 con la prioridad más alta (1000). El Spanning Tree que resulta de esta modificación se muestra en la Figura 2-3 como las líneas gruesas que conectan el Bridge 1 con el Bridge 3 y el Bridge 1 al Bridge 2. Ahora el bridge raíz es el Bridge 1. La conexión entre el Bridge 2 y el Bridge 3 está ahora bloqueada y sirve como ruta de respaldo de datos.

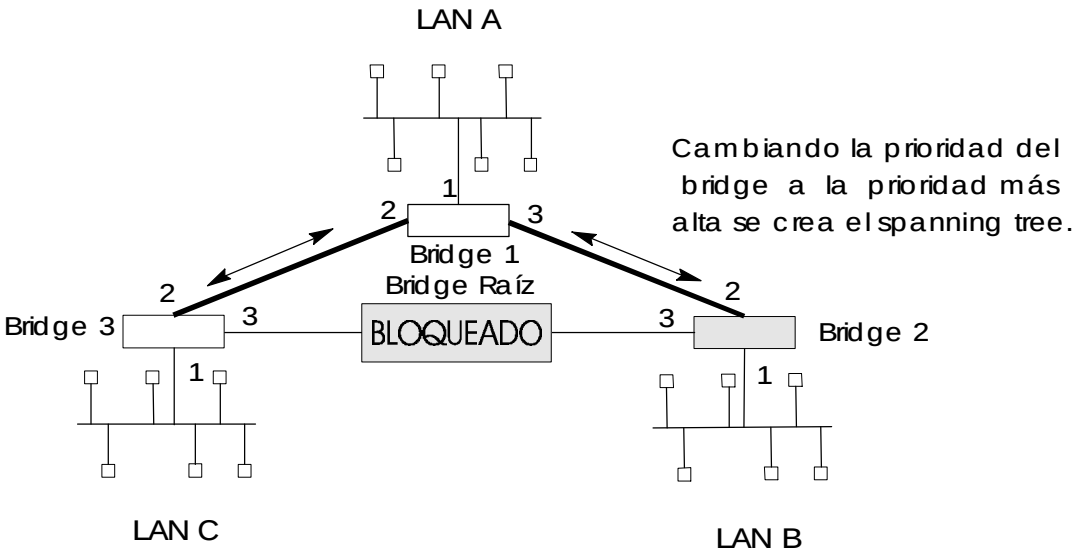


Figura 2-3. Spanning tree ajustado por el usuario

7. Bridges de Spanning Tree y Traducción del Formato del Paquete Ethernet

El protocolo SSTB envía los paquetes de acuerdo con el estándar IEEE 802.1D-1990 para bridges MAC (Medium Access Control). Éste puede crear un bridge transparente entre cualquier combinación de redes Ethernet/IEEE 802.3, localmente o vía líneas serie. El protocolo también proporciona una traducción apropiada de la cabecera para los paquetes de Ethernet.

Una red Ethernet/IEEE 802.3 puede soportar a la vez el nivel de conexión de datos Ethernet basado en el valor del campo largo/tipo en la cabecera MAC.

La aproximación básico consiste en la traducción de los paquetes Ethernet a paquetes de Información no Numerada (Unnumbered Information, UI) IEEE 802.3 utilizando el IEEE 802 SNAP SAP. El Identificador de Protocolo (Protocol Identifier) SNAP tiene como OUR (Oganizationally Unique Identifier) el valor 00-00-00, cuyos dos últimos bytes son el valor *tipo* de Ethernet.

La traducción se hace cuando se envía una trama a un LAN. El formato de la trama original se conserva a través de las líneas serie.

Capítulo 3
Utilización del Bridging de Encaminamiento de Origen (Source Route Bridging, SRB)

1. Relativo a SRB

El Source Route Bridging (SRB) es un método de envío de tramas a través de una red de bridge en la que el equipo de origen identifica la ruta que seguirá la trama. En un esquema de routing distribuido, las tablas de routing en cada bridge determinan la ruta que toman los datos a través de la red. En comparación, en un esquema de Source Route Bridging el equipo de origen define la ruta completa en la trama transmitida.

El SRB proporciona bridging local sobre Token Rings de 4 y 16 Mbps. Véase la Figura 3-1. También puede conectar LANs remotas a través de enlaces de telecomunicaciones operando a velocidades de hasta E1.

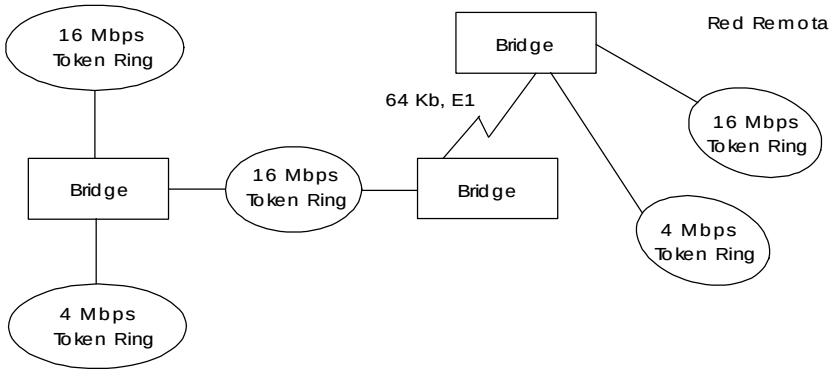


Figura 3-1. Muestra de la conectividad del bridge de source routing

Entre sus características el Bridge de source routing proporciona:

- *Compatibilidad con IBM.* El bridge es compatible con el bridge de source routing de IBM. Puede conectar sistemas ejecutables de IBM PC LANs como el OS/2 y el NetBIOS. También puede llevar tráfico IBM SNA entre PC LANs y ordenadores centrales.
- *Rendimiento y velocidad.* Debido a que el bridging ocurre en el nivel de enlace de datos en lugar de en el nivel de red, la conversión del paquete y el mantenimiento de la tabla de direcciones no son necesarios. Esto significa menor overhead y mayor velocidad en las decisiones de routing.
- *Bridge tunneling.* Encapsulando los paquetes de encaminamiento de origen, el bridge envía dinámicamente estos paquetes a través de internetworking al equipo de destino deseado sin degradación o restricciones de los tamaños de red.
- *Conservación del FCS.* Los bridges Teldat conservan la secuencia de control de trama de las Tramas encaminadas específicamente (Specifically Routed Frames, SRF). Esto protege contra la alteración de datos de las tramas de bridge.

Los equipos finales de source routing ven esta ruta (el túnel) como un único salto, sin reparar en la complejidad de la red. Esto ayuda a superar el límite de distancia normal de siete saltos encontrado en las configuraciones de source routing. Esta característica también permite conectar equipos finales de source routing a través de medios que no son de encaminamiento de origen (por ejemplo redes Ethernet).

2. Activar SRB

La siguiente información señala los pasos iniciales que se requieren para activar la opción de bridging SRB ofrecida por el bridge ASRT.

- **Enable bridge.** Activa el bridging en todas las interfaces del LAN. Se pueden incluir interfaces WAN (líneas seerie) utilizando el comando **ADD PORT**.
- **Disable transparent** *port#.* Desactiva el bridging transparente en todos los puertos.
- **Enable source routing** *port# segment#/bridge#.* Cuando se activa el source routing en más de dos puertos se requiere un número de segmento adiccional para asignar un segmento virtual interno que se necesita para configuraciones SRB 1:N.

Si sólo se quiere el source routing, hay que desactivar el bridging transparente en las interfaces.

No se deben incluir interfaces que tradicionalmente no soportan source routing. Por ejemplo, si se desactiva el bridging transparente y se activa el source routing en un puerto de Ethernet, la facilidad del bridging se desactiva para ese puerto.

Tras completar los procedimientos arriba descritos, se puede introducir **LIST BRIDGE** para verificar la configuración. Si se quieren hacer cambios en la configuración, véase el Capítulo 7 **"Configuración ASRT"** de este manual. Una vez que se acaba de cambiar la configuración, se tiene que reiniciar el router para que la nueva configuración tenga efecto.

3. Cómo funciona el SRB

Como ya se ha mencionado, el equipo de origen define la ruta completa en la trama transmitida en una configuración de source routing. El bridge de source routing es dinámico. Ambos equipos de origen y bridges toman parte en el descubrimiento de la ruta y en el proceso de envío. Los siguientes pasos describen este proceso:

1. Un equipo de origen envía una trama transparente y descubre que el destino de la trama no está en su propio (local) segmento o anillo.
2. El equipo de origen construye una trama broadcast de *descubrimiento de ruta* y la transmite al segmento local.
3. Todos los bridges del segmento local capturan la trama de descubrimiento de ruta y la envían sobre sus redes conectadas.
4. Mientras la trama de descubrimiento de ruta continua su búsqueda del equipo final de destino, cada bridge que la envía añade su propio número de bridge y número de segmento al campo de información de routing (RIF) en la trama. Mientras la trama sigue pasando a través de la red de bridge, el RIF recopila una lista de pares de bridge y de números de segmento describiendo la ruta hasta el destino. Cuando la trama broadcast por fin alcanza su destino, contiene la secuencia exacta de direcciones desde el origen hasta el destino.
5. Cuando el equipo final de destino recibe la trama, genera una trama de respuesta que incluye la ruta de encaminamiento para la comunicación. Las tramas que recorren otras partes de la red de bridge (acumulando información de encaminamiento irrelevante mientras tanto) nunca alcanzan el equipo final de destino y ningún equipo las llega a recibir.
6. El equipo de origen recibe la ruta de encaminamiento aprendida. Entonces puede transmitir información a través de esta ruta establecida.

4. Formatos de Trama SRB

Como los mencionados bridges interconectan LANs mediante tramas de datos transmitidas, específicamente tramas MAC entre las entidades MAC separadas de las LANs que hacen bridge. Las tramas MAC proporcionan la información de envío necesaria con la forma de direcciones de origen y destino. Esta información es esencial para la transmisión y recepción de datos con éxito.

En el source routing, la decisión de envío de la trama de datos se basa en la información de encaminamiento dentro de la trama. Antes de enviar la trama, los equipos finales han obtenido la ruta hasta el equipo de destino mediante el *descubrimiento de ruta*. El equipo de origen que origina la trama designa la ruta que se recorrera, incluyendo una descripción de la ruta en el RIF de la trama transmitida. Un estudio más pormenorizado de los diversos tipos de tramas de source routing bridge ayuda a explicar con más detalle como el bridge obtiene y transmite esta información de routing.

Debido a que las tramas MAC de source routig contienen información necesaria para la comunicación de datos en entornos multi-anillo, se diferencian ligeramente en el formato de las típicas tramas MAC Token Ring. La presencia de un 1 en el RII dentro del campo dirección de origen indica que un RIF que contiene información de routing sigue a la dirección de origen. La Figura 3-2 proporciona una mirada exhaustiva al formato del campo de la dirección de origen de una trama de source routing.

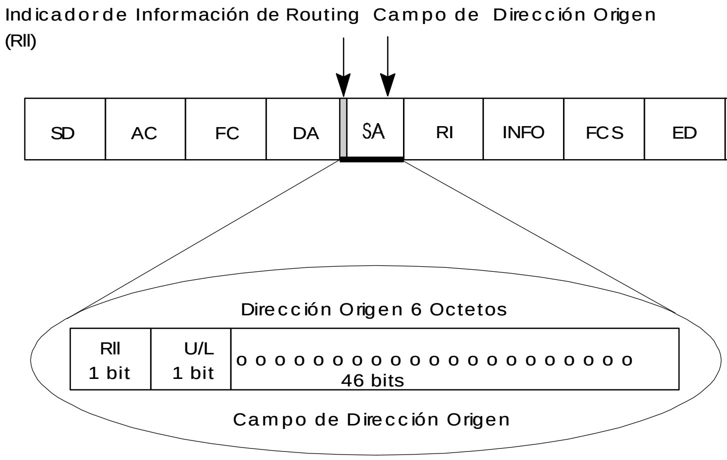


Figura 3-2. 802.5 Formato de la Dirección de Origen.

Cuando el RII en el campo de dirección de origen se establece a 1, está presente un RIF después de la dirección de origen. Se requiere el RIF porque proporciona la información de ruta durante el source routing. Éste consiste en un campo de control de routing (RC) de 2 octetos y en una serie de campos diseñadores de ruta (route designator, RD) de 2 octetos. La Figura 3-3 proporciona una mirada exhaustiva al formato del campo de información de routing (Routing Information Field)

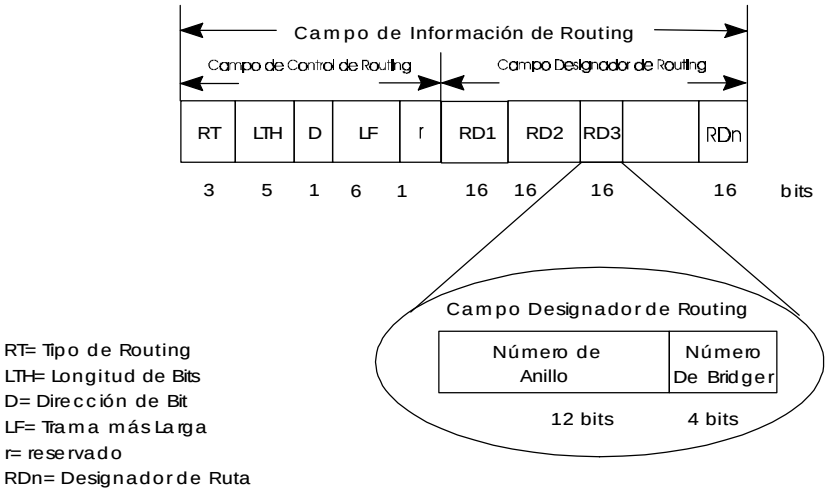


Figura 3-3. 802.5 Campo de Información de Encaminamiento

La siguiente información describe cada campo específico que se encuentra en el RIF:

- *Tipo de Encaminamiento (Routing Type, RT).* Indicado por las posiciones de bit si la trama va a seguirse a través de la red a lo largo de una ruta específica o a lo largo de una ruta (o rutas) que llegan a todas las LANs interconectadas.

Dependiendo de las posiciones de bit en este campo la trama de encaminamiento de origen puede identificarse como uno de los siguientes tipos:

- Trama exploradora de todas las rutas, (All-Route Explorer, ARE) (trama exploradora)
- Trama exploradora de Spanning-Tree (Spanning-Tree Explorer, STE) (trama exploradora)
- Trama específicamente encaminada (Specifically-Routed Frame, SRF) (trama de datos)

  Las tramas exploradoras de todas las rutas existen si los bits RT se establecen a 10x donde x es un bit *sin importancia*. Estas tramas se generan y encaminan a lo largo de cada ruta que no se repite en la red (desde el origen hasta el destino). Esto tiene como resultado tantas tramas que llegan al equipo final de destino como rutas distintas hay desde el equipo final de origen. Este tipo de encaminamiento se puede usar como respuesta al hecho de recibir una trama de descubrimiento de ruta enviada a lo largo del spanning tree hasta el equipo de origen presente por todas las rutas disponibles. Los bridges que envían añaden diseñadores de encaminamiento a la trama.

  Una *trama exploradora de spanning-tree* existe si los bits TR se establecen a 11x donde x es un bit *sin importancia*. Sólo los bridges Spanning Tree transmiten la trama desde una red a otra. Esto significa que la trama aparece sólo una vez en cada anillo en la red y por lo tanto sólo una vez en el equipo final de destino. Un equipo que inicia el proceso de descubrimiento de ruta usaría este tipo de trama. El bridge añade campos diseñadores de routing a la trama. También se puede utilizar para tramas enviadas a equipos que utilizan una dirección de grupo.

  Las tramas específicamente encaminadas existen si el primer bit RT se establece a 0. Cuando éste es el caso, los campos designadores de ruta (Route Designator, RD) contienen direcciones de destino específicas. Durante la fase de descubrimiento de ruta, este tipo de trama se utiliza en respuesta a una trama ARE. Los datos del usuario se llevan siempre en el formato de trama SRF.

- *Longitud de bits (Length bits, LTH).* Indica la longitud (en octetos) del campo RI.

- *Dirección de bit (Direction bit, D).* Indica la dirección que toma la trama para atravesar las redes conectadas. Si este bit está establecido a 0, la trama recorre las redes conectadas en el orden en el que están especificadas en el campo de información de routing (por ejemplo RD1 a RD2 a .... a RDn). Si la dirección de bit está establecida a 1, la trama recorre las redes en el orden contrario.
- *Bits de trama más larga (Largest Frame Bits, LF).* Indica el tamaño de trama más largo del campo INFO que se puede transmitir entre dos equipos finales que se están comunicando en una ruta específica. Los bits LF son significativos sólo para tramas STE y ARE. En un SRF, el bridge ignora los bits LF y no los puede modificar. Un equipo que origina una trama exploradora establece los bits LF al tamaño de trama mayor que puede manejar. Los bridges que envían establecen los bits LF al valor más largo que no excede el mínimo de:
  - El valor indicado a los bits LF recibidos
  - La Unidad de datos de servicio MAC (MAC Service Data Unit, MSDU) más larga soportada por el puerto desde el que la trama se recibió.
  - El MSDU más largo soportado por el puerto en el que la trama se va a transmitir

    El equipo de destino reduciría más el valor LF para indicar su capacidad de trama máxima.

    Los codificadores de bits LF están hechos de un codificador base de 3-bit y un codificador extendido de 3-bit (6 bits en total). El bridge SRT contiene un indicador de interpretación de modo LF para que el bridge pueda seleccionar bits LF base o extendidos. Cuando el indicador de interpretaciones de modo LF está establecido en *modo base*, el bridge establece los bits LF en tramas exploradoras con los valores *base* de trama más largos. Cuando el indicador de modo LF está establecido en *modo extendido*, el bridge establece los bits LF en tramas exploradoras con los valores *extendidos* de trama más largos.
- *Campos designadores de ruta (Route Designator fields, RDn),* indica la ruta específica a través de la red de acuerdo con la secuencia de los campos RD. Cada RD contiene un número de anillo de 12-bit de red único y un número de bridge de 4-bit que diferencia entre dos o más bridges cuando se conectan los dos mismos anillos (bridges paralelos). El último número de bridge en el campo de información de encaminamiento tiene un valor nulo (todo ceros).

5. La Opción Explorador Spanning Tree

La opción *explorador Spanning Tree* permite seleccionar una única ruta hacia un destino cuando la red tiene dos o más bridges que conectan las mismas LANs. Con esta característica activada, únicamente los bridges seleccionados reciben tramas STE. No hay que confundirlo con el protocolo spanning tree, esta opción permite simular una red Spanning Tree.

5.1. Simular una Red Spanning Tree

Los bridges SRB participan en el Protocolo Spanning Tree propietario de IBM (Spanning Tree Protocol, STP). La participación en STP permite a los bridges SRB reducir una topología de red en malla en un spanning tree sin bucles de manera automática. Para una red con bridges SRB paralelos, como muestra la Figura 3-4, el algoritmo STP bloquea automáticamente uno de los puertos de un bridge (en este ejemplo el Bridge B). Esto provoca que las tramas STE se envíen únicamente vía Bridge A. Se pueden configurar bridges de manera que no participen en STP y activar o desactivar manualmente STP en cada puerto de cada bridge. Obviamente, no se recomienda la configuración manual, pero puede requerirse en ciertas circunstancias.

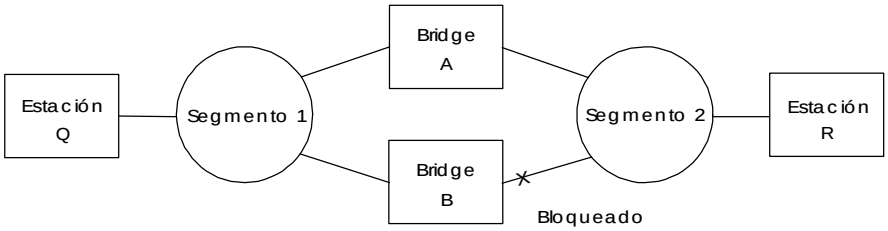


Figura 3-4. Muestra de Bridge Paralelo

6. SRB y Frame Relay

La interfaz Frame Relay envía tramas de encaminamiento de origen hacia y desde el equipo que hece de bridge, proporcionando que el source routing bridge esté habilitado en el Circuito Virtual Permanente (PVC).

Un número de anillo de destino se configura para cada PVC. Se bloquean algunos PVCs que no son parte de la ruta de datos activa para mantener la topología sin bucles.

Capítulo 4
Utilización de la Conversión de Bridge de Encaminamiento de Origen Transparente (Route-Transparent Bridge, SR-TB)

1. Relativo a la Conversión SR-TB

La opción de conversión de Source Route-Transparent Bridge (SR-TB) interconecta redes utilizando source route bridging (dominio de source routing) y bridging transparente (dominio de bridge transparente). Esta opción une de forma transparente ambos dominios. Los equipos en ambos dominios no son conscientes de la existencia del bridge SR-TB. Cualquier equipo en la red combinada parece estar en su propio dominio.

El source routing está disponible en el modelo SRT, entre los Token Rings de source routing adyacentes. Los bridges de source route único no pueden coexistir con bridges SRT que unen LANs Ethernet y Token Ring. Debido a que un nodo final Token Ring necesita comunicarse con un nodo Ethernet, se debe configurar para omitir RIFs. Pero si el nodo final se configura para omitir RIFs, no se puede comunicar a través del bridge de source routing común que requiere ese RIF.

El SR-TB consigue su funcionalidad transformando tramas del dominio del bridging transparente en tramas de source routing antes de enviarlas al dominio de source routing (y viceversa). El bridge hace esto mediante el mantenimiento de una base de datos de las direcciones de equipos finales, cada una con su RIF en el dominio de source routing. También dirige el descubrimiento de ruta por los equipos finales presentes en el campo del bridging transparente. Utiliza el descubrimiento de ruta para encontrar la ruta hasta el equipo de destino en el dominio de source routing. El bridge envía tramas direccionadas a un destino desconocido en el formato Explorador de Spanning Tree (Spanning Tree Explorer, STE).

El SR-TB puede manejar tres tipos de Spanning Tree:

- Un Spanning Tree formado por un dominio de bridge transparente.
- Un Spanning Tree formado por un dominio de bridge de source routing.
- Un Spanning Tree especial en el que todos los bridges son SR-TB.

Las siguientes secciones tratan el funcionamiento del SR-TB de forma más detallada.

2. Activar el SR-TB

La información que sigue señala los pasos iniciales que se requieren para activar la opción de bridging SR-TB ofrecida por el bridge ASRT.

- **Enable bridge.** Habilita el bridging en todas las interfaces de LAN. Se pueden incluir interfaces WAN (líneas serie) utilizando el comando **ADD PORT**.
- **Disable transparent** *port#*. Desactiva el bridging transparente en las interfaces fundamentales.
- **Enable source-routing** *port#.* Activa el encaminamiento de origen para puertos determinados. Cuando el source routing está habilitado en más de dos puertos, se requiere un número de segmento adicional para asignar un segmento virtual interno necesario para configuraciones SRB 1:N
- **Enable sr-tb-conversion** *segment#.* Activa la conversión de tramas de source routing en tramas transparentes y viceversa. También se debe asignar un número de segmento de dominio y un tamaño de dominio MTU para representar el dominio de bridging transparente *completo*

Tras completar los procedimientos arriba descritos, se puede introducir **LIST BRIDGE** para la visualización de la configuración actual de bridge. Esto permite verificar y controlar la configuración.

Si se quieren hacer cambios en la configuración, véase el **Capítulo 7 "Configuración ASRT"** de este manual donde se facilitan más detalles. Al acabar de hacer los cambios en la configuración, se debe reiniciar el router para que la nueva configuración tenga efecto.

3. Cómo funciona la Conversión SR-TB

Durante el bridging SR-TB, se divide una red en dos o más dominios separados. Cada dominio se compone de una colección de segmentos de LANs interconectados por bridges que operan bajo un método común de bridging. Esto permite redes compuestas de dos tipos de dominios:

- Source Routing
- Bridging transparente

La Figura 4-1 muestra un ejemplo de estos dominios. Con dominios separados, cada dominio de source routing tiene una topología broadcast de único camino establecida para sus bridges. Únicamente se designan para enviar tramas broadcast de único camino aquellos bridges que pertenecen a ese Spanning Tree source routing. En este caso, las tramas que llevan el indicador broadcast de único camino se encaminan a cada segmento del dominio de source routing. Sólo llega a cada segmento una copia de la trama, ya que el Spanning Tree de source routing no permite rutas múltiples entre dos equipos en el campo.

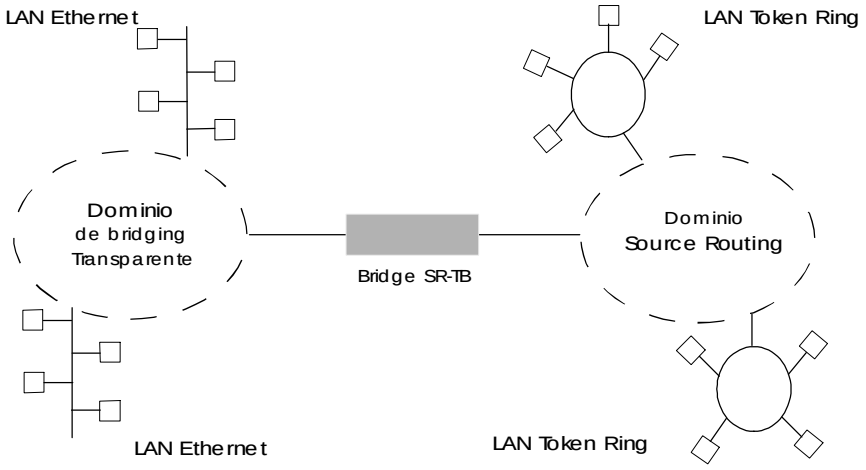


Figure 4-1. Bridge SR-TB que conecta dos campos

4. Operaciones Específicas de Source Routing y Bridging Transparente

El SR-TB es un dispositivo de dos puertos con una interfaz MAC asignada al segmento de la LAN en el lado del source routing y otra al segmento de la LAN en el lado del bridging transparente. Cada equipo final lee el nivel apropiado de la MAC para su segmento de LAN.

En el lado del bridging transparente, el SR-TB funciona igual que cualquier otro bridge transparente. Mantiene una tabla de direcciones para los equipos que sabe que son equipos de bridging transparente. Observa los protocolos entre bridges necesarios para crear y mantener la red de Spanning Tree ya que más de un SR-TB une campos distintos.

El SR-TB envía una trama recibida desde el equipo de bridging transparente hasta el lado del source routing sólo si no encuentra la dirección de destino de la trama en la tabla de dirección del lado del bridging transparente.

En el lado del bridging de source-routing, el SR-TB combina de una manera específica las funciones de un bridge de source routing y las de un equipo final de source routing. Como equipo final de source-routing, mantiene una asociación de direcciones de destino e información de routing. Comunica bien como un equipo final para aplicaciones del propio bridge (por ejemplo gestión de red) o bien como un intermediario para equipos en el lado del bridging transparente.

El SR-TB sólo envía una trama recibida desde el equipo de bridging transparente hasta el lado de source routing del bridge si no encuentra la dirección de destino de la trama en la tabla de dirección del lado de bridging transparente. Las tramas transmitidas por el equipo de source routing del bridge llevan la información de routing asociada con el bridge, si el bridge conoce y contiene tal información.

Como bridge de source-routing, el SR-TB participa en el proceso de descubrimiento de rutas y en el encaminamiento de tramas que ya llevan información de routing. El designador de rutas único del SR-TB consta del número de la LAN de la LAN individual en su lado de source routing y su propio número de bridge individual. También mantiene un único número de LAN representando todas las LANs en el lado del bridging transparente.

Trata cada caso de tramas recibidas y enviadas de manera diferente, como se describe en la **Tabla 4-1**.

Tabla 4-1. Tabla de decisión del Bridge SR-TB

Tipo de Trama Recibida	**Acción que desarrolla el SR-TB**
Trama no encaminada recibida por el equipo de source routing.	No copia o envía la trama que lleva la información de routing.
Trama broadcast con todas las rutas recibidas por el equipo de source routing.	Copia la trama y establece los bits A y C del indicador de broadcast en la trama repetida. Si la dirección de destino está en la tabla del bridging transparente, envía la trama sin información de routing a la red del bridging transparente. Si no, no envía la trama.
Trama broadcast de ruta única recibida por el equipo de source routing. El bridge no está designado como bridge broadcast de ruta única.	No copia o envía la trama.
Trama broadcast de ruta única recibida por el equipo de source routing. El bridge está designado como bridge broadcast de ruta única.	Copia partes de la trama, los bits A y C en el indicador broadcast, quita la información de routing de la trama y envía la trama modificada al lado de bridging transparente.

	Añade su número de bridge para salvar al campo de información de routing y el número LAN para el lado de bridging transparente. Cambia el indicador broadcast a no broadcast, complementa el bit D y almacena esta información de routing para la dirección de origen de la trama.
Trama no broadcast recibida por el equipo de source routing.	Si la trama lleva una ruta específica, el bridge examina la información de routing. Si el SR-TB es parte de la ruta y aparece entre el número de LAN para el lado de source routing y el número de LAN para el lado del bridging transparente, copia la trama y configura los bits A y C en la trama repetida. Envía la trama al lado de bridging transparente sin información de routing. Si el SR-TB no tiene todavía una ruta permanente para la dirección de origen, guarda una copia de la información de routing, complementa el bit D y almacena la información de routing salvada para la dirección de origen de la trama.
Trama recibida desde el lado de bridging transparente.	Para enviar la trama al lado de source routing, primero determina si tiene información de routing relacionada con la dirección de destino que lleva la trama. Si es así, añade información de routing a la trama, configura el R11 a 1 y pone en cola la trama para la transmisión en el lado de source routing. Si no es así, añade una campo de control de routing a la trama que conteniendo un indicador de broadcast de ruta única y dos designadores de ruta, que contienen los dos primeros números de LAN y su número de bridge individual propio.

4.1. Bridging SR-TB: Ejemplos

El SR-TB interconecta dominios de source-routing con dominios de bridging transparente uniendo de forma transparente los dominios. Durante la operación, los equipos de ambos dominios desconocen la existencia del SR-TB. Desde el punto de vista del equipo, cualquier equipo en la red combinada parece estar en su propio campo.

Las siguientes secciones proporcionan ejemplos específicos de tramas enviadas durante el bridging SR-TB. Estos ejemplos suponen que el SR-TB está designado bridge broadcast de ruta única. La Figura 4-2 proporciona la siguiente información para acompañar las situaciones descritas en cada sección:

- D es el número de bridge propio del bridge
- X es el número de LAN para la LAN en el lado de source routing

- Y es el número de LAN para la LAN en el lado del bridging transparente
- A, B, C, y D son equipos finales

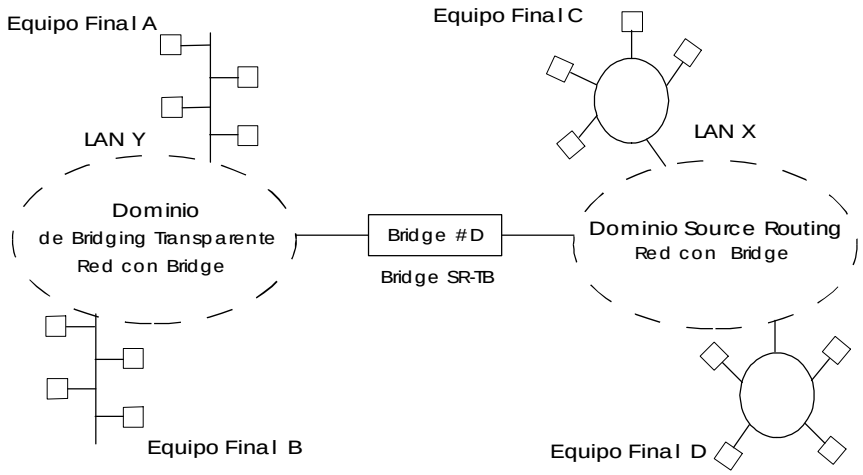


Figura 4-2. Ejemplos de Bridging SR-TB

a) *Ejemplo 1: Trama enviada desde el equipo final A al equipo final B*

Cuando el SR-TB recibe una trama con una dirección de origen del equipo final A y la dirección de destino del equipo final B, pone la dirección del equipo final A dentro de la tabla de dirección del lado de bridging transparente. Esta tabla contiene las direcciones de los equipos que se saben que están en el lado de bridging transparente del bridge. Éste es un comportamiento normal para el bridging transparente.

Si la dirección del equipo final B está en la tabla de dirección del lado de bridging transparente, el SR-TB no envía la trama. Si la dirección del equipo final B no está en la tabla de dirección del lado de bridging transparente y tampoco está en la tabla de dirección del lado de encaminamiento de origen, el SR-TB desconoce su localización. En este caso, el SR-TB reenvía la trama al lado de source routing como broadcast de ruta única sin petición de regreso para el explorador de ruta. Cualquier trama que envíe el equipo final B (sin tener en cuenta su destino) hace que su dirección sea incluida en la tabla de dirección del bridging transparente. Esto previene futuros envíos de tramas direccionadas en el equipo final B en el lado de encaminamiento de origen.

b) *Ejemplo 2: Trama enviada desde el equipo final A al equipo final C*

En este ejemplo, se trata la dirección del equipo final A del mismo modo que en el ejemplo anterior. Debido a que la dirección del equipo final C no está en la tabla de dirección del bridge transparente, el SR-TB envía la trama al lado del source routing.

Entonces el bridge busca la dirección del equipo final C en su tabla de dirección de source routing. Esta tabla contiene todas las direcciones conocidas y la información de routing relacionada para equipos en el lado de source routing del bridge. Si la dirección C está en la tabla de source routing, el bridge envía la trama utilizando la información de routing en la tabla de dirección. Si la dirección C no está en la tabla de source routing (o si aparece pero tiene información de routing nula), el bridge envía la trama al lado de source routing como broadcast de ruta única con petición de regreso del explorador de ruta.

Cuando el equipo final C recibe esta trama, introduce la dirección del equipo final A en su tabla de source routing junto con la dirección contraria del camino construido desde el bridge SR-TB y lo marca como una entrada temporal. Cuando más tarde el equipo final C intenta enviar la trama al

equipo final A, utiliza este camino específico, y como éste está marcado como temporal, la envía como camino no broadcast con petición de regreso del explorador de ruta.

Cuando la trama que regresa llega, el SR-TB la envía al lado de bridge transparente sin información de routing pero pone la ruta hasta el equipo final C en la tabla de source routing como camino temporal. Esto además provoca que la entidad de dirección de red (network management entity, SMT) envíe con retraso una trama exploradora de ruta con un broadcast para todas las rutas al equipo final C. Esto permite al equipo final C seleccionar la ruta óptima para tramas direccionadas al equipo final A, cuyo SR-TB pone después dentro de su tabla de source routing como una ruta permanente.

c) *Ejemplo 3: Trama enviada desde el equipo final C al equipo final D*

Si se envía la trama como no broadcast y cruza el segmento al que está conectado el bridge SR-TB, el bridge escanea el R11 archivado para la secuencia de routing (LAN X a Bridge Q a LAN Y). No puede encontrar la secuencia y por eso no envía la trama.

Si se envía la trama como broadcast de ruta única, el bridge descarta la trama si ya sabe que el equipo final D está en el lado de source routing. Si no lo sabe, envía la trama al lado de bridging transparente (menos la información de routing), y añade Q a Y a la información de routing.

Por último, guarda la información de routing para el equipo final C como ruta temporal en la tabla de source routing con un indicador de no broadcast y la dirección de bit completa.

Si se envía la trama como broadcast de todos los caminos, el SR-TB descarta la trama (porque la dirección del equipo final D no está presente en la tabla de dirección del bridging transparente) y asegura que la dirección del equipo final C está en la tabla de source routing.

d) *Ejemplo 4: Trama enviada desde el equipo final C al equipo final A*

Si se envía la trama como no broadcast, el SR-TB escanea el campo R11 para la secuencia de routing (X a Q a Y). Cuando lo encuentra, envía la trama al lado de bridging transparente. También almacena la información de routing para el equipo final C.

Si se envía la trama como broadcast de ruta única, el SR-TB la envía (menos la información de routing) al lado de bridging transparente y añade Q a Y a la información de routing. También configura el indicador de no broadcast, complementa los bits de dirección, e introduce la información de routing para la dirección de C en su tabla de source routing. Si existe ya una entrada temporal para el equipo final C en la tabla de source routing, el SR-TB actualiza la información de routing.

Si se envía la trama como broadcast de todas las rutas, el SR-TB la descarta, pero asegura que la dirección del equipo final C esté en la tabla de source routing.

5. SR-TB y Frame Relay

La interfaz Frame Relay soporta el bridging SR-TB enviando todas las tramas de bridge al equipo de bridge apropiado, asegurando que el bridging se habilita en el Circuito Virtual Permanente (Permanent Virtual Circuit, PVC).

Capítulo 5
Diversas Características de Bridge

1. Filtrado del Protocolo

Una única plataforma puede llevar a cabo tanto el bridging como el routing. El filtrado del Protocolo determina si los datos entrantes son de routing o se hace bridge con ellos, basándose en los contenidos del campo de dirección

La Tabla 5-1 muestra cómo el contenido del campo de dirección de destino resuelve la pregunta ¿Bridge o Router?.

Si el Direccionamiento MAC de Destino contiene:	**Acción que lleva a cabo el Bridge:**
Dirección de interfaz	Pasa la trama al protocolo configurado que encamina la trama.
Dirección Multicast o Broadcast	Si la trama pertenece a un protocolo configurado, pasa la trama al protocolo de avance. Si no, establece un bridge en la trama.
Otra Unicast	Si la trama pertenece a un protocolo configurado, descarta la trama. Si no, establece un bridge en la trama.

Tabla 5-1. Tabla de Decisión Route/Bridge

2. Característica IBM RT para Tráfico SNA

Algunos PCs IBM (RT PC ejecutando OS/2/EE) ejecutan SNA sobre Ethernet Tipo 2 en lugar de Ethernet 802.3. Esto requiere una cabecera adicional que contiene la longitud de los datos de usuario MAC seguidos por la cabecera 802.2 (LLC).

Se puede activar o desactivar el procesamiento de estas tramas en cada puerto por separado. Si se habilita, el bridge aprende el comportamiento del equipo origen y genera el formato correcto de trama. Pero si no hay información sobre el comportamiento del equipo (equipos multicast o desconocidos), el bridge produce tramas duplicadas, una en formato 802.3 y 802.2, y otra con la cabecera IBM-RT.

3. Encapsulación UB de Tramas XNS

Las tramas Ethernet XNS utilizan Ethertype 0x0600. Con un formato traducido Token Ring, estas tramas obtienen SNAP como se específica en IEEE.802.1H. Debido a que algunos equipos finales Token Ring usan el Ungermann-Bass OUI en el SNAP para estas tramas, hay un interruptor de configuración para activar esta encapsulación.

4. Opciones de Protocolo de Spanning Tree Múltiple

El ASRT permite ampliar las opciones de protocolo de Spanning Tree para cubrir tantas opciones de configuración como sea posible. Las siguientes secciones describen estas características.

4.1. Problemas del Protocolo de Spanning Tree Múltiple

La tecnología del bridging emplea diferentes algoritmos de spanning tree para soportar los distintos métodos de bridging. El propósito común de cada algoritmo es producir una topología sin bucles.

En el algoritmo spanning tree que usan los Bridges Transparentes (TB), se envían las Unidades de Datos de mensajes de Hello del Protocolo Bridge (Hello Bridge Protocol Data Units, BPDUs) y la Notificación de Cambio de Topología (Topology Change Notification, TCN) en una trama transparente a direcciones de grupo bien conocidas por todos las redes participantes (Token Ring, Ethernet, FDDI, etc.). Las tablas se construyen de esta información intercambiada y se calcula una topología sin bucles.

El SRB utiliza tramas transparentes para determinar una topología sin bucles. El algoritmo envía mensajes de Hello BPDUs en una trama transparente a direcciones funcionales bien conocidas. Los bridges SRB no usan TCN BPDUs. La configuración de estado de puerto creada como resultado de este algoritmo de Spanning Tree no afecta a la Trama Exploradora de Todas las Rutas (All Route Explorer, ARE) y al tráfico de Trama de Encaminamiento Específico (Specifically Routed Frame, SRF).

En la configuración de bridging que usan los bridges IBM 8209, se utiliza un método diferente de Spanning Tree para detectar los bridges 8209 paralelos. Este algoritmo usa mensajes de Hello BPDUs enviados como tramas STE a direcciones de grupo IEEE.802.1d en el Token Ring. En el Ethernet, los Saludos BPDUs se envían como tramas transparentes a la misma dirección de grupo. Este método permite a los 8209 construir Spanning Trees con bridges transparentes y otros bridges IBM 8209. De todas formas no participa en el protocolo Spanning Tree SRB, y se filtran los mensajes de Hello BPDUs enviados por los SRB. Como tal, no hay forma de evitar que el 8209 se convierta en el bridge raíz. Si el bridge 8209 se selecciona como raíz, el tráfico entre dos dominios STB podría tener que pasar a través de dominios Token Ring/SRB.

4.2. Ampliación del STP

La característica de ampliación del STP de bridge permite aumentar más el protocolo de Spanning Tree. Basándose en la personalidad del bridge, permite a los bridges tomar parte en el STP apropiado. Anteriormente, los bridges SRB sólo permitían la configuración manual de tree sin bucles en el Token Ring. Éste era el único mecanismo para prevenir los bucles en el caso de bridges SRB paralelos. Añadiendo la característica de ampliación del STP son posibles las siguientes combinaciones de algoritmos de Spanning Tree:

- Bridge Transparente Puro (STB) - protocolo Spanning Tree IEEE 802.1D.
- Bridge de source routing Puro (SRB) – protocolo Spanning Tree IBM SRB.

- Bridges Transparentes y de source routing como entidades separadas – protocolo Spanning Tree IEEE 802.1d para STB y configuración manual para la topología sin bucles del SRB.
- Bridge SR-TB – protocolo para puertos STB de Spanning Tree IEEE 802.1D y BPDUs IBM 8209 en puertos SRB para formar un único árbol de STB y SR-TB. Se permite pasar los mensajes Hello BPDU SRB al dominio DR pero no se procesan.

Los bridges IBM 8209 filtran tales tramas pero esto se permite como un bridge de dos puertos siendo el otro puerto un puerto de bridge transparente.

- Bridge ASRT – protocolo de Spanning Tree IEEE 802.1D se utiliza para hacer un árbol con bridges STB y SRT. Los 8209-como BPDU también se generan en interfaces SRB para hacer un tree con bridges SR-TB y IBM 8209.

Estos mensajes Hello BPDU se procesan tan pronto como se reciben. Esto crea dos mensajes Hello BPDU para ser generados y recibidos en todas las interfaces SR y STB. Debido a que los dos mensajes Hello BPDU transportan la misma información, no hay conflicto de información de puerto. Esto permite al bridge ASRT crear un Spanning Tree con bridges IBM 8209 y SR-TB junto con otros bridge en STB.

Capítulo 6
Utilización del Tunneling IP

1. Túnel de Bridging IP

El túnel de bridging IP es otra característica del software de bridging ASRT. Con la característica túnel de bridging activada, el software encapsula paquetes en los paquetes TCP/IP. Para el router el paquete es como un paquete TCP/IP. Una vez que una trama se encapsula en una envoltura IP, el equipo IP es responsable de seleccionar la interfaz de red apropiada basándose en la dirección de destino IP. Este paquete puede encaminarse de forma dinámica a través de grandes redes de interconexión sin degradación o restricciones de tamaño de red.

El túnel IP es para el bridge como uno de los puertos de bridge que utilizan IP como un dispositivo de entrada/salida de datos. En el puerto de bridge del túnel se puede configurar el comportamiento del bridge como STB, o SRB.

En la configuración SRB, el túnel IP ayuda a superar el límite de distancia habitual (7 saltos) que encontramos en las configuraciones de source routing. También permite conectar equipos finales de source routing a través de soportes físicos que no son de encaminamiento de origen, como por ejemplo las redes Ethernet.

El túnel de bridging también reduce las grandes cantidades de gasto indirecto que provoca el source routing en redes WANs.

Por último reduce la susceptibilidad del source routing a los defectos y fallos de las WAN (si falla un camino, todo el sistema debe reiniciar sus transmisiones).

Los equipos finales ven este camino o túnel como un simple salto, sin reparar en la complejidad de la red de interconexión. La Figura 6.1 muestra un ejemplo de una red de interconexión IP que utiliza la característica de túnel en su configuración.

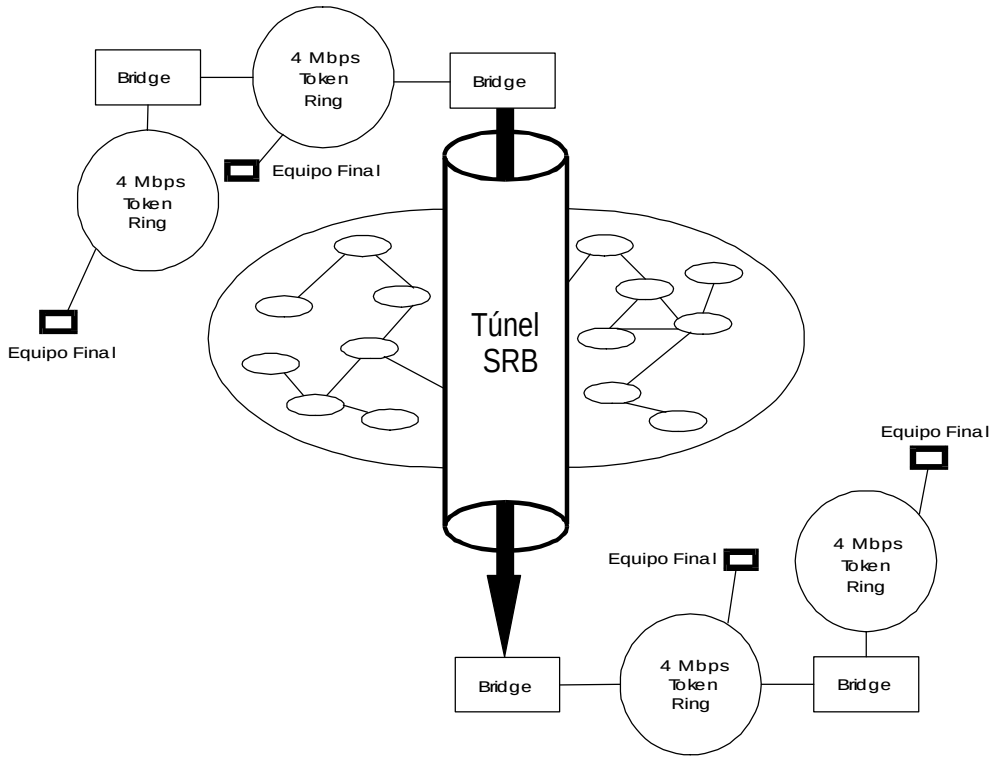


Figura 6.1. Los equipos finales ven el routing a través de una internet IP compleja como un salto

Los bridges participantes en el tunneling tratan la internet IP como un segmento de bridge. Cuando el paquete alcanza la interfaz de destino, las cabeceras TCP/IP se quitan automáticamente y el paquete interno actúa como un paquete estándar de source routing.

1.1. Encapsulación y OSPF

La ventaja que presenta la encapsulación es la posibilidad de añadir al proceso de routing el protocolo de routing dinámico OSPF. El OSPF ofrece las siguientes ventajas cuando se usa con la encapsulación:

- *Coste mínimo de routing*. El OSPF accede al camino más rápido (el túnel) con el menor retraso, permitiendo así a los administradores de red distribuir el tráfico por la ruta más barata.
- *Routing dinámico*. El OSPF busca el camino de coste mínimo, detecta fallos y reencamina el tráfico con gasto indirecto bajo.

Con el OSPF, los túneles dirigen de manera automática las rutas dentro de la red de internconexión. Si una línea o bridge falla en el camino el bridge túnel reencamina automáticamente el tráfico por otra camino nuevo. Si se restaura un camino, el túnel actualiza automáticamente escogiendo el mejor camino. Este reencaminamiento es completamente transparente para los equipos finales.

Capítulo 7
Configuración ASRT

1. Visualización de la Configuración ASRT

Esta sección describe los comandos de configuración de ASRT. Estos permiten especificar los parámetros para el bridge ASRT y sus interfaces. También permiten activar y configurar NetBIOS.

Para visualizar el prompt de configuración `ASRT config>.`

```
Config> PROTOCOL ASRT

-- ASRT Bridge user configuration --
ASRT config>
```

Para tener acceso a los comandos de configuración NetBIOS, hay que introducir **NETBIOS** en el prompt `ASRT config>` para obtener el prompt `NetBIOS config>`.

```
ASRT config> NETBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

2. Comandos de Configuración ASRT

Comando	Función
? (AYUDA)	Visualiza los comandos disponibles.
ADD	Añade direcciones de equipos a la base de datos permanente, proyección de dirección, puertos LAN/WAN, filtros de protocolo y un túnel entre equipos finales con acceso a una red IP.
BAN	Visualiza la configuración del nodo de acceso límite (boundary access node, BAN) o el indicador monitorizado.
CHANGE	Cambia el bridge y los números de segmento.
DELETE	Suprime las entradas de dirección de equipo, proyección de dirección específica, puertos LAN/WAN, filtros de protocolo y un túnel entre equipos finales a través de una red IP.
DISABLE	Desactiva el bridging, duplica tramas proyección entre direcciones de grupo y funcionales, propagación de las tramas exploradoras de spanning tree, encaminamiento de origen, encapsulación de Proteon FDDI, recepción de tramas exploradoras de spanning tree sobre un túnel, transformación de una trama de encaminamiento de origen en trama transparente, bridging transparente (spanning tree) y un túnel entre bridges.
ENABLE	Habilita el bridging, duplica tramas proyección entre direcciones de grupo y funcionales, propagación de las tramas exploradoras de spanning tree, encaminamiento de origen, encapsulación de Proteon FDDI, recepción de tramas exploradoras de spanning tree sobre un túnel, transformación de una trama de encaminamiento de origen en trama transparente, bridging transparente (spanning tree) y un túnel entre bridges.
LIST	Visualiza información la configuración de bridge completa o sobre parámetros de configuración seleccionados.
NETBIOS	Visualiza la configuración del NetBIOS o el indicador monitorizado.
NAME-CACHING	Permite entrar en el menú de configuración de la facilidad Name Caching.
SET	Establece el tiempo de vida para entradas de dirección dinámicas, dirección de bridge, tamaño de trama máximo para el tunneling, codificación de bit de la Trama más Larga (Largest Frame, LF), tamaño de trama máximo, bridge de protocolo spanning tree y parámetros de puerto, valores de Descriptor de Camino (Route Descriptor, RD) y filtrado del tamaño de la basa de datos.
EXIT	Vuelve al prompt anterior.

2.1. ? (HELP)

Hace una lista de los comandos disponibles desde el indicador actual. Después de un comando específico, hace una lista de sus opciones.

Sintaxis:

```
ASRT config> ?
```

Ejemplo:

```
ASRT config> ?
ADD
BAN
CHANGE
DELETE
DISABLE
ENABLE
LIST
NETBIOS
NAME-CACHING
SET
EXIT
ASRT config>
```

2.2. ADD

Añade información a la configuración de bridging. El router no guarda información añadida al indicador monitorizado cuando se reinicia el router.

En el prompt de configuración del ASRT, utilícese **ADD** para añadir la siguiente información a la configuración de bridging:

- Entradas de dirección de equipo a la base de datos permanente
- Proyección de dirección específica para un protocolo
- Puertos LAN/WAN
- Filtros de protocolo que filtran paquetes de forma selectiva basándose en su tipo de protocolo
- Túnel IP entre equipos finales y a través de red IP

Sintaxis:

```
ASRT config> ADD ?
ADDRESS
MAPPING
PROT-FILTER
PORT
TUNNEL
```

a) ADD ADDRESS addr-value

Añade entradas de dirección de equipo único a la base de datos filtrada permanente.

Las entradas de base de datos permanente no se destruyen por el proceso de encendido o apagado y son inmunes a las configuraciones de edad. Las entradas dinámicas no pueden reemplazar entradas permanentes.

El *addr-value* es la dirección de MAC de la entrada deseada. Puede ser una dirección individual, multicast o broadcast. También se puede especificar el mapa de puerto forwarding saliente para cada puerto entrante.

Ejemplo:

```
ASRT config> ADD ADDRESS
Address (in 12-digit hex)[]? 001122334455
Exclude destination address from all ports?(Yes/No)?
Use same output port mapping for all input Ports?(Yes/No)?
Output port mapping:
   Input Port Number[1]?
   Bridge to all ports?(Yes/No)? n
   Bridge to  port 1 -(Yes/No)? y
   Bridge to  port 2 –(Yes/No)? n
   continue to another input port? (Yes/No)? n
Source Address Filtering Applies? (Yes/No)? y
ASRT config>
```

Exclude destination address…	Establece el filtrado de dirección de destino para esa entrada. Sí provoca el filtrado de cualquier trama que contenga esta dirección como dirección de destino, sin importar de qué puerto proceda.
Use same output port mapping…	Sí crea un mapa de puerto saliente para todos los puertos entrantes en lugar de permitir la proyección sólo de puertos específicos. No provoca un indicador nuevo.
Input Port 1, Port 2	Contestar NO al parámetro anterior provoca la introducción en prompt del número del puerto de entrada (`Input Port Number [1]?`) para seleccionar cada puerto de entrada y sus puertos bridge de salida asociados.
Bridge to all ports?	Sí crea un mapa de puerto saliente que incluye todos los puertos. De este modo, cuando se recibe una trama con esta dirección se envía a todos los puertos salientes de envío excepto a los puertos entrantes. Los siguientes son ejemplos de cómo se hace esto de acuerdo con el mapa de puerto: Si se recibe una trama en el puerto 1 y el mapa de puerto indica 1 (para el puerto 1), se filtra la trama. Si se recibe la misma trama en el puerto 2 y el mapa de puerto indica 1 (para el puerto 1) se envía la trama al puerto 1. Si se recibe una trama en el puerto 1 y las direcciones parejas de la entrada del mapa del puerto indica 1, 2 ó 3, se envía la trama a los puertos 2 y 3. Si el mapa de puerto indica sin puerto (NONE/DAF) se filtra la trama. Esto se conoce como filtrado de la dirección de destino (DAF). Si no se encuentra entrada de dirección para emparejar la trama recibida, se envía a todos los puerto de envío (excepto el puerto de origen).
Bridge to port 1, port 2 etc.	Asocia una entrada de dirección con le puerto de bridge específico. Sí proyecta la dirección al puerto especificado por lo que ese puerto se incluye en la entrada de dirección del mapa de puerto. No omite la proyección de dirección para ese puerto.
continue to another input port?	Permite seleccionar el siguiente puerto de entrada para configurarlo.
Source address filtering applies	Permite el filtrado de la dirección de un puerto específico. Sí descarta tramas recibidas con direcciones de origen emparejadas con entradas de dirección en la base de datos filtrada con direcciones de origen filtradas activadas. Esto permite que un director de puerto aísle un equipo final no permitiendo utilizar un bridge en el tráfico.

La siguientes secciones presentan ejemplo de cómo utilizar **ADD ADDRESS** para dirigir entradas de dirección.

Activar la dirección de destino filtrándola para la entrada

```
ASRT config> ADD ADDRESS
Address (in 12-digit hex)[]? 000000334455
Exclude destination address from all ports?(Yes/No)? y
Source Address Filtering Applies? (Yes/No)? n
ASRT config>
```

Tras añadir la dirección, hay que verificar su estatus introduciendo **LIST RANGE**. El siguiente ejemplo muestra que no existe un mapa de puerto para esa entrada (en negrita) y el Filtrado de Dirección de Destino (DAF) está activada.

```
ASRT config> LIST RANGE
Start-Index[1]?
Stop-index[18]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-c2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-c2-00-00-01       RESERVED        NONE/DAF
01-80-c2-00-00-02       RESERVED        NONE/DAF
01-80-c2-00-00-03       RESERVED        NONE/DAF
01-80-c2-00-00-04       RESERVED        NONE/DAF
01-80-c2-00-00-05       RESERVED        NONE/DAF
01-80-c2-00-00-06       RESERVED        NONE/DAF
01-80-c2-00-00-07       RESERVED        NONE/DAF
01-80-c2-00-00-08       RESERVED        NONE/DAF
01-80-c2-00-00-09       RESERVED        NONE/DAF
01-80-c2-00-00-0a       RESERVED        NONE/DAF
01-80-c2-00-00-0b       RESERVED        NONE/DAF
01-80-c2-00-00-0c       RESERVED        NONE/DAF
01-80-c2-00-00-0d       RESERVED        NONE/DAF
01-80-c2-00-00-0e       RESERVED        NONE/DAF
01-80-c2-00-00-0f       RESERVED        NONE/DAF
03-00-00-00-80-00       RESERVED        NONE/DAF
00-00-00-33-44-55       PERMANENT       NONE/DAF
ASRT config>
```

Creación de mapas de puerto de salida separada para una entrada de dirección que tiene más de un puerto de entrada.

```
ASRT config>ADD ADDRESS
Address (in 12-digit hex)[]? 000000012345
Exclude destination address from all ports?(Yes/No)? n
Use same output port mapping for all input Ports?(Yes/No)? n
Output port mapping:
   Input Port Number[1]? 1
   Bridge to all ports?(Yes/No)? n
   Bridge to  port 1 -(Yes/No)? y
   Bridge to  port 2 -(Yes/No)? y
   Bridge to  port 3 -(Yes/No)? n
```

```
   Bridge to  port 4 -(Yes/No)? n
   continue to another input port? (Yes/No)? y
   Input Port Number[2]? 2
   Bridge to all ports?(Yes/No)? n
   Bridge to  port 1 -(Yes/No)? n
   Bridge to  port 2 -(Yes/No)? n
   Bridge to  port 3 -(Yes/No)? y
   Bridge to  port 4 -(Yes/No)? y
   continue to another input port? (Yes/No)? n
Source Address Filtering Applies? (Yes/No)? y
ASRT config>
```

Después de añadir la dirección hay que verificar su estatus introduciendo **LIST RANGE**. El siguiente ejemplo muestra una entrada (en negrita) que tiene los puertos 1 y 2 como puertos de entrada y tiene mapas de puerto separados para ambos puertos de entrada. El Filtrado de la Dirección de Origen (SAF) también está activada.

```
ASRT config> LIST RANGE
Start-Index[1]?
Stop-index[18]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
=======                 ==========      ========
                                        Output ports:

01-80-c2-00-00-01       RESERVED        NONE/DAF
01-80-c2-00-00-02       RESERVED        NONE/DAF
01-80-c2-00-00-03       RESERVED        NONE/DAF
01-80-c2-00-00-04       RESERVED        NONE/DAF
01-80-c2-00-00-05       RESERVED        NONE/DAF
01-80-c2-00-00-06       RESERVED        NONE/DAF
01-80-c2-00-00-07       RESERVED        NONE/DAF
01-80-c2-00-00-08       RESERVED        NONE/DAF
01-80-c2-00-00-09       RESERVED        NONE/DAF
01-80-c2-00-00-0a       RESERVED        NONE/DAF
01-80-c2-00-00-0b       RESERVED        NONE/DAF
01-80-c2-00-00-0c       RESERVED        NONE/DAF
01-80-c2-00-00-0d       RESERVED        NONE/DAF
01-80-c2-00-00-0e       RESERVED        NONE/DAF
01-80-c2-00-00-0f       RESERVED        NONE/DAF
03-00-00-00-80-00       RESERVED        NONE/DAF
00-00-00-01-23-45       PERM/SAF        Input Port:  1
                                        Output ports:  1, 2
                                        Input Port:  2
                                        Output ports:  3, 4

ASRT config>
```

Creación de un único mapa de puerto de salida para todos los puertos que llegan asociados con una entrada de dirección

```
ASRT config> ADD ADDRESS
Address (in 12-digit hex)[]? 000000556677
Exclude destination address from all ports?(Yes/No)? n
Use same output port mapping for all input Ports?(Yes/No)? y
   Bridge to all ports?(Yes/No)? n
   Bridge to  port 1 -(Yes/No)? y
   Bridge to  port 2 -(Yes/No)? y
   Bridge to  port 3 -(Yes/No)? n
   Bridge to  port 4 -(Yes/No)? y
Source Address Filtering Applies? (Yes/No)? y
ASRT config>
```

Después de añadir la dirección hay que comprobar su estatus introduciendo **LIST RANGE**. El siguiente ejemplo muestra una entrada (en negrita) que tiene un único mapa de puerto para todos lo puertos que llegan. El Filtrado de la Dirección de Origen (SAF) está activada.

```
ASRT config> LIST RANGE
Start-Index[1]?
Stop-index[19]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-c2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-c2-00-00-01       RESERVED        NONE/DAF
01-80-c2-00-00-02       RESERVED        NONE/DAF
01-80-c2-00-00-03       RESERVED        NONE/DAF
01-80-c2-00-00-04       RESERVED        NONE/DAF
01-80-c2-00-00-05       RESERVED        NONE/DAF
01-80-c2-00-00-06       RESERVED        NONE/DAF
01-80-c2-00-00-07       RESERVED        NONE/DAF
01-80-c2-00-00-08       RESERVED        NONE/DAF
01-80-c2-00-00-09       RESERVED        NONE/DAF
01-80-c2-00-00-0a       RESERVED        NONE/DAF
01-80-c2-00-00-0b       RESERVED        NONE/DAF
01-80-c2-00-00-0c       RESERVED        NONE/DAF
01-80-c2-00-00-0d       RESERVED        NONE/DAF
01-80-c2-00-00-0e       RESERVED        NONE/DAF
01-80-c2-00-00-0f       RESERVED        NONE/DAF
03-00-00-00-80-00       RESERVED        NONE/DAF
00-00-00-33-44-55       PERMANENT       NONE/DAF
00-00-00-55-66-77       PERM/SAF        Input Port:  ALL PORTS
                                        Output ports:  1, 2, 4

ASRT config>
```

b) ADD MAPPING

Añade una dirección funcional específica a la dirección de grupo mapeada para un indentificador de protocolo. Convierte la proyección de dirección únicamente en direcciones de destino que cruzan del Token Ring a Ethernet o viceversa.

> ***Nota: Para cada valor asignado Ethertype, hay que añadir el correspondiente valor SNAP-type. Esto es necesario para la asignación bidireccional.***

dlh-type	(Tipo cabecero de unión de datos); Las opciones son el Punto de Acceso de Servicio de Destino (Destination Sevice Access Point, DSAP), Ethertype o Protocolo de Acceso Subred (Subnetwork Access Protocol, SNAP).
type-field	Campo de tipo de protocolo.
	Introducir el tipo de protocolo DSAP en una serie de 1 a FE (hexadecimal)
	Introducir el tipo de protocolo Ethernet (Ether) en una serie de 5DD a FFFF (hexadecimal).
	Introducir el tipo de protocolo DSAP en formato de 10 cifras hexadecimal.
ga-address	Dirección de grupo/multicast de 6 byte (12 cifras hexadecimales)
fa-address	Introducir la dirección funcional en formato no canónico. Las direcciones funcionales son direcciones de grupo administradas localmente, principalmente utilizadas en redes Token Ring.

Los valores principalmente utilizados para el mapeo de dirección de grupo a dirección funcional de grupo DECnet son los siguientes:

Ethertype	Dirección de grupo	Dirección funcional
6002	ab-00-00-02-00-00	C0:00:20:00:00:00
6003	ab-00-00-03-00-00	C0:00:10:00:00:00
6003	ab-00-00-00-04-00	C0:00:08:00:00:00

SNAP	Dirección de grupo	Dirección funcional
00-00-00-6002	ab-00-00-02-00-00	C0:00:20:00:00:00
00-00-00-6003	ab-00-00-03-00-00	C0:00:10:00:00:00
00-00-00-6003	ab-00-00-00-04-00	C0:00:08:00:00:00

Ejemplo 1:

```
ASRT config> ADD MAPPING DSAP
Protocol Type in hex (1 - FF)[1]?
Group-Address (in 12-digit hex)[]? ab0000020000
Functional-Address (in noncanonical 12-digit hex)[]? c00020000000
ASRT config>
```

Ejemplo 2:

```
ASRT config> ADD MAPPING ETHER
Protocol Type in hex (5DD - FFFF)[0800]? 6002
Group-Address (in 12-digit hex)[]? ab0000020000
Functional-Address (in noncanonical 12-digit hex)[]? c00020000000
ASRT config>
```

Ejemplo 3:

```
ASRT config> ADD MAPPING SNAP
Address (in 10-digit hex)[0000000800]? 0000006003
Group-Address (in 12-digit hex)[]? ab0000030000
Functional-Address (in noncanonical 12-digit hex)[]? c00010000000
ASRT config>
```

c) ADD PROT-FILTER

Configura el bridge para filtrar paquetes en base a su tipo de protocolo. También descarta los paquetes ARP coincidentes. También se pueden aplicar filtros a todos los puertos o únicamente a los puertos seleccionados.

Están disponibles los siguientes filtros de protocolo:

SNAP packets Protocolo de Acceso de Subred con tipo de protocolo introducido en formato de 10 cifras hexadecimales.

Ether packets Tipo Ethernet con el tipo de protocolo introducido en un rango de 5DD a FFF (Hexadecimal).

DSAP packets Protocolo DSAP con el tipo de protocolo introducido en un rango de 1 a FE (hexadecimal).

No se pueden añadir los protocolos encaminados habilitados al router (los que están visualizados por el comando **CONFIGURATION** en el prompt +) para el filtrado. A continuación están los filtros de protocolo comunes y sus valores.

Tipos DSAP

Protocolo	**SAP (valor hexadecimal)**
Banyan SAP	BC (utilizado sólo para 802.5)
Novell IPX SAP	EO (utilizado sólo para 802.5)
NetBIOS SAP	FO
ISO Connectionless Internet	FE

Identificadores de Protocolo SNAP

Protocolo	**SNAP OUIΛP (10 cifras)**
AppleTalk Phase 2	08-00-07-80-9B
AppleARP Phase 2	00-00-00-80-F3
Proprietary	00-00-93-00-02
AppleTalk Phase 1 for FDDI	
Proprietary	00-00-93-00-03
AppleTalk ARP Phase 1 for FDDI	

Tipos Ethernet

Protocolo	**Tipo Ethernet (valor hexadecimal)**
IP	0800
ARP	0806
CHAOS	0804
DECnet MOP Dump/Load	6000
DECnet MOP Remote Console	6002
DECnet	6003
DEC LAT	6004
DEC LAVC	6007
XNS	0600
Maintenance Packet Type	7030
Apollo Domain	8019 (Ethernet)
Novel NetWare IPX	8137 (Ethernet)
AppleTalk Phase 1	809B
AppleARP Phase 1	80F3
Loopback assistance	9000

Ejemplo 1:

```
ASRT config> ADD PROT-FILTER DSAP
Protocol Type in hex (1 - FE)[1]?
   Filter packets arriving on all ports?(Yes/No)? n
(Yes/No)? nackets arriving on  port 1 -
(Yes/No)? yackets arriving on  port 2 -
ASRT config>
```

Ejemplo 2:

```
ASRT config> ADD PROT-FILTER ETHER
Protocol Type in hex (5DD - FFFF)[0800]?
   Filter packets arriving on all ports?(Yes/No)? y
ASRT config>
```

Ejemplo 3:

```
ASRT config> ADD PROT-FILTER SNAP
Address (in 10-digit hex)[0000000800]?
   Filter packets arriving on all ports?(Yes/No)? y
ASRT config>
```

d) ADD PORT

Añade un puerto LAN/WAN a la configuración de bridge. Asocia un número de puerto con el número de interfaz y habilita la participación de ese puerto en el bridging transparente.

Ejemplo:

```
ASRT config> ADD PORT
Interface Number[0]? 2
Port Number[2]? 2
ASRT config>
```

Si la interfaz es una interfaz Frame Relay, aparece un prompt para asignar un nombre de circuito.

Ejemplo:

```
ASRT config> ADD PORT
Interface Number[0]? 1
Port Number[3]?
Assign circuit name[]? Prueba-01
ASRT config>
```

e) ADD TUNNEL

Crea un túnel IP para un puerto de bridge. Este túnel proporciona un pasillo para una trama de bridge a través de una red IP. Se tiene que activar el IP para utilizar el túnel. Este túnel se considera un único salto entre los bridges sin importar la complicación de la ruta a través de la internet IP.

Sólo se puede añadir un túnel. Se tiene que introducir un número de puerto (*port#*) que no se utilice para ninguna otra interfaz LAN/WAN. Interiormente, el router asigna el número de interfaz 225 para marcar esa interfaz como virtual.

El bridging transparente está habilitado en ese puerto por omisión. Se puede activar el source routing utilizando el comando **ENABLE SOURCE-ROUTING**.

Ejemplo:

```
ASRT config> ADD TUNNEL
Port Number[5]? 5
ASRT config>
```

2.3. BAN

Visualiza el prompt `BAN config>`. Se puede acceder a este prompt introduciendo **BAN** en la guía `ASRT config>` como se ve a continuación.

Sintaxis:

```
ASRT config> BAN
```

Ejemplo:

```
ASRT config> BAN
Boundary Access Node user Configuration
BAN config>
```

2.4. CHANGE

Cambia el bridge de source-routing y los números de segmento en la configuración del bridging.

Sintaxis:

```
ASRT config> CHANGE ?
BRIDGE
SEGMENT
```

a) CHANGE BRIDGE

Cambia los números de bridge en la configuración del bridging.

Ejemplo:

```
ASRT config> CHANGE BRIDGE
Bridge number in hex (1 - 9, A - F)[1]? 2
ASRT config>
```

b) CHANGE SEGMENT

Cambia los números de segmento en la configuración del bridging.

Ejemplo:

```
ASRT config> CHANGE SEGMENT
Old segment number in hex(1 - FFF)[1]?
New segment number in hex(1 - FFF)[1]? 2
ASRT config>
```

2.5. DELETE

El comando **DELETE** borra información.

Sintaxis:

```
ASRT config> DELETE ?
ADDRESS
MAPPING
PROT-FILTER
PORT
```

a) DELETE ADDRESS

Borra la entrada de direcciones MAC de la base de datos permanente.

Introducir el valor añadido en formato hexadecimal de 12 cifras. No se pueden borrar direcciones multicast reservadas. Si se trata de borrar una entrada de dirección que no existe, se recibirá un mensaje:

```
Record matching that address not Found
```

Ejemplo:

```
ASRT config>DELETE ADDRESS
Address (in 12-digit hex)[]? 001122334455
ASRT config>
```

b) DELETE MAPPING

Borra direcciones específicas asignadas para un protocolo determinado.

dlh-type (Data-link-header type); Las opciones son el Punto de Acceso del Servicio de Destino (Destination Service Access Point, DSAP), Ethertype o SNAP.

type-field Campo de tipo de protocolo.

Introducir el tipo de protocolo DSAP en un rango de 1 a FE (hexadecimal).

Introducir el tipo de protocolo Ethernet (Ether) en un rango de 5DD a FFF (hexadecimal).

Introducir el tipo de protocolo Subnetwork Access Protocol (SNAP) en formato hexadecimal de 10 cifras.

ga-address Dirección de grupo /multicast de 6-byte (hexadecimal de 12 cifras).

Sintaxis:

```
ASRT config> DELETE MAPPING ?
DSAP
ETHER
SNAP
```

· DELETE MAPPING DSAP

Ejemplo:

```
ASRT config> DELETE MAPPING DSAP
Protocol Type in hex (1 - FF)[1]? FE
Group-Address (in 12-digit hex)[]? AB0000020000
ASRT config>
```

· DELETE MAPPING ETHER

Ejemplo:

```
ASRT config> DELETE MAPPING ETHER
Protocol Type in hex (5DD - FFFF)[0800]?
Group-Address (in 12-digit hex)[]? ab0000020000
ASRT config>
```

· DELETE MAPPING SNAP

Ejemplo:

```
ASRT config> DELETE MAPPING SNAP
Address (in 10-digit hex)[0000000800]? 0000006002
Group-Address (in 12-digit hex)[]? AB0000020000
ASRT config>
```

c) DELETE PROT-FILTER

Borra los identificadores de protocolo previamente especificados utilizados en el filtrado. Se pueden borrar los filtros de todos los puertos o de los puertos seleccionados. Estos filtros incluyen los siguientes:

SNAP Packets	Protocolo de Acceso a Subred (Subnetwork Access Protocol) con tipo de protocolo introducido en un formato hexadecimal de 10 cifras.
Ethernet Packets	Tipo Ethernet con tipo de protocolo introducido en una escala de 5DD a FFFF (hexadecimal).
DSAP Packets	Protocolo de Punto de Acceso del Servicio de Destino (Destination Service Access Point) con un tipo de protocolo introducido en una escala de 1 a FE (hexadecimal).

Sintaxis:

```
ASRT config> DELETE PROT-FILTER ?
DSAP
ETHER
SNAP
```

· DELETE PROT-FILTER DSAP

Ejemplo:

```
ASRT config> DELETE PROT-FILTER DSAP
Protocol Type in hex (1 - FE)[1]? 1
   Delete filter on all ports?(Yes/No)? yes
ASRT config>
```

· DELETE PROT-FILTER ETHER

Ejemplo:

```
ASRT config> DELETE PROT-FILTER ETHER
Protocol Type in hex (5DD - FFFF)[800]? FFFF
   Delete filter on all ports?(Yes/No)? yes
ASRT config>
```

· DELETE PROT-FILTER SNAP

Ejemplo:

```
ASRT config> DELETE PROT-FILTER SNAP
Address (in 10-digit hex)[0000000800]?
   Delete filter on all ports?(Yes/No)? n
   Delete filter on  port 1 -(Yes/No)? y
   Delete filter on  port 2 -(Yes/No)? n
ASRT config>
```

d) DELETE PORT

Quita un puerto de la configuración de bridge. Ya que la activación del bridge configura por omisión todos los dispositivos de LAN para que tomen parte en el bridging, este comando permite especificar qué dispositivos deben participar o no en el bridging. Normalmente el número de puerto es mayor en

uno que el número de interfaz. Si el número de puerto (port#) es un túnel IP, el número de puerto (*port#*) quita un túnel IP de la configuración de bridge.

Ejemplo:

```
ASRT config> DELETE PORT
Port Number[1]? 1
ASRT config>
```

2.6. DISABLE

Desactiva las siguientes funciones de bridge:

- La funcionalidad de todo el bridging.
- Creación de tramas duplicadas para entornos de bridge mezclados (manejo del tráfico de la red).
- Asignación entre direcciones de grupo y direcciones funcionales.
- Propagación de las tramas exploradoras de spanning tree.
- Source routing en un puerto determinado.
- Recepción de las tramas exploradoras de spanning tree sobre un túnel.
- Transformación de trama de source routing a trama transparente y viceversa.
- Funcionalidad de bridging transparente (spanning tree) en un puerto determinado.

Para la característica de túnel, **DISABLE** desactiva un túnel entre equipos finales en la red IP.

Sintaxis:

```
ASRT config> DISABLE ?
BRIDGE
DLS
DUPLICATE
ETHERTYPE-IBMRT-PC
FA-GA-MAPPING
IBM8209_SPANNING_TREE
SOURCE-ROUTING
SR-TB-CONVERSION
STP
SPANNING-TREE-EXPLORER
TRANSPARENT
TREE
UB-ENCAPSULATION
```

a) DISABLE BRIDGE

Desactiva la funcionalidad del bridging por completo. No elimina los valores de bridging configurados previamente.

Ejemplo:

```
ASRT config> DISABLE BRIDGE
ASRT config>
```

b) DISABLE DLS

Desactiva el DLSw en el bridge. (El router que ejecuta el DLSw aparece como un bridge para los equipos finales).

Ejemplo:

```
ASRT config> DISABLE DLS
ASRT config>
```

c) DISABLE DUPLICATE

Desactiva la creación de tramas duplicadas en entornos de bridge mezclados. El SR-TB en una interfaz 802.5 (con source routing y bridging transparente activados), podría crear inconsistencias cuando se utilizan bridges en las tramas para un destino desconocido o multicast. El bridge no sabe si el destino está en un bridge de source routing (únicamente) o en un bridge transparente.

Para solucionar esto, el bridge emite duplicados de estas tramas (por omisión). Una trama tiene campos de encaminamiento de origen (un spanning tree explorador RIF) y la otra está formateada para el bridging transparente (sin RIF). El comando **DISABLE DUPLICATE** permite eliminar esta duplicación permitiendo desactivar la creación de un de estos tipos de tramas. El comando **DISABLE DUPLICATE** no permite desactivar ambos tipos de tramas de forma simultánea.

El comando **DISABLE DUPLICATE STE** indica al bridge que se abstenga de enviar las tramas exploradoras de spanning tree creadas para el entorno de encaminamiento de origen. El comando **DISABLE DUPLICATE TSF** indica al bridge que se abstenga de emitir tramas de spanning transparente al entorno de bridging transparente. En ambos casos, el bridge normalmente envía los dos tipos de tramas. Desactivar el bridging transparente también desactiva la creación de tramas transparentes.

Sintaxis:

```
ASRT config> DISABLE DUPLICATE ?
STE
TSF
```

- DISABLE DUPLICATE STE

Ejemplo:

```
ASRT config> DISABLE DUPLICATE STE
Port Number[1]? 1
ASRT config>
```

- DISABLE DUPLICATE TSF

Ejemplo:

```
ASRT config> DISABLE DUPLICATE TSF
Port Number[1]? 2
ASRT config>
```

d) DISABLE ETHERTYPE-IBMRT-PC

Desactiva la traducción de tramas SNA a formato Ethernet 2 utilizado por los RT IBM que ejecutan OS/2/EE. Para más información véase el apartado 2 "Característica IBM RT para Tráfico SNA" en el Capítulo 5.

Ejemplo:

```
ASRT config> DISABLE ETHERTYPE-IBMRT-PC
Port Number[1]? 1
ASRT config>
```

e) DISABLE FA-GA-MAPPING

Desactiva la asignación de la dirección de grupo a dirección funcional (y viceversa). En ciertas circunstancias, se puede desactivar la asignación de forma global entre dirección de grupo y dirección funcional.

Ejemplo:

```
ASRT config> DISABLE FA-GA-MAPPING
ASRT config>
```

f) DISABLE IBM8209_SPANNING_TREE

Impide que los bridges participen en los protocolos de spanning tree con bridges IBM 8209.

Ejemplo:

```
ASRT config> DISABLE IBM8209_SPANNING_TREE
ASRT config>
```

g) DISABLE SOURCE-ROUTING

Desactiva el source routing en un puerto determinado para una interfaz de bridge que ya toma parte en el bridging.

Ejemplo:

```
ASRT config> DISABLE SOURCE-ROUTING
Port Number[1]?
ASRT config>
```

h) DISABLE SR-TB-CONVERSION

Desactiva la transformación de la trama de source routing en trama transparente y viceversa.

Ejemplo:

```
ASRT config> DISABLE SR-TB-CONVERSION
ASRT config>
```

i) DISABLE STP

Desactiva la participación del STP para el bridge completo.

Ejemplo:

```
ASRT config> DISABLE STP
ASRT config>
```

j) DISABLE SPANNING TREE-EXPLORER

Impide a un puerto que permita la propagación de tramas exploradoras de spanning tree si está habilitado el source routing. Sólo se debe utilizar este comando si el bridging transparente *no* está habilitado en el puerto. En este caso, está automáticamente de acuerdo con el spanning tree transparente.

Ejemplo:

```
ASRT config> DISABLE SPANNING-TREE-EXPLORER
Port Number[1]? 1
ASRT config>
```

k) DISABLE TRANSPARENT

Desactiva la funcionalidad del bridging transparente en un puerto determinado. Este comando es útil para casos en los que es conveniente un método alternativo de comunicación como el source routing.

Este comando es útil cuando se quiere activar, por ejemplo, el SRB y SR-TB. Sin embargo, el comando tiene riesgos, por lo que se debe utilizar con cuidado. Por ejemplo, su utilización en una interfaz Ethernet desactiva el bridging para esa interfaz. Este comando se utiliza para activar las funcionalidades de bridge SRB y SR-TB.

Ejemplo:

```
ASRT config> DISABLE TRANSPARENT
Port Number[1]? 1
ASRT config>
```

l) DISABLE TREE

Desactiva la participación STP para el bridge en cada puerto.

Ejemplo:

```
ASRT config> DISABLE TREE
Port Number[1]? 2
ASRT config>
```

Nota: La desactivación del STP en cada puerto puede producir bucles en la red debido a la existencia de bridges paralelos.

m) DISABLE UB-ENCAPSULATION

Desactiva la encapsulación Ungermann-Bass OUI para tramas XNS. El bridge sigue remitiendo tramas XNS tanto a Ethernet como Token Ring utilizando, como es habitual, la encapsulación SNAP con un OUI de todo ceros.

Ejemplo:

```
ASRT config> DISABLE UB-ENCAPSULATION
ASRT config>
```

2.7. ENABLE

Habilita las siguientes funciones:

- Toda la funcionalidad del bridging
- La creación de tramas duplicadas para entornos de bridging mezclados (tratamiento del tráfico de la red)
- La asignación entre dirección de grupo y dirección funcional
- La propagación de tramas exploradoras de spanning tree
- El source routing en puerto determinado
- La recepción de tramas exploradoras de spanning tree sobre un túnel
- La transformación de una trama de source routing en una trama transparente y viceversa
- La funcionalidad de bridging transparente (spanning tree) en puerto determinado.

Para la característica de túnel, **ENABLE** habilita un túnel entre equipos finales a través de una red IP.

Sintaxis:

```
ASRT config> ENABLE ?
BRIDGE
DLS
DUPLICATE
ETHERTYPE-IBMRT-PC
FA-GA-MAPPING
IBM8209_SPANNING_TREE
SOURCE-ROUTING
SR-TB-CONVERSION
SPANNING-TREE-EXPLORER
STP
TRANSPARENT
TREE
UB-ENCAPSULATION
```

a) ENABLE BRIDGE

Habilita el bridging transparente en todos los dispositivos LAN (interfaces) configurados en el router. Asigna números de puerto a cada interfaz como el número de interfaz anterior más 1. Por ejemplo, si la interfaz 0 es un dispositivo LAN, su número de puerto es 1.

Ejemplo:

```
ASRT config> ENABLE BRIDGE
ASRT config>
```

b) ENABLE DLS

Habilita el DLSw sobre el bridge. El router que ejecuta el DLSw es como un bridge para los equipos finales.

Ejemplo:

```
ASRT config> ENABLE DLS
ASRT config>
```

c) ENABLE DUPLICATE

Habilita la generación de tramas duplicadas STE (Spanning Tree Explorer) o TSF (Transparent Spanning Frames). Este comando está disponible para contrarrestar el comando **DISABLE DUPLICATE**. La generación de trama duplicada está activada por omisión. El comando **ENABLE DUPLICATE** puede estar seguido por una trama del tipo **TSF** o **STE** para activar específicamente uno de los tipos de trama, o para el tipo de trama **BOTH** que da el mismo resultado que un tipo de trama no especificado.

Sintaxis:

```
ASRT config> ENABLE DUPLICATE ?
BOTH
STE
TSF
PORT
```

- *ENABLE DUPLICATE BOTH*

Ejemplo:

```
ASRT config> ENABLE DUPLICATE BOTH
Port Number[1]? 2
ASRT config>
```

- *ENABLE DUPLICATE STE*

Ejemplo:

```
ASRT config> ENABLE DUPLICATE STE
Port Number[1]? 2
ASRT config>
```

- *ENABLE DUPLICATE TSF*

Ejemplo:

```
ASRT config> ENABLE DUPLICATE TSF
Port Number[1]? 1
ASRT config>
```

- *ENABLE DUPLICATE PORT*

Ejemplo:

```
ASRT config> ENABLE DUPLICATE PORT
Port Number[1]? 2
ASRT config>
```

d) ENABLE ETHERTYPE-IBMRT-PC

Activa la traducción de tramas SNA a formato Ethernet 2 utilizado por los RT IBM que ejecutan OS/2/EE. Para más información véase la sección 2 “Característica IBM RT para Tráfico SNA” en el Capítulo 5.

Ejemplo:

```
ASRT config> ENABLE ETHERTYPE-IBMRT-PC
Port Number[1]? 1
ASRT config>
```

e) ENABLE FA-GA-MAPPING

Habilita la asiganción de direcciones de grupo a direcciones funcionales y viceversa. Se necesita esto para remitir tramas entre Token Ring y otros medios (excepto línea de serie). En Token Rings, las direcciones funcionales están más generalizadas aunque son direcciones de grupo asignadas de manera local debido a restricciones del hardware. Otros medios usan comúnmente direcciones de grupo. En circunstancias normales la asignación entre direcciones de grupo y dirección funcional es inevitable. La asignación está habilitada por omisión si se han añadido direcciones asignadas. Activar/desactivar la asignación permite tener una posibilidad llegado el caso de borrar registros de asignaciones añadidas.

Ejemplo:

```
ASRT config> ENABLE FA-GA-MAPPING
ASRT config>
```

f) ENABLE IBM8209_SPANNING_TREE

Permite a los bridges participar en protocolos Spanning Tree con bridges IBM 8209.

Ejemplo:

```
ASRT config> ENABLE IBM8209_SPANNING_TREE
ASRT config>
```

g) ENABLE SOURCE-ROUTING

Habilita el source routing para un puerto determinado. Se utiliza este comando cuando se quiere utilizar el source routing en parte del bridge. Si el source routing es la única característica que se quiere, hay que desactivar el bridging transparente en la interfaz. La primera vez que se escribe el comando se debe escribir el número de bridge. Posteriormente ya no es necesario.

port# Puerto válido que participa en la configuración de bridge.

segment# Número de 12-bit que representa el LAN/WAN a los que los medios están ligados. Todos los medios en otros bridges ligados a este LAN/WAN se deben configurar con el mismo valor. Para el correcto funcionamiento del source routing, es muy importante que todos los bridges ligados a este LAN/WAN tengan la misma perspectiva del valor de identificación LAN/WAN.

bridge# Valor único de 4-bit entre todos los bridges ligados al mismo LAN/WAN. Este valor se requiere cuando se habilita el source routing en la primera interfaz. Para interfaces posteriores, esta entrada es opcional. Se recomienda que el número de bridge (*bridge#*) sea único en el segmento.

Nota: Si la configuración es una situación donde dos segmentos ya han sido configurados (por ejemplo una configuración 1:N SRB), se mueve por un parámetro de segmento virtual # adicional.

Ejemplo:

```
ASRT config> ENABLE SOURCE-ROUTING
Port Number[1]? 2
Segment Number for the port in hex(1 - FFF)[1]? 3
Bridge Virtual Segment Number in hex(1 - FFF)[1]? 2
ASRT config>
```

h) ENABLE SR-TB-CONVERSION

Se permite para la compatibilidad entre dominios de source routing y bridging transparente. Cuando está activada esta característica, el bridge permite que se acepten las tramas de encaminamiento de origen en dominios de bridging transparente quitando los RIF y convirtiéndolos en tramas transparentes.

El bridge también reúne información del routing relacionada a los equipos de source routing desde los RIF de tramas de source routing pasajeras. Utiliza esta información RIF para convertir tramas transparentes en tramas de encaminamiento de origen. Si un RIF no está disponible para un equipo, el bridge envía la trama como una trama exploradora de spanning tree en el dominio de source routing.

Para que la transformación opere correctamente, se debe dar al dominio de bridging transparente un número de segmento. Hay que configurar los bridges SR-TB conectados a ese dominio con el mismo número de segmento.

Ejemplo:

```
ASRT config> ENABLE SR-TB-CONVERSION
TB-Domain Segment Number in hex(1 - FFF)[1]?
Bridge Virtual Segment Number in hex(1 - FFF)[1]?
TB-Domain's MTU[1470]? 1400
TB-Domain's MTU is adjusted to 1350
ASRT config>
```

i) ENABLE SPANNING-TREE-EXPLORER

Permite al puerto admitir la propagación de tramas exploradoras spanning tree si está habilitado el source routing. Este comando es válido en puertos Token Ring y WAN únicamente. Esta característica está activada por omisión cuando está configurado el source routing en el puerto.

Ejemplo:

```
ASRT config> ENABLE SPANNING-TREE-EXPLORER
Port Number[1]? 2
ASRT config>
```

j) ENABLE STP

Habilita a participación del STP para todo el bridge.

Ejemplo:

```
ASRT config> ENABLE STP
ASRT config>
```

k) ENABLE TRANSPARENT

Habilita la funcionalidad de bridging transparente en un puerto determinado. En circunstancias normales, este comando no es necesario.

Ejemplo:

```
ASRT config> ENABLE TRANSPARENT
Port Number[1]? 2
ASRT config>
```

l) ENABLE TREE

Habilita la participación del STP para el bridge por puerto.

Ejemplo:

```
ASRT config> ENABLE TREE
Port Number[1]? 2
ASRT config>
```

m) ENABLE UB-ENCAPSULATION

Hace que las tramas XNS Ethernet 2 se traduzcan en Token Ring utilizando el Ungermann-Bass OUI en la cabecera SNAP. Hay que enviar las tramas Token Ring que contengan la cabecera UB OUI a Ethernets como tramas del tipo 0x0600 Ethernet 2, en lugar de cómo tramas del tipo 802.3/802.2.

Ejemplo:

```
ASRT config> ENABLE UB-ENCAPSULATION
ASRT config>
```

2.8. LIST

Visualiza información sobre la configuración completa del bridge o sobre parámetros seleccionados de la configuración.

Sintaxis:

```
ASRT config> LIST ?
ADDRESS
BRIDGE
FILTERING
MAPPING
PERMANENT
PORT
PROT-FILTER
PROTOCOL
RANGE
```

a) LIST ADDRESS

Lee una entrada de dirección de la base de datos permanente.

Ejemplo:

```
ASRT config> LIST ADDRESS
Address (in 12-digit hex)[]? 000000123456
00-00-00-12-34-56         PERMANENT     Input Port:  ALL PORTS
                                        Output ports:  1, 2

ASRT config>
```

Ejemplo:

```
ASRT config> LIST ADDRESS
Address (in 12-digit hex)[]? 001122334455
00-11-22-33-44-55         PERM/SAF      Input Port:  1
                                        Output ports:  1, 2

ASRT config>
```

Address	Entrada de dirección en formato hexadecimal de 12 cifras	
Entry Type	*Permanent*	La entrada es permanente y sobrevive a los encendidos/apagados del sistema y a los reinicios.
	Reserved	La entrada está reservada por el comité IEEE802.1d para su uso futuro. Las tramas para direcciones reservadas son descartadas.
	Registered	La entrada se debe al propio bridge.
	SAF	Aparece después del tipo de entrada si se configura el filtrado de dirección de origen.
Input Port	Los números de puerto(s) de entrada relacionados con esa entrada de dirección.	
Output Port	Los números de puerto(s) de salida relacionados con esa entrada de dirección. NONE/DAF indican que el filtrado de dirección de destino se emplea porque ningún puerto ha sido seleccionado para estar relacionado con esa entrada de dirección.	

b) LIST BRIDGE

Hace una lista de toda la información general relacionada con el bridge.

Ejemplo:

```
ASRT config> LIST BRIDGE

                Source Routing Transparent Bridge Configuration
              ===================================================

Bridge:    Enabled                              Bridge behavior: ADAPTIVE SRT
                   +---------------------------------------+
-------------------|       SOURCE ROUTING INFORMATION      |-----------------
                   +---------------------------------------+
Bridge Number:           01                     Segments:          1
Max ARE Hop Cnt:         14                     Max STE Hop cnt:  14
1:N SRB:                 Active                 Internal Segment:  0x001
LF-bit interpret:        Extended
                   +---------------------------------------+
-------------------|            SR-TB INFORMATION          |-----------------
                   +---------------------------------------+
SR-TB Conversion:        Enabled
TB-Virtual Segment:      0x001                  MTU of TB-Domain:  1350
                   +---------------------------------------+
-------------------|    SPANNING TREE PROTOCOL INFORMATION |-----------------
                   +---------------------------------------+
Bridge Address:          Default                Bridge Priority:   32768/0x8000
STP Participation:       IEEE802.1d and IBM-8209
                   +---------------------------------------+
-------------------|        TRANSLATION INFORMATION        |-----------------
                   +---------------------------------------+
FA<=>GA Conversion:      Enabled                UB-Encapsulation:  Enabled
DLS for the bridge:      Enabled
                   +---------------------------------------+
-------------------|            PORT INFORMATION           |-----------------
                   +---------------------------------------+
Number of ports added: 2
Port:   1      Interface:       0      Behavior:   STB & SRB   STP: Enabled

Port:   2      Interface:       1      Behavior:    STB Only   STP: Enabled
 Circuit name: test


ASRT config>
```

Bridge	Indica si el bridge está habilitado o desactivado.
Bridge Behavior	El método de bridging que se está utilizando. Los valores son el STB para el transparente, SRB para el source routing y el SR-TB para el bridging transformado de source routing a transparente.
Bridge Address	Dirección de bridge especificada por el usuario (si está establecida).
Bridge Priority	Una dirección de bridge de octetos de orden superior que se encuentra en el identificador de bridge, al igual que el MAC que se obtiene del puerto de número más bajo de la dirección establecida por el comando **SET BRIDGE**.
Bridge Number	Distingue entre los múltiples bridges que están conectados a los dos mismos anillos.
Number of Source Routing Segments	El número de los segmentos del bridge de source routing configurados para el dominio de source routing.

SRB: Max ARE/STE Hop cnt	El número máximo de saltos para tramas que transmiten desde el bridge a una interfaz determinada asociada con el bridging de source routing.
SR-TB Conversion	Indica si la transformación de trama de bridge de source routing/transparente está activada o no.
TB-Virtual Segment	El número de segmento del dominio de bridging transparente.
MTU for TB-Domain	El tamaño máximo de trama (unidades máximas de transmisión) que el bridge transparente puede transmitir y recibir.
1:N Source Routing	El estado actual del encaminamiento de origen 1:N ACTIVO o NO ACTIVO.
Internal Virtual Segment	Visualiza el número de segmento virtual configurado para el bridging SRB 1:N.
SRB LF-bit interpretation	Indica el modo de interpretación de codificación del bit más largo (LF) de la trama si el source routing está activado en este bridge (BÁSICO o EXTENDIDO).
FA-GA conversion	Indica si la transformación FA-GA está activada o no.
Spanning Tree Protocol Participation	Los tipos de protocolo de spanning tree en los que toma parte el bridge.
Number of ports added	El número de puertos de bridge añadidos a la configuración del bridging.
Port Number	Un número definido por el usuario que se asigna a una interfaz utilizando el comando **ADD PORT**.
Interface Number	Identifica los dispositivos que están conectados a un segmento de red por medio de un bridge. Se deben añadir al menos dos interfaces para que participen en el bridging. Utilizar el valor 225 para el bridging.
Port Behavior	Indica el método de bridging que está utilizando ese puerto. Los valores son STB para el transparente, SRB para el source routing y SR-TB para el bridging de transformación de source routing transparente.

c) LIST FILTERING

Muestra los parámetros asociados al filtrado del bridge.

Ejemplo:

```
ASRT config> LIST FILTERING
Filtering Database Size : 2048
Ageing Time (in seconds): 300
Resolution  (in seconds): 5
ASRT config>
```

Filtering Database Size: número de entradas que se pueden tener en la base de datos de filtrado de bridge.

Ageing Time: tiempo de desaparición de las entradas dinámicas en la base de datos de filtrado.

Resolution: resolución temporal.

Más información disponible en los comandos **SET AGE**, y **SET FILTERING**.

d) LIST MAPPING

Hace una lista del mapeo de dirección específica para un protocolo determinado.

Sintaxis:

```
ASRT config> LIST MAPPING ?
DSAP
ETHER
SNAP
```

- *LIST MAPPING DSAP*

Ejemplo:

```
ASRT config> LIST MAPPING DSAP

PROTOCOL TYPE           GROUP ADDRESS           FUNCTIONAL ADDRESS
=============           =============           ==================
aa                      01-02-03-04-05-06        0a:0b:0c:0d:0e:0f

ASRT config>
```

- *LIST MAPPING ETHER*

Ejemplo:

```
ASRT config> LIST MAPPING ETHER

PROTOCOL TYPE           GROUP ADDRESS           FUNCTIONAL ADDRESS
=============           =============           ==================
ffee                    01-01-01-02-02-02        aa:bb:cc:dd:ee:ff

ASRT config>
```

- *LIST MAPPING SNAP*

Ejemplo:

```
ASRT config> LIST MAPPING SNAP

PROTOCOL TYPE           GROUP ADDRESS           FUNCTIONAL ADDRESS
=============           =============           ==================
000000-0800             ab-00-00-02-00-00        c0:00:20:00:00:00

ASRT config>
```

e) LIST PERMANENT

Visualiza el número de entradas en la base de datos permanente del bridge.

Ejemplo:

```
ASRT config> LIST PERMANENT
Number of entries in Permanent Database: 19
ASRT config>
```

f) LIST PORT

Visualiza la información de puerto relacionada a puertos ya configurados. El router pregunta por el puerto del que se quiere hacer una lista. Si no se especifica el número ([-1]) visualiza todos los puertos.

Ejemplo:

```
ASRT config> LIST PORT
Port Number[-1]?
Port Id (dec)    : 128: 1, (hex): 80-01
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging and Source Routing
SRB: Segment Number: 0x002       MTU:  4399     STE Forwarding: Disabled
Duplicates Frames Allowed:   STE: No   , TSF: Yes
Assoc Interface  : 0
Path Cost        : 0
IBM RT-PC Ethertype (0x80D5) processing is enabled
------------------------------------------------------------------------------
Port Id (dec)    : 128: 2, (hex): 80-02
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 1  Circuit name: prueba
Path Cost        : 0
------------------------------------------------------------------------------
ASRT config>
```

Port ID	El ID consiste en dos partes: la prioridad de puerto y el número de puerto. En el ejemplo, 128 es la prioridad y 1, 2 y 3 el número de puerto. En formato hexadecimal, el byte de orden inferior indica el número de puerto y el byte de orden superior la prioridad.
Port State	Si el puerto está o no activado.
Port Supports	Visualiza el método de bridging soportado por el puerto (por ejemplo, el bridging transparente, el bridging de source routing).
SRB	Sólo se visualiza cuando está activado el SRB y hace una lista de la información del bridging de source routing. Ésta incluye el número de segmento SRB (en hexadecimal), el tamaño de Unidad de Transmisión Máxima y si la transmisión de las Tramas Exploradoras de Spanning Tree está activada o no.
Duplicate Frames Allowed	Visualiza una interrupción y el total de los tipos de tramas duplicadas que se permiten.
Assoc Interface	Número de interfaz asociado con el puerto que se visualiza, y el nombre del circuito FR si corresponde.
Path Cost	Coste asociado con el puerto que se utiliza para posibles costes de ruta de origen. El rango es de 1 a 65535.

Nota: Si está activado el procesamiento de tipo de Ether IBM RT-PC aparece en esta visualización. Si no está activado, no aparece su estatus.

g) LIST PROT-FILTER

Lee una lista actual de los tipos de protocolo de filtrado. Se puede hacer una lista de los filtros de forma selectiva por puertos o visualizar todos los puertos a la vez. Port Number selecciona el puerto de bridge del que se quiere hacer una lista.

Ejemplo:

```
ASRT config> LIST PROT-FILTER
Port Number[-1]?
No DSAP Filter Records Associated
Protocol Class: ETHER
Protocol Type : 0800
Protocol State: FILTERED
Port Map      : 1, 2
==========================
No SNAP Filter Records Associated
ASRT config>
```

Port Number	Se visualiza para cada puerto si se hace una lista de todos los puertos.
Protocol Class	Visualiza la clase de protocolo (SNAP, Ether, o DSAP).
Protocol Type	Protocolo ID en formato hexadecimal.
Protocol State	Indica que ese protocolo se está filtrando para un puerto seleccionado.

h) LIST PROTOCOL

Visualiza información del bridge relacionada con el protocolo de spanning tree.

Ejemplo:

```
ASRT config> LIST PROTOCOL
Bridge Identifier               : 32768/000000000000 (using port address)
Bridge-Max-Age (in seconds)     : 20
Bridge-Hello-Time (in seconds)  : 2
Bridge-Forward-Delay (in seconds): 15
ASRT config>
```

Nota: Cada uno de estos parámetros relacionados con el bridge está también descrito con detalle en los capítulos anteriores.

Bridge Identifiers	Valor de 8 bytes en formato ASCII. Si no se establece la dirección de bridge antes de visualizar esta información, los seis bytes de orden inferior visualizados como cero indican la dirección por defecto MAC de un puerto. Cuando se selecciona un bridge como el bridge origen, transmite la duración máxima del bridge y el tiempo de los mensajes "Hello" del bridge a todos los bridges de la red a través de los mensajes de "Hello" BPDUs.

Bridge-Max-Age La duración máxima (período de tiempo) que debe utilizarse para interrumpir la información relacionada con el protocolo de spanning tree.

Bridge-Hello-Time Intervalo de tiempo entre los mensajes de "Hello" BPDUs.

Bridge-Forward-Delay Intervalo de tiempo que se utiliza antes de cambiar a otro estado (si este bridge debe convertirse el origen).

i) LIST RANGE

Lee un rango de entradas de dirección de la base de datos permanente. Para hacerlo, primero hay que determinar el tamaño de la base de datos utilizando para ello la del comando de **LIST PERMANENT**. De este valor se determina después un valor de índice de inicio para el rango de entrada. El índice de inicio es único para el tamaño de la base de datos. Después se puede elegir un índice de detención para visualizar un número limitado de entradas. Esta entrada es opcional. Si no se proporciona el índice de detención, el valor predeterminado es el tamaño de la base de datos. Las entradas de dirección contienen la siguiente información:

Ejemplo:

```
ASRT config> LIST RANGE
Start-Index[1]? 17
Stop-index[19]? 19
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
03-00-00-00-80-00       RESERVED        NONE/DAF
00-00-00-12-34-56       PERMANENT       Input Port:  ALL PORTS
                                        Output ports:  1, 2

00-11-22-33-44-55       PERM/SAF        Input Port:  1
                                        Output ports:  1, 2

ASRT config>
```

Address Dirección MAC de 6 bytes de la entrada.

Entry Type Especifica uno de los siguientes tipos:

- *Reserved* Reservado por el comité IEEE802.1d.
- *Registered* Direcciones unicast pertenecientes al hardware de comunicaciones propietario relacionado con las direcciones box o multicast activadas por los enviadores de protocolo.
- *Permanent* Entradas introducidas en el proceso de configuración que sobreviven a lo apagados y encendidos o a los reinicios del sistema.
- *Static* Entradas introducidas en el proceso de monitorización que no sobreviven a los apagados y encendidos o a los reinicios del sistema y que son eternas.
- *Dynamic* Entradas que aprende el bridge de forma dinámica que no sobreviven a los encendidos y apagados o a los reinicios del sistema y cuya duración está relacionada con ellos.
- *Free* Localizaciones en la base de datos que se pueden llenar libremente con entradas de direcciones.

Port Map Mapa de puerto saliente para todos los puertos entrantes.

2.9. NETBIOS

Visualiza el prompt de configuración NetBIOS. Introducir **NETBIOS** en el prompt `ASRT config>` para visualizar el prompt de configuración NetBIOS.

Véase el Capítulo 10 "Comandos de Filtrado y Cache NetBIOS", para una explicación de los comandos NetBIOS.

Sintaxis:

```
ASRT config> NETBIOS
```

Ejemplo:

```
ASRT config> NETBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

Nota: Si usted no ha adquirido la característica NetBIOS, recibirá el siguiente mensaje si utiliza este comando:

```
NetBIOS Support not in load.
```

2.10. NAME-CACHING

Utilizar el comando **NAME-CACHING** para entrar en el menú de configuración de la facilidad Name Caching.

Sintaxis:

```
ASRT config> NAME-CACHING
Name Cache Config>
```

Comandos	Función
? (AYUDA)	Visualiza todos los comandos Name-caching de configuración, o lista las opciones de un comando específico.
DISABLE	Deshabilita la facilidad Name-caching y el filtrado de tramas duplicadas.
ENABLE	Habilita la facilidad Name-caching y el filtrado de tramas duplicadas.
LIST	Permite mostrar las configuraciones Name-caching actualmente implentadas.
PORT	Selecciona el interfaz al cual se van a aplicar los comandos Name-caching.
TIMER	Configura el temporizador de entrada desocupada, el temporizador del servidor, y el tiempo durante el cual se filtran las tramas duplicadas.
EXIT	Permite salir del prompt de configuración de Name-caching.

a) ? AYUDA

Utilizar el comando **?** para obtener un listado de los comandos disponibles en el nivel de prompt actual. También se puede introducir ? después de un comando específico para visualizar todas sus opciones.

Ejemplo:

```
Name Cache Config> ?
DISABLE
ENABLE
LIST
PORT
TIMER
EXIT
```

b) DISABLE

Deshabilita la facilidad Name-caching y el filtrado de tramas duplicadas.

Sintaxis:

```
Name Cache Config> DISABLE ?
ADD-NAME-FILTERING
NAME-CACHING
```

- #### DISABLE ADD-NAME-FILTERING

Deshabilita el filtrado de tramas duplicadas. Las tramas duplicadas pueden ser ADD-NAME o ADD-GROUP-NAME.

Ejemplo:

```
Name Cache Config> DISABLE ADD-NAME-FILTERING
Name Cache Config>
```

- #### DISABLE NAME-CACHING

Deshabilita la facilidad Name-caching.

Ejemplo:

```
Name Cache Config> DISABLE NAME-CACHING
Name Cache Config>
```

c) ENABLE

Habilita la facilidad Name-caching y el filtrado de tramas duplicadas.

Sintaxis:

```
Name Cache Config> ENABLE ?
ADD-NAME-FILTERING
NAME-CACHING
```

- *ENABLE ADD-NAME-FILTERING*

Habilita el filtrado de tramas duplicadas. Las tramas duplicadas pueden ser ADD-NAME o ADD-GROUP-NAME.

Ejemplo:

```
Name Cache Config> ENABLE ADD-NAME-FILTERING
Name Cache Config>
```

- *ENABLE NAME-CACHING*

Habilita la facilidad Name-caching.

Ejemplo:

```
Name Cache Config> ENABLE NAME-CACHING
Name Cache Config>
```

d) LIST

Utilizar el comando **LIST** para mostrar las configuraciones Name-caching actualmente implentadas.

Ejemplo:

```
Name Cache Config> LIST

  Server name caching:      Enabled
  Server timeout:           3
  Add name frame filtering: Enabled
  Add name frame timeout:   7
  Entry timeout:            900

Name Cache Config>
```

e) PORT

Utilizar el comando **PORT** para seleccionar el puerto del bridge al cual se van a aplicar los comandos Name-caching de configuración.

Ejemplo:

```
Name Cache Config> PORT
Port[1]? 2
Name Cache Port Config>
```

Una vez dentro del prompt *Name Cache Port Config>*, están disponibles los siguientes comandos

Sintaxis:

```
Name Cache Port Config> ?
DISABLE
ENABLE
LIST
EXIT
```

f) TIMER

Utilizar el comando **TIMER** para configurar el temporizador de entrada desocupada , el temporizador del servidor, y el tiempo durante el cual se filtran las tramas duplicadas.

Sintaxis:

```
Name Cache Config> TIMER ?
ADD-NAME
ENTRY
SERVER-RESPONSE
```

- *TIMER ADD-NAME*

Configura el tiempo durante el cual se filtran tramas duplicadas. El valor por defecto es 7 segundos.

Ejemplo:

```
Name Cache Config> TIMER ADD-NAME
Time in seconds (1-32) [7]?
Name Cache Config>
```

- *TIMER ENTRY*

Configura el temporizador de entrada desocupada. Si un cliente y servidor no hace referencia al nombre de la entrada dentro del intervalo de tiempo configurado en este temporizador, la entrada se rechaza. El valor por defecto es 900 segundos.

Ejemplo:

```
Name Cache Config> TIMER ENTRY
Time in seconds (10-65535) [900]?
Name Cache Config>
```

- *TIMER SERVER-RESPONSE*

Configura la respuesta del servidor. Si un servidor no responde a una petición nombre dentro del tiempo configurado, la información MAC y RIF de la entrada se convierte en inválida. El valor por defecto es 3 segundos.

Ejemplo:

```
Name Cache Config> TIMER SERVER-RESPONSE
Time in seconds (1-16) [3]?
Name Cache Config>
```

g) EXIT

Utilizar el comando **EXIT** para volver al prompt ASRT.

Ejemplo:

```
Name Cache Config> EXIT
ASRT config>
```

2.11. SET

Utilizar el comando **SET** para establecer los siguientes parámetros:

- Tiempo de duración para entradas de dirección dinámica en la base de datos de filtrado.
- Dirección de bridge.
- Interpretación de la codificación del bit de Trama más Larga (Largest Frame -LF-) para el source routing.
- Tamaño del MAC Service Data Unit (MSDU).
- Bridge del protocolo de spanning tree protocol bridge y parámetros de puerto.
- Límite del Route Descriptor (RD).
- Tamaño de la base de datos de filtrado de bridge.

Sintaxis:

```
ASRT config> SET ?
AGE
BRIDGE
FILTERING
LF-BIT-INTERPRETATION
MAXIMUM-PACKET-SIZE
PORT
PROTOCOL
ROUTE-DESCRIPTOR-LIMIT
```

a) SET AGE

Establece el tiempo de desaparición de las entradas dinámicas en la base de datos de filtrado cuando el puerto con la entrada está en estado de envío. Esta duración también se usa para las entradas RIF de duración en la tabla RIF en el caso de una personalidad de bridge SR-TB.

El valor por omisión del temporizador de duración es 300 segundos con un rango de 1 a 1.000.000 segundos. El valor predeterminado para el parámetro de resolución es 5, con un rango de 1 a 60 segundos.

Ejemplo:

```
ASRT config> SET AGE
seconds[300]? 250
resolution[5]?
ASRT config>
```

b) SET BRIDGE

Establece la dirección de bridge. En casos en que una interfaz de línea serie (o túnel) es el puerto con menor número, se debe utilizar este comando de manera que el bridge tenga una única dirección cuando se reinicia. Esto es necesario porque las líneas serie no tienen su propia dirección MAC.

Ejemplo:

```
ASRT config> SET BRIDGE
Bridge Address (in 12-digit hex)[]? 001122334455
ASRT config>
```

Nota: Cada bridge de la red debe tener una única dirección para que el protocolo de spanning tree opere correctamente.

Ésta es la dirección de bridge de orden inferior de 6 octetos en el identificador de bridge. Por defecto, *la dirección de bridge* está establecida a la dirección MAC (Media Access Control) del puerto numerado más bajo en la inicialización. Se puede utilizar este comando para no hacer caso de la dirección por omisión e introducir su propia dirección única.

No utilizar guiones o dos puntos para separar cada octeto. Si se introduce la dirección en un formato erróneo se recibe el mensaje

```
Illegal Address
```

Si no se introduce una dirección en el prompt, se recibirá el mensaje

```
Zero length address supplied
```

y el bridge mantiene su valor previo. Para volver a la dirección de bridge por defecto, introducir una dirección con todo ceros.

c) SET FILTERING

Establece el número de entradas que se pueden tener en la base de datos de filtrado de bridge. El valor por defecto es 1024 veces el número de puertos de bridge. Para más información véase el comando **LIST FILTERING** en este capítulo.

Ejemplo:

```
ASRT config> SET FILTERING
database-size[2048]?
ASRT config>
```

d) SET LF-BIT-INTERPRETATION

Establece la interpretación de la codificación del bit de Trama más Larga (LF) si está activado el source routing en este bridge.

Sintaxis:

```
ASRT config> SET LF-BIT-INTERPRETATION ?
BASIC
EXTENDED
```

- #### SET LF-BIT-INTERPRETATION BASIC

En modo **BASIC** sólo se usan tres bits del campo de control de routing. Esto es algo normal en los bridges de source routing existentes hoy en día. Los nodos **EXTENDED** y **BASIC** son compatibles.

Ejemplo:

```
ASRT config> SET LF-BIT-INTERPRETATION BASIC
ASRT config>
```

- #### SET LF-BIT-INTERPRETATION EXTENDED

En modo **EXTENDED**, se utilizan seis bits del campo de control de routing para representar la unidad de datos máxima que soporta el bridge. El valor predeterminado es **EXTENDED**. Los nodos **EXTENDED** y **BASIC** son compatibles.

Ejemplo:

```
ASRT config> SET LF-BIT-INTERPRETATION EXTENDED
ASRT config>
```

e) SET MAXIMUM-PACKET-SIZE

Establece el tamaño más largo del MAC Service Data Unit (MSDU) para el puerto, si está activado el source routing en ese puerto. Evidentemente, establecer el MSDU no tiene consecuencias en los medios tradicionalmente transparentes. Un valor MSDU mayor que el tamaño de paquete configurado en el router se toma como un error.

El valor por defecto es el tamaño configurado como tamaño del paquete para ese interfaz.

Ejemplo:

```
ASRT config> SET MAXIMUM-PACKET-SIZE
Port Number[1]? 2
MSDU size[4399]? 4000
MSDU is adjusted to 2052
ASRT config>
```

f) SET PORT

Permite Habilitar o Deshabilitar un puerto del bridge.

Sintaxis:

```
ASRT config> SET PORT ?
BLOCK
DISABLE
```

- #### SET PORT BLOCK

Habilita un puerto de los que tiene configurado el bridge.

Ejemplo:

```
ASRT config> SET PORT BLOCK
Port Number[1]? 2
ASRT config>
```

- #### SET PORT DISABLE

Deshabilita un puerto de los que tiene configurado el bridge. El estado del puerto pasa a Disabled.

Ejemplo:

```
ASRT config> SET PORT DISABLE
Port Number[1]? 2
ASRT config>
```

g) SET PROTOCOL

Modifica el bridge de protocolo de spanning tree o los parámetros de puerto para una nueva configuración o para sintonizar los parámetros de configuración para adaptar una topología específica.

- #### SET PROTOCOL BRIDGE

Introducir **PROTOCOL BRIDGE** para modificar con este comando como se explica más abajo.

Cuando se establecen estos valores, hay que asegurarse de que las siguientes relaciones existen entre los parámetros o la entrada será descartada:

2 * (Retraso de encaminamiento del Bridge - 1 segundo) > Duración Máxima del Bridge

Duración Máxima del Bridge > 2 * (Tiempo de mensaje de Hello del Bridge + 1 segundo)

Ejemplo:

```
ASRT config> SET PROTOCOL BRIDGE
Bridge-Max-Age[20]? 25
Bridge-Hello-Time[2]?
Bridge-Forward-Delay[15]? 17
Bridge-Priority[32768]?
ASRT config>
```

Bridge Maximum Age	Duración máxima (período de tiempo) utilizada para temporizar la información relacionada del protocolo de spanning tree.
Bridge Hello Time	Intervalo de tiempo entre mensajes Hello BPDUs.
Bridge Forward Delay	Intervalo de tiempo antes de cambiar a otro estado (este bridge debe convertirse en origen).
Bridge Priority	Una dirección de bridge de orden superior de 2 octetos que se encuentra en el Identificador de Bridge, pudiendo ser tanto la dirección MAC obtenida del puerto de número más bajo como la dirección establecida por el comando **SET BRIDGE**.

- #### SET PROTOCOL PORT

Introducir **PROTOCOL PORT** para modificar los parámetros de puerto de protocolo de spanning tree.

Ejemplo:

```
ASRT config> SET PROTOCOL PORT
Port Number[1]?
Port Path-cost (0 for default)[0]?
Default Path Cost is Selected
Port Priority[128]?
ASRT config>
```

Port Number	Número de puerto de bridge; selecciona el puerto para el que el coste de ruta y la prioridad de puerto se cambiaran.
Path Cost	Coste asociado con el puerto que se utiliza para posible coste de ruta origen. La escala es 1 a 65535. 0 indica coste de ruta por defecto.
Port Priority	Identifica la prioridad de puerto para el puerto específico. El rango es de 0 a 255.

h) SET ROUTE-DESCRIPTOR-LIMIT

Permite asociar un largo máximo de Route Descriptor (RD) para las tramas All Route Explorer (ARE) o Spanning Tree Explorer (STE) enviadas por el bridge si está activado el source routing.

Sintaxis:

```
ASRT config> SET ROUTE-DESCRIPTOR-LIMIT ?
ARE
STE
```

- **SET ROUTE-DESCRIPTOR-LIMIT ARE**

Introducido como ARE si el parámetro *RD-limit-value* está aplicado al All Route Explorer (ARE).

Ejemplo:

```
ASRT config> SET ROUTE-DESCRIPTOR-LIMIT ARE
RD-limit-value (Hop count)[14]?
ASRT config>
```

- **SET ROUTE-DESCRIPTOR-LIMIT STE**

Introducido como STE dependiendo de si el parámetro *RD-limit-value* está aplicado al Spanning Tree Explorer (STE).

Ejemplo:

```
ASRT config> SET ROUTE-DESCRIPTOR-LIMIT STE 10
ASRT config>
```

RD-limit-value	Especifica el número máximo de RDs que pueden contenerse en el Routing Information Field (RIF) del tipo de trama especificado por el tipo de límite RD. Este campo toma valores de 0 a 14. El valor límite por defecto RD para tramas ARE y STE es 14.

2.12. EXIT

Utilizar el comando para volver al prompt *Config>*.

Sintaxis:

```
ASRT config> EXIT
```

Ejemplo:

```
ASRT config> EXIT
Config>
```

Capítulo 8
Monitorización ASRT

1. Visualización de la Monitorización ASRT

Esta sección describe los comandos de monitorización de ASRT. Estos permiten especificar los parámetros para el bridge ASRT y sus interfaces. También permiten activar y monitorizar NetBIOS.

Para visualizar el prompt de monitorización ASRT>

```
+ PROTOCOL ASRT
ASRT>
```

Nota: El bridge tiene que estar habilitado para poder acceder a la monitorización ASRT.

Para tener acceso a los comandos de monitorización NetBIOS, hay que introducir **NETBIOS** en el prompt ASRT> para obtener el prompt NetBIOS>.

```
ASRT> NETBIOS

NetBIOS Support User Console

NetBIOS>
```

2. Comandos de Monitorización ASRT

Comando	Función
? (HELP)	Visualiza los comandos disponibles.
ADD	Añade direcciones de equipos a la base de datos permanente, proyección de dirección, puertos LAN/WAN, filtros de protocolo y un túnel entre equipos finales con acceso a una red IP.
BAN	Visualiza la configuración del nodo de acceso límite (boundary access node, BAN) o el indicador monitorizado
CACHE	Visualiza las entradas de la memoria asociada para un puerto específico
DELETE	Suprime las entradas de dirección de equipo, proyección de dirección específica, puertos LAN/WAN, filtros de protocolo y un túnel entre equipos finales a través de una red IP.
FLIP	Revisa la dirección MAC de canónico al formato 802.5 (no canónico o IBM)
LIST	Visualiza información la configuración de bridge completa o sobre parámetros de configuración seleccionados.
NETBIOS	Visualiza la configuración del NetBIOS o el indicador monitorizado
NAME-CACHING	Permite entrar en el menú de monitorización de la facilidad Name Caching
EXIT	Vuelve al indicador anterior.

2.1. ? (AYUDA)

Hace una lista de los comandos disponibles desde el indicador actual. Después de un comando específico, hace una lista de sus opciones.

Sintaxis:

```
ASRT> ?
```

Ejemplo:

```
ASRT> ?
ADD
BAN
CACHE port_number
DELETE mac_address
FLIP mac_address
LIST
NETBIOS
NAME-CACHING
EXIT
ASRT>
```

2.2. ADD

En el prompt de monitorización ASRT, añade la siguiente información a la configuración de bridging. (Estos añadidos a la base de datos no sobreviven después de un reinicio).

Sintaxis:

```
ASRT> ADD ?
DESTINATION-ADDRESS-FILTER mac_address
STATIC-ENTRY mac_address input_port [output_ports...]
```

a) ADD DESTINATION-ADDRESS-FILTER

Añade un filtro de dirección de destino a la base de datos permanente del router.

Ejemplo:

```
ASRT> ADD DESTINATION-ADDRESS-FILTER
Destination MAC address [00-00-00-00-00-00]? 00-01-02-03-04-05
ASRT>
```

b) ADD STATIC-ENTRY

Añade entradas de dirección estática a la base de datos permanente del router. Los puertos de salida son opcionales.

Para crear una entrada estática con múltiples mapas de puerto (uno por puerto de entrada), introducir el comando varias veces.

Ejemplo:

```
ASRT> ADD STATIC-ENTRY
MAC address [00-00-00-00-00-00]? 11-22-33-44-55-66
input port, 0 for any[0]?
output port, 0 for none[0]? 1
output port, 0 to end[0]? 0
ASRT>
```

2.3. BAN

Visualiza el prompt BAN>. Se puede acceder a este prompt introduciendo **BAN** en el prompt ASRT> como se ve a continuación.

Sintaxis:

```
ASRT> BAN
```

Ejemplo:

```
ASRT> BAN
Boundary Access Node Console
BAN>
```

2.4. CACHE

Visualiza los contenidos de la memoria cache de routing de un puerto de bridging seleccionado. Si el puerto no tiene una memoria cache, se verá el mensaje:

```
PORT DOESN'T HAVE A CACHE
```

Sintaxis:

```
ASRT> CACHE <port#>
```

Ejemplo:

```
ASRT>CACHE
Port Number[1]? 2
MAC Address    MC*  Entry Type       Age  Port(s)
00-00-93-00-c0-d0   Dynamic           20  2 (TKR/1)
ASRT>
```

MAC Address — Dirección MAC de 6 bytes de la entrada.

Entry Type — Visualiza uno de los siguientes tipos de entrada de dirección:

- *Reserved* — Reservado por el Estándar IEEE802.1D.
- *Registered* — Direcciones unicast pertenecientes al hardware de comunicaciones propietario adjunto a las direcciones multicast activada para los encaminadores de protocolo.
- *Permanent* — Entradas configuradas del usuario.
- *Static* — Entradas de monitorización.
- *Dynamic* — Aprendidas por el bridge de forma dinámica. No sobreviven al encendido o apagado o a los sitemas de reinicializar y su tiempo de duración está relacionado con la entrada.
- *Free* — Localizaciones en la base de datos que se pueden llenar por las entradas de direcciones.
- *Unknown* — Desconocido para el bridge. Pueden ser fallos y/o direcciones ilegales.

Age — Edad en segundos de cada entrada dinámica. La edad puede disminuir en cada intervalo de resolución.

Port(s) — El número de puerto relacionado con la entrada. Visualiza el nombre de la interfaz (siempre que la interfaz tenga una memoria cache).

2.5. DELETE

Borra las entradas de dirección de estación (MAC) de la base de datos.

Sintaxis:

```
ASRT> DELETE <dirección MAC>
```

Ejemplo:

```
ASRT> DELETE
MAC address [00-00-00-00-00-00]? 00-01-02-03-04-05
ASRT>
```

2.6. FLIP

Permite examinar las direcciones específicas MAC en los formatos canónicos y no canónicos repasando el formato de la dirección. El comando **FLIP** traduce direcciones IEEE 802.5 de su formato típico no canónico al formato canónico utilizado universalmente por el procedimiento de monitorización de bridge y ELS y viceversa.

Sintaxis:

```
ASRT> FLIP <dirección MAC>
```

Ejemplo:

```
ASRT> FLIP
MAC address [00-00-00-00-00-00]? 01-02-03-04-05-06
IEEE 802 canonical bit order:    01-02-03-04-05-06
IBM Token-Ring native bit order: 80:40:c0:20:a0:60

ASRT>
```

2.7. LIST

Visualiza información sobre la monitorización completa del bridge o sobre parámetros seleccionados de la monitorización.

Sintaxis:

```
ASRT> LIST ?
ADAPTIVE
BRIDGE
CONVERSION
DATABASE
FILTERING
PORT
SOURCE-ROUTING
SPANNING-TREE-PROTOCOL
TRANSPARENT
TUNNEL
```

a) LIST ADAPTIVE

Hace una lista de toda la información general relativa al bridge SR-TB que transforma entre tipos de bridging. Hay un número de opciones de grupo de datos generales que pueden visualizarse con **LIST ADAPTIVE**. Estos incluyen los siguientes:

- *Config* - Visualiza la información general relacionada con el bridge SR-TB.
- *Counters* - Visualiza todos los contadores del bridge SR-TB.
- *Database*- Visualiza los contenidos de la base de datos RIF del bridge SR-TB.

Sintaxis:

```
ASRT config> LIST ADAPTIVE ?
CONFIG
COUNTERS
DATABASE
```

- ### LIST ADAPTIVE CONFIG

Ejemplo:

```
ASRT> LIST ADAPTIVE CONFIG
Adaptive bridge:            Enabled
Translation database size:  0
Aging time:                 15 seconds
Aging granularity           5 seconds

Port  Segment  Interface      State       MTU  DUP:TSF STE
   1  001      TKR/0          Enabled     2052      Yes   Yes
   -  001      Adaptive       Enabled     1470
ASRT>
```

Adaptive bridge	Estado actual del bridge transformado SR-TB, tanto activado como desactivado.
Translation database size	Tamaño actual de la base de datos del SR-TB, que contiene direcciones MAC y RIFs asociados al dominio de source routing.
Aging time	Temporizador de la duración establecido en segundos. Todas las entradas de la base de datos RIF SR:TB que superen este límite de tiempo se descartan.
Aging granularity	Las veces que se escanean las entradas para encontrar el vencimiento de acuerdo con el temporizador de duración.
Port	Número del puerto relacionado con el bridging de transformación.

Segment	Número de segmento de encaminamiento de origen asignado al puerto relacionado con el bridging de transformación.
Interface	Dispositivo conectado a un segmento de red del bridge de transformación.
State	Estado actual del puerto del bridge de transformación.
MTU	Tamaño máximo de la trama (desde el final del RIF hasta el principio del FCS) que el bridge de transformación puede transmitir y recibir.
DUP: TSF STE	Indica si se envían tramas STE duplicadas (Spanning Tree Explorer) o TSF (Transparent Spanning Frames).

- *LIST ADAPTIVE COUNTERS*

Ejemplo:

```
ASRT> LIST ADAPTIVE COUNTERS
Hash collision count:                0
Adaptive database overflow count:    0
ASRT>
```

Hash Collision Count	Número de direcciones que fueron almacenadas (mediante función hash) en la misma localización en la tabla hash. Este número es acumulativo y refleja el número total de incidentes de colisión hash que se producen. Los aumentos en este número pueden indicar un problema del tamaño de la tabla potencial.
Adaptive Database Overflow	Número de veces que una dirección se ha sobrescrito mientras que la tabla de base de datos de transformación se quedaba sin espacio.

- *LIST ADAPTIVE DATABASE*

El comando **LIST ADAPTIVE DATABASE** permite seleccionar determinadas porciones de la base de datos RIF del bridge adaptativo para visualizarlas. Esto se debe al tamaño potencial de la base de datos. Las opciones de visualización incluyen las siguientes:

ADDRESS	- Visualiza los datos sobre una dirección que se encuentra en la base de datos.
ALL-SEGMENTS	- Visualiza la base de datos completa.
PORT	- Visualiza todas las entradas del bridge de transformación para un puerto específico.
SEGMENT	- Visualiza todas las entradas del bridge de transformación relacionadas con el puerto que tiene el número de segmento especificado.

Los ejemplos siguientes muestran cada una de las opciones de este comando.

Nota: Estos sólo se visualizan si está activado el bridging adaptable.

Ejemplo 1:

```
ASRT> LIST ADAPTIVE DATABASE ADDRESS
MAC address [00-00-00-00-00-00]? 00a026400ba4
Canonical MAC address:           00-a0-26-40-0b-a4
IBM Token-Ring native address:   80:05:64:02:d0:25
Via port:                        1 (TKR/0       )
Entry age:                       315
RIF Routing type:                ARE (100)
RIF length:                      6
RIF Direction:                   1
RIF Largest frame:               1470
RIF Route Descriptor  LAN ID     Bridge Number
1                     100        1
2                     200        0
ASRT>
```

Ejemplo 2:

```
ASRT> LIST ADAPTIVE DATABASE ALL-SEGMENTS
Canonical Address  Interface    Port  Seg    Age  RIF: Type Direct   Length  LF
IBM MAC Address    RIF

00-00-93-78-b7-3a  TKR/0            1  100    310       ARE  Reverse   6      1470
80:00:c9:1e:ed:5c  869010012000

00-a0-26-40-0b-a4  TKR/0            1  100    320       ARE  Reverse   6      1470
80:05:64:02:d0:25  869010012000

ASRT>
```

Ejemplo 3:

```
ASRT> LIST ADAPTIVE DATABASE PORT
Port number[1]? 2
Canonical Address  Interface    Port  Seg    Age  RIF: Type Direct   Length  LF
IBM MAC Address    RIF

00-0a-83-78-b7-a4  TKR/1            2  200    300       ARE  Reverse   6      1470
80:00:c9:1e:ed:25  869010011000

ASRT>
```

Ejemplo 4:

```
ASRT> LIST ADAPTIVE DATABASE SEGMENT
Segment number[1]? 100
Canonical Address  Interface    Port  Seg    Age  RIF: Type Direct   Length  LF
IBM MAC Address    RIF

00-00-93-78-b7-3a  TKR/0            1  100    315       ARE  Reverse   6      1470
80:00:c9:1e:ed:5c  869010012000

00-a0-26-40-0b-a4  TKR/0            1  100    320       ARE  Reverse   6      1470
80:05:64:02:d0:25  869010012000

ASRT>
```

La siguiente información se visualiza para cada entrada:

Canonical address	Dirección MAC del nodo correspondiente a esta entrada visualizada en el formato no canónico de IBM.
Interface	Nombre de la interfaz de red que aprendió esta entrada.
Port	Número del puerto que aprendió esta entrada de dirección.
Seg	Número del segmento que aprendió esta dirección.
Age	Duración de la entrada en segundos.
RIF Type	Tipo de RIF (SRF, STE, o ARE).
RIF Direction	Dirección de RIF (Adelante o Atrás).
RIF Length	Largo de RIF en bytes.
RIF LF	Valor más largo de la trama en el RIF.
RIF	Campo de Información de Encaminamiento RIF (Routing Information Field) aprendido de este nodo.

b) LIST BRIDGE

Hace una lista de toda la información general relacionada con el bridge.

Ejemplo:

```
ASRT> LIST BRIDGE
Bridge ID (prio/add):  32768/00-a0-26-40-0c-e4
Bridge state:          Enabled
UB-Encapsulation:      Disabled
Bridge type:           SR-TB
Bridge capability:     ASRT
Number of ports:       2
STP Participation:     IEEE802.1d on TB ports and IBM-8209 on SR ports

                                                        Maximum
Port   Interface      State     MAC Address          Modes  MSDU  Segment  Flags
   1   TKR/0          Up        00-a0-26-40-0c-e4    SR     2096     100     RD
   2   Eth/0          Up        00-a0-26-40-0c-e5        T  1514             RD

Flags:  RE = IBMRT PC behavior Enabled,  RD = IBMRT PC behavior Disabled

SR bridge number:      1
SR virtual segment:    000
Adaptive segment:      200
ASRT>
```

Bridge ID (prio/add)	Identificador del bridge.
Bridge State	Indica si el bridging está activado o no.
UB-Encapsulation	Indica si está habilitada o no el encapsulado UB.
Bridge Type	El tipo de bridge configurado (None, SRB, STB, SRT, SR-TB o ASRT).
Bridge capability	Capacidad del bridge (ASRT, STB, SRB o STB/SRB).
Number of Ports	Número de puertos configurados para ese bridge.
STP Participation	Tipo de participación en el Protocolo Spaning Tree.
Port	Número asignado a una interfaz utilizando el comando **ADD PORT**.
Interface	Dispositivos conectados a un segmento de red por medio de un bridge.
State	El estado actual del puerto (Up o Down).
MAC address	La dirección MAC asociada con ese puerto en formato canónico.

Modes	El modo de bridging para ese puerto. *T* indica el bridging transparente. *SR* indica source routing. *A* indica bridging adaptable.
MSDU	El tamaño máximo de trama (unidad de datos) (incluyendo el cabecero MAC pero no el campo FCS) que el bridge de source routing puede transmitir y recibir en esta interfaz.
Segment	El número de segmento de bridge de source routing asignado a ese puerto (si lo hay).
FLAGS	Indica si está habilitado el IBM RT.
SR bridge number	El número de bridge de source routing asignado por el usuario.
SR virtual segment	EL número de segmento virtual del bridge de source routing, si lo hay.
Adaptive segment	EL número de segmento utilizado en el dominio de source routing para encaminar hacia el dominio transparente.

c) LIST CONVERSION

Visualiza información general sobre las normas del bridge para la conversión de los formatos de tramas basándose en el tipo de trama. Se puede visualizar los siguientes grupos de datos generales con el comando **LIST CONVERSION**.

Sintaxis:

```
ASRT> LIST CONVERSION ?
ALL
ETHERTYPE
SAP
SNAP
```

- #### LIST CONVERSION ALL

Visualiza todas las normas.

Ejemplo:

```
ASRT> LIST CONVERSION ALL
Ethernet type 0800 translations:
Group ab-00-00-04-00-00 <=> Functional c0-00-08-00-00-00 (03:00:10:00:00:00)

IEEE 802.2 destination SAP 01 translations:
Group ab-00-00-01-00-00 <=> Functional c0-00-30-00-00-00 (03:00:0c:00:00:00)

IEEE 802 SNAP PID 00-00-00-60-02 translations:
Group ab-00-00-02-00-00 <=> Functional c0-00-20-00-00-00 (03:00:04:00:00:00)

ASRT>
```

- #### LIST CONVERSIÓN ETHERTYPE

Visualiza las normas para todos los tipo de Ethernet o para un tipo específico de Ethernet.

Ejemplo:

```
ASRT> LIST CONVERSION ETHERTYPE
Ethernet type (in hexadecimal), 0 for all[0]?
Ethernet type 0800 translations:
Group ab-00-00-04-00-00 <=> Functional c0-00-08-00-00-00 (03:00:10:00:00:00)

ASRT>
```

- *LIST CONVERSIÓN SAP*

Visualiza las normas para todos los identificadores de protocolo SAP o un tipo específico SAP 802.2.

Ejemplo:

```
ASRT> LIST CONVERSION SAP
SAP (in hexadecimal), 100 for all[100]?
IEEE 802.2 destination SAP 01 translations:
Group ab-00-00-01-00-00 <=> Functional c0-00-30-00-00-00 (03:00:0c:00:00:00)

ASRT>
```

- *LIST CONVERSIÓN SNAP*

Visualiza las normas para todos los identificadores de protocolo SNAP o un tipo específico SNAP 802.2.

Ejemplo:

```
ASRT> LIST CONVERSION SNAP
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-60-02 translations:
Group ab-00-00-02-00-00 <=> Functional c0-00-20-00-00-00 (03:00:04:00:00:00)

ASRT>
```

d) LIST DATABASE

Hace una lista de los contenidos de las bases de datos de filtrado transparente. Se pueden elegir los siguientes grupos de datos para visualizarlos con el comando **LIST DATABASE.**

Sintaxis:

```
ASRT> LIST DATABASE ?
ALL-PORTS
DYNAMIC
LOCAL
PERMANENT
PORT port_number
RANGE mac_address mac_address
STATIC
```

- *LIST DATABASE ALL-PORTS*

Visualiza la base de datos completa del bridging transparente.

Ejemplo:

```
ASRT> LIST DATABASE ALL
MAC Address    MC*  Entry Type       Age  Port(s)

00-00-0c-07-ac-00   Dynamic          320  2 (Eth/0       )
00-00-0c-07-ac-0d   Dynamic          320  2 (Eth/0       )
00-00-24-31-33-c1   Dynamic          315  2 (Eth/0       )
00-00-b4-95-33-bc   Dynamic          280  2 (Eth/0       )
00-00-c0-57-eb-6b   Dynamic          275  2 (Eth/0       )
00-00-c0-6a-eb-6b   Dynamic          120  2 (Eth/0       )
00-60-08-79-33-4d   Dynamic          315  2 (Eth/0       )
00-60-08-79-33-5a   Dynamic          315  2 (Eth/0       )
00-60-52-02-83-42   Dynamic          130  2 (Eth/0       )
00-60-97-13-8c-cd   Dynamic          220  2 (Eth/0       )
00-60-97-13-8d-77   Dynamic          235  2 (Eth/0       )
00-60-97-27-bc-c6   Dynamic          315  2 (Eth/0       )
00-60-97-3c-48-f4   Dynamic          250  2 (Eth/0       )
00-60-97-3e-52-d5   Dynamic          235  2 (Eth/0       )
00-60-97-3e-53-cb   Dynamic          290  2 (Eth/0       )
00-60-97-3e-53-d6   Dynamic           10  2 (Eth/0       )
00-60-97-3e-53-d7   Dynamic          320  2 (Eth/0       )
00-60-97-3e-6c-07   Dynamic          315  2 (Eth/0       )
00-60-97-3e-6d-a7   Dynamic           75  2 (Eth/0       )
00-80-5f-43-bc-ec   Dynamic          190  2 (Eth/0       )
00-80-5f-a6-04-d0   Dynamic          295  2 (Eth/0       )
00-a0-24-23-d3-8a   Dynamic          110  2 (Eth/0       )
00-a0-26-40-0e-ec   Dynamic          320  2 (Eth/0       )
00-a0-26-40-10-ac   Dynamic          285  2 (Eth/0       )
00-a0-26-5c-4e-26   Dynamic          195  2 (Eth/0       )
00-a0-c9-a7-e6-66   Dynamic          320  2 (Eth/0       )
00-b0-64-b8-8b-40   Dynamic          300  2 (Eth/0       )
00-c0-4f-0a-37-f2   Dynamic          320  2 (Eth/0       )
00-c0-4f-9c-11-b7   Dynamic          230  2 (Eth/0       )
00-c0-4f-9c-12-2a   Dynamic          310  2 (Eth/0       )
00-d0-58-35-d2-e0   Dynamic          270  2 (Eth/0       )
01-80-c2-00-00-00*  Registered            1
01-80-c2-00-00-01*  Reserved              All
01-80-c2-00-00-02*  Reserved              All
01-80-c2-00-00-03*  Reserved              All
01-80-c2-00-00-04*  Reserved              All
01-80-c2-00-00-05*  Reserved              All
01-80-c2-00-00-06*  Reserved              All
01-80-c2-00-00-07*  Reserved              All
```

```
01-80-c2-00-00-08*  Reserved              All
01-80-c2-00-00-09*  Reserved              All
01-80-c2-00-00-0a*  Reserved              All
01-80-c2-00-00-0b*  Reserved              All
01-80-c2-00-00-0c*  Reserved              All
01-80-c2-00-00-0d*  Reserved              All
01-80-c2-00-00-0e*  Reserved              All
01-80-c2-00-00-0f*  Reserved              All
03-00-00-00-80-00*  Reserved              All
08-00-09-a3-04-21   Dynamic          270  2 (Eth/0       )
08-00-20-83-56-ff   Dynamic          320  2 (Eth/0       )
08-00-4e-09-ba-4c   Dynamic          320  2 (Eth/0       )
08-00-4e-12-da-34   Dynamic          205  2 (Eth/0       )
08-00-5a-93-6d-fa   Dynamic          305  2 (Eth/0       )

ASRT>
```

Nota: Los campos descritos se visualizan para todas la opciones del comando de la base de datos de la lista.

MAC Address — Una dirección en formato hexadecimal de 12 cifras (formato canónico).

*MC** — Un asterisco detrás de una entrada de dirección indica que la entrada tiene un flag que la identifica como una dirección multicast.

Entry Type — Especifica uno de los siguientes tipos:

- *Reserved* — Reservado por el estándar IEEE802.1D.
- *Registered* — Formado por direcciones unicast pertenecientes a interfaces que participan en el bridge o direcciones multicast activadas por los encaminadores de protocolo.
- *Permanent* — Introducido en el proceso de configuración y sobrevive a los encendidos/apagados o los reinicios del sistema.
- *Static* — Introducido en el proceso de monitorización, no sobrevive a los encendidos/apagados o reinicios del sistema y no tienen duración.
- *Dynamic* — Aprendido por el bridge de forma dinámica y no sobreviven a los encendidos/apagados o reinicios del sistema y tienen una duración relacionada con la entrada.
- *Free* — Este tipo no se utiliza y no se debe ver excepto en condiciones ocasionales de *race* entre el proceso de monitorización y el bridge.
- *Unknown* — Tipo de entrada desconocido. Puede indicar un fallo del software. Informe al Servicio de Atención al Cliente sobre el tipo de entrada hexadecimal.

Age — La duración (en segundos) de cada entrada dinámica. La duración decrece en cada intervalo de resolución.

Port(s) — El número(s) del puerto saliente para esa entrada. También se hace una lista del tipo de dispositivo para entradas únicas de puerto. Si hay una entrada dinámica de túnel IP, el puerto es 5 para el túnel IP.

• LIST DATABASE DYNAMIC

Visualiza todas las entradas dinámicas (aprendidas) de la base de datos de dirección.

Ejemplo:

```
ASRT> LIST DATABASE DYNAMIC
MAC Address     MC*  Entry Type       Age  Port(s)

00-00-0c-07-ac-00   Dynamic          315  2 (Eth/0       )
00-00-0c-07-ac-0d   Dynamic          315  2 (Eth/0       )
00-00-24-31-33-c1   Dynamic          140  2 (Eth/0       )
00-00-b4-95-33-bc   Dynamic          250  2 (Eth/0       )
00-00-c0-57-eb-6b   Dynamic          175  2 (Eth/0       )
00-00-c0-6a-eb-6b   Dynamic           50  2 (Eth/0       )
00-00-e8-41-ad-13   Dynamic          315  2 (Eth/0       )
ASRT>
```

- *LIST DATABASE LOCAL*

Visualiza todas las entradas locales (reservadas) de la base de datos de dirección.

Ejemplo:

```
ASRT> LIST DATABASE LOCAL
MAC Address     MC*  Entry Type       Age  Port(s)

00-a0-26-40-0c-e4   Registered            1 (TKR/0       )
00-a0-26-40-0c-e5   Registered            2 (Eth/0       )
01-80-c2-00-00-00*  Registered            1
ASRT>
```

- *LIST DATABASE PERMANENT*

Visualiza todas las entradas permanentes de la base de datos de dirección.

Ejemplo:

```
ASRT> LIST DATABASE PERMANENT
MAC Address     MC*  Entry Type       Age  Port(s)

00-11-22-33-44-55   Permament            1 (TKR/0       )  ->  1-2
ASRT>
```

- *LIST DATABASE PORT*

Visualiza todas las entradas de un puerto determinado.

Ejemplo:

```
ASRT> LIST DATABASE PORT
Port Number[1]?
MAC Address    MC*  Entry Type       Age  Port(s)

00-a0-26-40-0c-e4   Registered            1 (TKR/0       )
01-80-c2-00-00-00*  Registered            1
01-80-c2-00-00-01*  Reserved              All
01-80-c2-00-00-02*  Reserved              All
01-80-c2-00-00-03*  Reserved              All
01-80-c2-00-00-04*  Reserved              All
01-80-c2-00-00-05*  Reserved              All
01-80-c2-00-00-06*  Reserved              All
01-80-c2-00-00-07*  Reserved              All
01-80-c2-00-00-08*  Reserved              All
01-80-c2-00-00-09*  Reserved              All
01-80-c2-00-00-0a*  Reserved              All
01-80-c2-00-00-0b*  Reserved              All
01-80-c2-00-00-0c*  Reserved              All
01-80-c2-00-00-0d*  Reserved              All
01-80-c2-00-00-0e*  Reserved              All
01-80-c2-00-00-0f*  Reserved              All
03-00-00-00-80-00*  Reserved              All
ASRT>
```

- *LIST DATABASE RANGE*

Visualiza un rango de entradas de la base de datos de la base de datos de dirección total filtrada del bridging transparente. Se da una dirección MAC de comienzo y finalización para definir el rango. Se visualizan todas las entradas que estén dentro de este rango.

Ejemplo:

```
ASRT> LIST DATABASE RANGE
First MAC address [00-00-00-00-00-00]?
Last MAC address [FF-FF-FF-FF-FF-FF]? 00-00-ff-ff-ff-ff
MAC Address    MC*  Entry Type       Age  Port(s)

00-00-0c-07-ac-00   Dynamic           315  2 (Eth/0       )
00-00-0c-07-ac-0d   Dynamic           315  2 (Eth/0       )
00-00-b4-95-33-bc   Dynamic           270  2 (Eth/0       )
00-00-c0-57-eb-6b   Dynamic           315  2 (Eth/0       )
00-00-c0-eb-51-a4   Dynamic           290  2 (Eth/0       )
00-00-e8-3d-1b-bc   Dynamic           240  2 (Eth/0       )
00-00-e8-3d-1c-dc   Dynamic           305  2 (Eth/0       )
00-00-e8-3d-31-48   Dynamic           275  2 (Eth/0       )
00-00-e8-3d-a5-04   Dynamic           270  2 (Eth/0       )
00-00-e8-41-ad-13   Dynamic           265  2 (Eth/0       )
ASRT>
```

- *LIST DATABASE STATIC*

Visualiza las entradas estáticas de la base de datos de dirección.

Ejemplo:

```
ASRT> LIST DATABASE STATIC
MAC Address     MC*  Entry Type       Age  Port(s)

01-02-03-0a-0b-0c*  Static                1 (TKR/0       )  ->  1-2
ASRT>
```

e) LIST FILTERING

Se puede visualizar el siguiente grupo de datos generales con el comando **LIST FILTERING**.

Sintaxis:

```
ASRT> LIST FILTERING ?
ALL
ETHERTYPE
SAP
SNAP
```

- *LIST FILTERING ALL*

Visualiza todas las entradas de la base de datos de filtrado.

Ejemplo:

```
ASRT> LIST FILTERING ALL
Ethernet type 9000 is bridged & processed on ports 1-2
IEEE 802.2 destination SAP 00 is bridged & processed on ports 1-2
IEEE 802.2 destination SAP 42 is routed on ports 1-2
IEEE 802 SNAP PID 00-00-00-90-00 is bridged & processed on ports 1-2
ASRT>
```

Los descriptores utilizados para explicar cómo se comunican los paquetes incluyen los siguientes.

- Routed - Los paquetes que se pasan al encaminador de routing para ser enviados.
- Filtered - Los paquetes que se filtran de forma administrativa por el usuario estableciendo los filtros de protocolo.
- Bridged and routed – Un identificador de protocolo para el cual hay una entidad de protocolo dentro del sistema que no es un encaminador. Un ejemplo es el protocolo de repetición de nivel de conexión. Se utiliza un bridge en los paquetes unicast de este protocolo o se procesan localmente si se envían a una dirección registrada. Los paquetes multicast se envían y procesan localmente para una dirección multicast registrada.

Todos los descriptores arriba explicados también se aplican a los paquetes ARP con este Ethertype.

- *LIST FILTERING ETHERTYPE*

Visualiza las entradas de la base de datos de filtrado del tipo de protocolo de Ethernet.

Ejemplo:

```
ASRT> LIST FILTERING ETHERTYPE
Ethernet type (in hexadecimal), 0 for all[0]?
Ethernet type 9000 is bridged & processed on ports 1-2
ASRT>
```

- *LIST FILTERING SAP*

Visualiza las entradas de la base de datos de filtrado del protocolo SAP.

Ejemplo:

```
ASRT> LIST FILTERING SAP
SAP (in hexadecimal), 100 for all[100]?
IEEE 802.2 destination SAP 00 is bridged & processed on ports 1-2
IEEE 802.2 destination SAP 42 is routed on ports 1-2
ASRT>
```

- *LIST FILTERING SNAP*

Visualiza las entradas de la base de datos de filtrado del identificador de protocolo SNAP.

Ejemplo:

```
ASRT> LIST FILTERING SNAP
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-90-00 is bridged & processed on ports 1-2
ASRT>
```

f) LIST PORT

Visualiza el estado de los puertos del bridge.

Ejemplo:

```
ASRT> LIST PORT
Port Number[-1]?
Port Id (dec)    : 128: 1, (hex): 80-01
Port State       : Forwarding
STP Participation: Enabled
Port Supports    : Source Routing Bridging Only
SRB: Segment Number: 0x100       MTU:  2052     STE Forwarding: Auto
Assoc Interface #/name : 00/TKR/0
--------------------------------------------------------------------------------
Port Id (dec)    : 128: 2, (hex): 80-02
Port State       : Forwarding
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Duplicates Frames Allowed:   STE: Yes  , TSF: Yes
Assoc Interface #/name : 01/Eth/0
--------------------------------------------------------------------------------
ASRT>
```

g) LIST SOURCE-ROUTING

Visualiza la información de configuración del bridge de source routing. Hay opciones de grupo de datos generales que se pueden visualizar con el comando **LIST SOURCE-ROUTING**:

Sintaxis:

```
ASRT> LIST SOURCE-ROUTING ?
CONFIGURATION
COUNTERS
STATE
```

- ***LIST SOURCE-ROUTING CONFIGURATION***

Visualiza la información general relativa al bridge SRB.

Ejemplo:

```
ASRT> LIST SOURCE-ROUTING CONFIGURATION
Bridge number:                1
Bridge state:                 Enabled
Maximum STE hop count         14
Maximum ARE hop count         14
Virtual segment:              000

Port   Segment    Interface      State       MTU  STE Forwarding
  1        100    TKR/0          Enabled    2052       Auto
  -        200   Adaptive       Enabled   1470        Yes
ASRT>
```

Bridge number	Número de bridge (en hexadecimal) asignado a este bridge.
Bridge state	Indica si el bridging está activado o no.
Maximum STE hop count	Máximo número de saltos para las tramas Spanning Tree Explorer que transmiten desde el bridge para una interfaz determinada asociada con el bridging de source routing.
Maximum ARE hop count	Máximo número de saltos para las tramas All Route Explorer que transmiten desde el bridge para una interfaz determinada asociada con el bridging de source routing.
Virtual segment	Número de segmento virtual asignado al bridging 1:N.
Port	Número de puertos asociados al bridging de source routing.
Segment	Números de segmento asignados para redes asociadas con el bridging de source routing.
Interface	Nombres de interfaz asociados. Listas adaptables para interfaces que toman parte en el SR-TB.
State	Estado actual del puerto (Activado o Desactivado).
MTU	Tamaño MTU establecido para ese puerto.
STE Forwarding	Indica si los Spanning Tree Explorers recibidos en ese puerto son enviados (Yes) y si los STE procedentes de otros puertos salen de este puerto.

- *LIST SOURCE ROUTING COUNTERS*

Visualiza todos los contadores del bridge SRB.

Sintaxis:

```
ASRT> LIST SOURCE-ROUTING COUNTERS ?
ALL-PORTS
PORT port_number
SEGMENT segment_number
```

El comando **LIST SOURCE ROUTING COUNTERS** presenta tres opciones para visualizar información:

- *All-ports* - Visualiza contadores para todos los puertos.
- *Port* - Visualiza contadores para un puerto especifico.
- *Segment* - Visualiza contadores para el puerto correspondiente a un segmento especifico.

Los siguientes ejemplo muestran cada una de las opciones de visualización de este comando.

Ejemplo 1:

```
ASRT> LIST SOURCE-ROUTING COUNTERS ALL
Counters for port 1, segment 100, interface TKR/0       :
SRF frames received:          0    sent:          0
STE frames received:      18876    sent:          0
ARE frames received:        168    sent:          0
SR frames sent as TB:                         0
TB frames sent as SR:                     26494
Dropped, in queue overflow:                   0
Dropped, source address filter:               0
Dropped, destination address filter:          0
Dropped, protocol filtering:                  0
Dropped, invalid ri length:                   0
Dropped, duplicated segment:              18814
Dropped, segment mismatch:                    0
Dropped, duplicated lan id:                   0
Dropped, stehop count exceeded:               0
Dropped, arehop count exceeded:               0
Dropped, no buffer available:                 0
Dropped, mtu exceeded:                        0

Counter for port - segment 200, Adaptive:
ASRT>
```

Port	Números de puertos relacionados con el bridging de source routing.
Segment	Números de segmentos de source routing en hexadecimal.
Interface	Nombre de la interfaz de red.
SRF Frames Received/Sent	Tramas Encaminadas Específicamente (Specifically Routed Frames) recibidas o enviadas en este bridge.
STE Frames Received/Sent	Tramas de Spanning Tree Explorer recibidas o enviadas en este bridge.
ARE Frames Received/Sent	All Routes Explorer Frames recibidas o enviadas en este bridge.

SR Frames Sent as TB	Tramas de source routing recibidas en esta interfaz que fueron enviadas como tramas de bridge transparente.
TB Frames Sent as SR	Tramas de bridge transparente recibidas en esta interfaz que fueron enviadas como tramas de source routing.
Dropped, in queue overflow	Tramas descartadas porque la cola de entrada ha sobrepasado su capacidad.
Dropped, source address filter	Tramas descartadas porque la dirección de origen coincide con un filtro de dirección origen de la base de datos de filtrado.
Dropped, destination address filter	Tramas descartadas porque esta dirección de destino coincide con un filtro de dirección destino en la base de datos de filtrado.
Dropped, protocol filtering	Tramas descartadas porque su identificador de protocolo está siendo filtrado de forma administrativa.
Dropped, invalid ri lenght	Tramas descartadas porque el tamaño del RIF es menor que 2 o mayor que 30.
Dropped, duplicate segment	Tramas descartadas a causa de un segmento duplicado en el RIF. Esto ocurre normalmente para las tramas ARE.
Dropped, segment mismatch	Tramas descartadas porque el número de segmento saliente no coincide con nadie en este bridge.
Dropped, duplicated lan id	Tramas descartadas a causa de un ID de LAN duplicado.
Dropped, stehop count exceeded	Tramas descartadas porque el STE supera el numero de saltos permitidos.
Dropped, arehop count exceeded	Tramas descartadas porque el ARE supera el número de saltos permitidos.
Dropped, no buffer available	Tramas descartadas por no disponer de buffer.
Dropped, mtu exceeded	Tramas descartadas por sobrepasar el MTU.

Ejemplo 2:

```
ASRT> LIST SOURCE-ROUTING COUNTERS PORT
Port Number[1]?
Counters for port 1, segment 100, interface TKR/0       :
SRF frames received:          0    sent:          0
STE frames received:      25134    sent:          0
ARE frames received:        231    sent:          0
SR frames sent as TB:                         0
TB frames sent as SR:                     35349
Dropped, in queue overflow:                   0
Dropped, source address filter:               0
Dropped, destination address filter:          0
Dropped, protocol filtering:                  0
Dropped, invalid ri length:                   0
Dropped, duplicated segment:              25048
Dropped, segment mismatch:                    0
Dropped, duplicated lan id:                   0
Dropped, stehop count exceeded:               0
Dropped, arehop count exceeded:               0
Dropped, no buffer available:                 0
Dropped, mtu exceeded:                        0

ASRT>
```

Ejemplo 3:

```
ASRT> LIST SOURCE-ROUTING COUNTERS SEGMENT
Segment number[1]? 100
Counters for port 1, segment 100, interface TKR/0       :
SRF frames received:          0    sent:          0
STE frames received:      25285    sent:          0
ARE frames received:        232    sent:          0
SR frames sent as TB:                         0
TB frames sent as SR:                     35570
Dropped, in queue overflow:                   0
Dropped, source address filter:               0
Dropped, destination address filter:          0
Dropped, protocol filtering:                  0
Dropped, invalid ri length:                   0
Dropped, duplicated segment:              25198
Dropped, segment mismatch:                    0
Dropped, duplicated lan id:                   0
Dropped, stehop count exceeded:               0
Dropped, arehop count exceeded:               0
Dropped, no buffer available:                 0
Dropped, mtu exceeded:                        0

ASRT>
```

- *LIST SOURCE-ROUTING STATE*

Visualiza la información relativa al estado del bridge SRB.

Ejemplo:

```
ASRT> LIST SOURCE-ROUTING STATE

Bridge state:                Up

Port   Segment    Interface      State  STE Forwarding
   1       100    TKR/0          Up           Yes

ASRT>
```

h) LIST SPANNING-TREE-PROTOCOL

Visualiza la información del protocolo de spanning tree. El bridge transparente utiliza el protocolo spanning tree para formar una topología sin bucles. Se pueden visualizar las siguientes opciones de grupo de datos generales con el comando **LIST SPANNING-TREE-PROTOCOL**:

Sintaxis:

```
ASRT> LIST SPANNING-TREE-PROTOCOL ?
CONFIGURATION
COUNTERS
STATE
TREE
```

- *LIST SPANNING-TREE-PROTOCOL CONFIGURATION*

Visualiza la información que concierne al protocolo spanning tree.

Ejemplo:

```
ASRT> LIST SPANNING-TREE-PROTOCOL CONFIGURATION
Bridge ID (prio/add):  32768/00-a0-26-40-0c-e4
Bridge state:          Enabled
Maximum age:           20 seconds
Hello time:            2 seconds
Forward delay:         15 seconds
Hold time:             1 seconds
Filtering age:         320 seconds
Filtering resolution:  5 seconds

Port  Interface      Priority      Cost      State
   1  TKR/0              128      1062      Enabled
   2  Eth/0              128       100      Enabled
ASRT>
```

- *LIST SPANNING-TREE-PROTOCOL COUNTERS*

Visualiza los contadores de protocolo spanning tree.

Ejemplo:

```
ASRT> LIST SPANNING-TREE-PROTOCOL COUNTERS
Time since tolopology change (seconds)       0
Topolgy changes:                             4
BPDUs received:                              1
BPDUs sent:                                  5673

Port  Interface      BPDUs received  BDPU input overflow  Forward transitions
   1    TKR/0                    0                    0                    1
   2    Eth/0                    1                    0                    1
ASRT>
```

- *LIST SPANNING-TREE-PROTOCOL STATE*

Visualiza la información del estado actual del protocolo de spanning tree.

Ejemplo:

```
ASRT> LIST SPANNING-TREE-PROTOCOL STATE
Designated root (prio/add):    32768/00-a0-26-40-0c-e4
Root cost:                     0
Root port:                     Self
Current (root) maximum age:    20 seconds
Current (root) hello time:     2 seconds
Current (root) Forward delay:  15 seconds
Topology change detected:      FALSE
Topology change:               FALSE

Port      Interface      State
   1      TKR/0          Forwarding
   2      Eth/0          Forwarding
ASRT>
```

- *LIST SPANNING-TREE-PROTOCOL TREE*

Visualiza la información actual del spanning tree incluyendo información del puerto, la interfaz y el coste.

Ejemplo:

```
ASRT> LIST SPANNING-TREE-PROTOCOL TREE
Port                            Designated  Desig.              Designated  Des.
No. Interface                         Root   Cost                  Bridge  Port
 1  TKR/0         32768/00-a0-26-40-0c-e4      0  32768/00-a0-26-40-0c-e4  80-01
 2  Eth/0         32768/00-a0-26-40-0c-e4      0  32768/00-a0-26-40-0c-e4  80-02
ASRT>
```

i) LIST TRANSPARENT

Visualiza la información de configuración del bridge transparente. Se pueden visualizar las siguientes opciones de grupo de datos generales con el comando **LIST TRANSPARENT**:

Sintaxis:

```
ASRT> LIST TRANSPARENT ?
CONFIGURATION
COUNTERS
STATE
```

- *LIST TRANSPARENT CONFIGURATION*

Visualiza la información que concierne al bridge transparente.

Ejemplo:

```
ASRT> LIST TRANSPARENT CONFIGURATION
Filtering database size:    2066
Aging time:                 320 seconds
Aging granularity           5 seconds

Port    Interface      State        MTU
   2    Eth/0          Enabled      1514
ASRT>
```

- *LIST TRANSPARENT COUNTERS*

Visualiza los contadores de bridge transparente. Introducir **ALL-PORTS** después del comando para visualizar los contadores para todos los puertos o introducir **PORT** seguido del número específico de puerto después del comando para visualizar los contadores de un puerto en particular.

Ejemplo:

```
ASRT> LIST TRANSPARENT COUNTERS PORT 2
Counters for port 2, interface Eth/0       :
Total frames received by interface:          559984
Frames submitted to bridging:                 92964
Frames submitted to routing:                      0
Dropped, source address filtering:                0
Dropped, dest address filtering:             513339
Dropped, protocol filtering:                      0
Dropped, no buffer available to copy:             0
Dropped, input queue overflow:                    0
Dropped, source port blocked:                    84
Frames sent by bridging:                        423
Dropped, dest port blocked:                       0
Dropped, transmit error:                          0
Dropped, too big to send on port:                 0

ASRT>
```

- *LIST TRANSPARENT STATE*

Visualiza la información de estado transparente.

Ejemplo:

```
ASRT> LIST TRANSPARENT STATE
Filtering database size:          2066
Number of static entries:            2
Number of dynamic entries:         576
Hash collision count:              111
Fitering database overflow:          0
ASRT>
```

j) LIST TUNNEL

Visualiza la información de configuración del túnel. Se puede visualizar las siguientes opciones de grupo de datos generales con el comando **LIST TUNNEL**:

Sintaxis:

```
ASRT> LIST TUNNEL ?
BRIDGES
CONFIG
```

- *LIST TUNNEL BRIDGES*

Visualiza la información del bridge túnel.

Ejemplo:

```
ASRT> LIST TUNNEL BRIDGES

SR Segment  IP Address:
  001         177.3.1.243
  002         193.45.12.244

ASRT>
```

- *LIST TUNNEL CONFIG*

Visualiza la información que concierne a la configuración del túnel.

Ejemplo:

```
ASRT> LIST TUNNEL CONFIG

Tunnel IP addresses:
224.186.0.0 (Class D multicast)

ASRT>
```

2.8. NETBIOS

Visualiza el prompt de monitorización NetBIOS. Introducir **NETBIOS** en el prompt ASRT> para visualizar el prompt de monitorización NetBIOS.

Véase el Capítulo 10 “Comandos de Filtrado y Cache NetBIOS”, para una explicación de los comandos NetBIOS.

Sintaxis:

```
ASRT> NETBIOS
```

Ejemplo:

```
ASRT> NETBIOS

NetBIOS Support User Console

NetBIOS>
```

Nota: Si usted no ha adquirido la característica NetBIOS, recibirá el siguiente mensaje si utiliza este comando:

```
NetBIOS Support not in load.
```

2.9. NAME-CACHING

Utilizar el comando **NAME-CACHING** para entrar en el menú de monitorización de la facilidad Name Caching.

Sintaxis:

```
ASRT> NAME-CACHING
Name Cache>
```

Comandos	Función
? (AYUDA)	Visualiza todos los comandos Name Caching de monitorización, o lista las opciones de un comando específico.
LIST	Permite mostrar todas las estadisticas y contadores relacionados con el Name Caching.
PORT	Selecciona el interfaz al cual se van a aplicar los comandos Name-Caching.
EXIT	Permite salir del prompt de monitorización de Name Caching.

a) ? (AYUDA)

Utilizar el comando **?** para obtener un listado de los comandos disponibles en el nivel de prompt actual. También se puede introducir ? después de un comando específico para visualizar todas sus opciones.

Ejemplo:

```
Name Cache> ?
PORT
LIST
EXIT
Name Cache>
```

b) LIST

Utilizar el comando **LIST** para mostrar las estadisticas y los contadores actualizados de Name Caching. Esta información puede visualizarse globalmente o por interfaz, utilizando previamente el comando **PORT**.

Sintaxis:

```
Name Cache> LIST ?
ADD-NAMES
CACHE
```

- *LIST ADD-NAMES*

Muestra la totalidad de las entradas utilizadas para filtrar tramas Add Names y Add Group Names.

Ejemplo:

```
Name Cache> LIST ADD-NAMES

                                                Add (Group) Name
        Name                    MAC           Received      Filtered
 -------------------    -----------------    ----------    ----------
 DELL1           <00>   00-00-83-a5-ba-1b             3             2
 NBSDLS          <00>   00-00-83-a5-ba-1b             3             2
 DELL1           <03>   00-00-83-a5-ba-1b             3             2
 DELL1                  00-00-83-a5-ba-1b             3             2
 NBSDLS          <1e>   00-00-83-a5-ba-1b             3             2
 NBSDLS          <1d>   00-00-83-a5-ba-1b             3             2
 ##__MSBROWSE__#<01>   00-00-83-a5-ba-1b             3             2

Name Cache>
```

- *LIST CACHE*

Sintaxis:

```
Name Cache> LIST CACHE ?
RIFS
STATISTICS
```

LIST CACHE RIFS

Muestra el RIF y la información MAC de todos los nombre de servidor validos y conocidos

Ejemplo:

```
Name Cache> LIST CACHE RIFS

      Server              MAC Address        Routing Information Field
-------------------    -----------------  -------------------------------
 SOPORTE                Invalid           Invalid
 FYUBERO                Invalid           Invalid


Name Cache>
```

LIST CACHE STATISTICS

Muestra el número de veces que determinadas operaciones se han ejecutado contra un nombre de servidor en concreto.

Ejemplo:

```
Name Cache> LIST CACHE STATISTICS

                                        Broadcasts
      Server            Received    Converted    Forwarded    Filtered
 ------------------    ----------  -----------  -----------  ----------
 SOPORTE                        2            0            2           0
 FYUBERO                        2            0            2           0

Name Cache>
```

c) PORT

Utilizar el comando **PORT** para seleccionar el puerto del bridge al cual se van a aplicar los comandos Name Caching de monitorización.

Ejemplo:

```
Name Cache> PORT
Port[1]? 1
Name Cache Port>
```

Una vez dentro del prompt *Name Cache Port>*, están disponibles los siguientes comandos

Sintaxis:

```
Name Cache Port> ?
LIST
EXIT
```

- *LIST*

Sintaxis:

```
Name Cache Port> LIST ?
ADD-NAMES
CACHE
```

LIST ADD-NAMES

Muestra las entradas utilizadas por un puerto especifico para filtrar tramas duplicadas de Add Names y Add Group Names.

Ejemplo:

```
Name Cache Port> LIST ADD-NAMES

 Add (Group) Name Frames:
    Received          1435
    Filtered          231

Name Cache Port>
```

LIST CACHE

Muestra los contadores de caches relativos a un puerto especifico. Estos contadores se agregan a todas las operaciones de nombre de cache en el puerto especificado.

Ejemplo:

```
Name Cache Port> LIST CACHE

 Name Request Broadcast Frames:
    Received          356
    Converted         30
    Forwarded         310
    Filtered          16

Name Cache Port>
```

- *EXIT*

Utilizar el comando **EXIT** para volver al prompt Name Cache.

Ejemplo:

```
Name Cache Port> EXIT
Name Cache>
```

d) EXIT

Utilizar el comando **EXIT** para volver al prompt ASRT.

Ejemplo:

```
Name Cache> EXIT
ASRT>
```

2.10. EXIT

Utilizar el comando **EXIT** para volver al prompt +.

Sintaxis:

```
ASRT> EXIT
```

Ejemplo:

```
ASRT> EXIT
+
```

Capítulo 9
Utilización de NetBIOS

1. Relativo a NetBIOS

NetBIOS fue diseñado únicamente para utilizarlo en una LAN. No es un protocolo que se pueda encaminar y típicamente se utiliza un bridge en él o se cambia mediante DLSw.

NetBIOS depende de tramas broadcast para la mayoría de sus funciones. Mientras que esto puede no representar un problema en entornos LAN, estos broadcast pueden ser costosos en entornos de internetworking causando congestión, así como costes incrementados para enlaces WAN.

NetBIOS utiliza servicios tipo LLC1 (LLC1) y tipo LLC2 (LLC2):

- LLC1 proporciona transferencia de datos sin conexión. Requiere resolución de conflicto de nombre, flujos de equipo de reunión de estatus y flujos de circuito y de conexión de sistema.
- LLC2 proporciona una transmisión de datos de conexión orientada que utiliza tráfico de una trama enviado sobre conexiones LLC2 establecidas.

1.1. Nombres NetBIOS

Los nombres NetBIOS son la clave de la comunicación entre equipos NetBIOS. Un equipo NetBIOS debe conocer su nombre para comunicarse con otros equipo NetBIOS.

Los nombres NetBIOS tienen caracteres 16 ASCII. IBM y Microsoft reservan el carácter décimo sexto para el nombre NetBIOS.

Hay dos tipos de nombres NetBIOS:

- Nombres individuales representan un solo cliente o servidor NetBIOS y debe ser único dentro de la red NetBIOS.
- Los nombre de grupo representan un grupo de equipos NetBIOS (un dominio Servidor OS/2 LAN, por ejemplo). Estos nombres no deben ser los mismos que los nombres individuales NetBIOS en la red.

Un único equipo NetBIOS puede tener múltiples nombres individuales o de grupo. La aplicación NetBIOS genera nombres basados en el nombre o nombres que configura el administrador de red.

1.2. Resolución del Conflicto de Nombre NetBIOS

Antes de que un equipo NetBIOS utilice un nombre individual NetBIOS, se debe asegurar que el nombre es único. Para hacer esto, el equipo difunde repetidamente una trama de Resolución de Conflicto de Nombre a todos los equipos NetBIOS. Si el equipo no obtiene respuesta, presupone que el nombre es único y utiliza el nombre.

1.3. Procedimiento de Sesión de Sistema NetBIOS

Para establecer una sesión NetBIOS para tipos de operación de transmisión de datos, el cliente NetBIOS primero determina la dirección MAC del servidor NetBIOS. En redes Token Ring, el cliente también utiliza técnicas de encaminamiento de origen para determinar el encaminamiento LLC al servidor.

A continuación se muestra el procedimiento para establecer una sesión:

1. El cliente difunde repetidamente una trama Spanning Tree Explorer (STE) NetBIOS UI que contiene el nombre NetBIOS del servidor a todos los equipos NetBIOS.

2. Cuando el servidor recibe la trama, responde al cliente con la correspondiente trama All Routes Explorer (ARE) NetBIOS UI que contiene la dirección MAC del servidor y, para Token Ring, la ruta hasta el servidor.

   Entonces el cliente puede hacer cualquiera de las siguientes cosas:

   a. Establecer una conexión LLC 2 para comunicarse con el servidor utilizando tramas-I.
   b. Empezar a comunicarse con el servidor utilizando tramas NetBIOS UI específicamente encaminadas.

2. Reducir el Tráfico NetBIOS

Hay dos formas de reducir la cantidad del tráfico de difusión NetBIOS:

- Filtrar tantas tramas de difusión NetBIOS como sea posible.
- Enviar tramas sin filtrar NetBIOS UI el menor número posible de puertos de bridge o sesiones DLSw TCP.

La siguiente tabla hace una lista de los filtros NetBIOS.

Tipo de filtro	Filtros
MAC Address	Tramas tanto para la dirección MAC de origen como la de destino.
Frame Type	Tipos específicos de tramas NetBIOS.
Duplicate Frame	Tramas duplicadas
Response	Respuestas para las cuales el router no envió una trama de difusión NetBIOS.
Byte	Tramas por offset de byte y longitud del campo dentro de una trama.
Name	Tramas por los nombres NetBIOS de origen y destino.

Una vez que el router filtra las tramas, el name caching y la cache de rutas controlan el modo en que el router encamina las restantes tramas.

El Capítulo 12, “Utilización del Filtrado MAC,” describe el filtrado de dirección MAC.

Las siguientes secciones describen el tipo de trama, la trama duplicada, y el filtrado de respuesta, el name caching y el route caching, y el filtrado de nombre y de byte.

2.1. Filtrado del Tipo de Trama

El filtrado del tipo de trama permite filtrar los siguientes tipos de tramas:

- Resolución del Conflicto de Nombre
- Difusión General
- Control de Traza

Resolución de Conflicto de Nombre

Los equipos NetBIOS utilizan las tramas de Resolución del Conflicto de Trama para asegurarse de que sus nombres son únicos. Las tramas de Resolución de Conflicto de Trama son Add-Name-Query, Add-Group-Name-Query, Add-Name Response, y Name-In-Conflict.

Utilizar las siguientes directrices para determinar cuándo filtrar las tramas de Resolución de Conflicto de Trama:

- Es importante que los nombres NetBIOS de los equipos a los que están establecidos una sesión NetBIOS (típicamente un servidor) sean únicos.
- Normalmente también es importante que los nombres NetBIOS individuales de equipos dentro del mismo grupo (o dominio) sean únicos.
- Con frecuencia no es importante que los nombres NetBIOS de los equipos desde los cuales se establece una sesión NetBIOS (típicamente un cliente) sean únicos, especialmente a través de dominios.

Por esta razón, las redes en las que hay un buen control sobre que los nombres de servidores pueden obtener ventaja mediante las tramas de filtrado de resolución de conflicto de nombre. Esto es especialmente verdad para las redes DLSw.

Difusión General

Los equipos NetBIOS utilizan las tramas de Difusión General para enviar datos a todos los equipos NetBIOS en una red. Rara vez los equipos utilizan esta trama y se pueden filtrar de forma normal. La trama NetBIOS de Difusión General es Datagram-Broadcast.

Tramas de Control de Traza

Las tramas de Control de Traza terminan trazas NetBIOS en todos los equipos NetBIOS en una red. Esta trama rara vez se utiliza y se puede filtrar de forma normal. La trama NetBIOS de Control de Traza es Terminate-Trace.

2.2. Configuración del Filtrado del Tipo de Trama

Para el tráfico de bridge, el router no filtra ninguno de los tipos de trama señalados arriba por omisión. De todas formas, si se está utilizando un bridge en tráfico de NetBIOS en enlaces WAN, podría ser beneficioso filtrar estas tramas. Para encender o apagar el filtrado del tipo de trama para el bridging, introducir **SET FILTERS BRIDGE**.

Para el tráfico DLSw, el router filtra todos los tipos de trama señalados anteriormente por omisión. Para encender o apagar el filtrado de tipo de trama para DLSw, introducir **SET FILTERS DLSW**.

Por ejemplo:

```
NetBIOS config> SET FILTERS BRIDGE

Filter Name Conflict frames(Yes/No)(N)? y

Name conflict filtering is              ON

Filter General Broadcast frames(Yes/No)(N)? n

General broadcast filtering is         OFF

Filter Trace Control frames(Yes/No)(N)? y

Trace control filtering is              ON

NetBIOS config>
```

2.3. Filtrado de Trama Duplicada

Cuando un equipo envía tramas difundidas, normalmente envía más de 10 tramas (el valor predeterminado es 6) en intervalos fijos (el valor predeterminado es 5 segundos).

El filtrado de trama duplicada provoca que el encaminador envíe sólo un ejemplo de cada trama dentro de un período de tiempo que se puede configurar. La **Figura 9-1** muestra cómo el filtrado de trama duplicada reduce el número de tramas difundidas que se envían sobre el DLSwWAN.

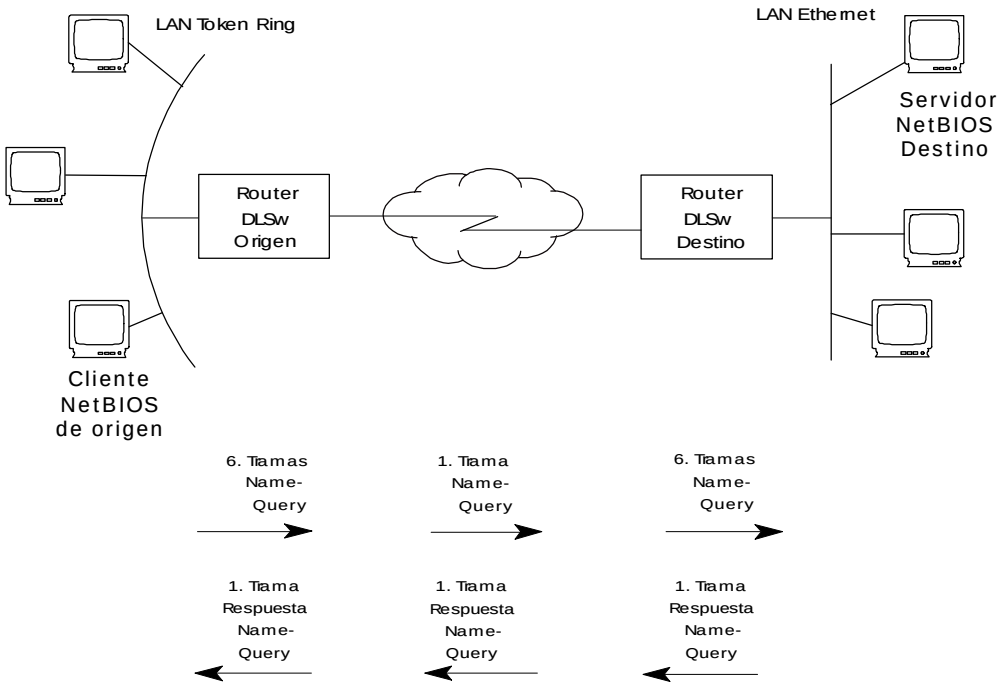


Figura 9-1. Establecer una sesión NetBIOS sobre DLSw

Aquí está el proceso que utiliza el cliente NetBIOS de origen para establecer una sesión con el servidor NetBIOS destino.

1. Tras verificar que el nombre es único, el cliente NetBIOS de origen envía seis tramas Name-Query en intervalos de medio segundo.
2. El router DLSw de origen recibe la primera trama Name-Query y la envía al encaminador DLSw de destino. El router de origen filtra las restantes cinco tramas.
3. El router DLSw de destino recibe la primera trama Name-Query. Entonces asume la responsabilidad de establecer la sesión y envía tramas Name-Query a sus LANs relacionados como si fuese el equipo NetBIOS de origen.
4. El equipo NetBIOS de destino responde a las tramas Name-Query con la correspondiente trama Name-Recognized que contiene su dirección MAC. Para tramas Token Ring, El equipo NetBIOS de destino también envía la ruta al servidor.
5. El router DLSw de destino devuelve después una trama Specifically-Router Frame (SRF) al router DLSw de origen, que envía la trama al equipo NetBIOS de origen.

2.4. Cómo Duplicar Trabajos de Filtrado de Trama

Duplicar trabajos de filtrado de trama manteniendo una base de datos de trama comando NetBIOS. Éstas incluyen las siguientes: Name-Query, Status-Query, Datagram, Add-Name-Query, Add-Group-Name-Query, y Name-In-Conflict.

La **Figura 9-2** muestra el proceso de filtrado de trama duplicada para tráfico de bridge. En este ejemplo, el router recibe seis tramas Name-Query en intervalos de medio segundo. El Duplicate Frame Filter Timeout está establecido en 1,5 segundos, y el Duplicate Frame Detect Timeout en 5 segundos.

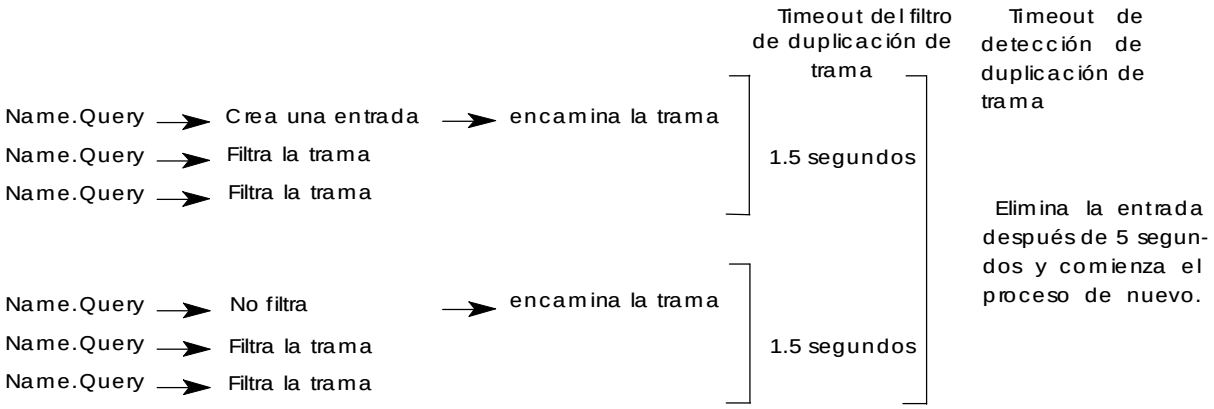


Figura 9-2. Proceso de filtrado de trama duplicada para tráfico de bridge

Aquí están los pasos para el filtrado de trama duplicada;

1. Cuando el router recibe un nueva trama, crea una entrada para esa trama en la base de datos de trama duplicada y envía la trama.
2. El router filtra cualquier trama duplicada que recibe dentro del intervalo de filtro de trama (en este caso 1,5 segundos).
3. Si el router recibe una trama duplicada después de que haya pasado este tiempo, envía la trama y reinicia el temporizador.

El router repite este proceso hasta que vence el temporizador de identificación de trama duplicada.

Para tráfico DLSw, el proceso de filtrado de trama duplicada es el mismo, excepto que el DLSw no utiliza el temporizador de filtro de trama duplicada. El DLSw utiliza sólo el temporizador de identificación de trama duplicada. Una vez que el router de origen crea una entrada, filtra todas las tramas duplicadas hasta que vence el temporizador de identificación de trama duplicada. Para DLSw, también se puede controlar el número de tramas de consulta que envía el encaminador DLSw de destino durante un período de tiempo que se puede configurar.

2.5. Configurar el Filtrado de Trama Duplicada

El filtrado de trama duplicada siempre está activa para tráfico DLSw. No se puede activar o desactivar.

El filtrado de trama duplicada está desactivada por omisión para el tráfico de bridge. Se puede activar o desactivar para el bridging utilizando los comandos **ENABLE DUPLICATE-FILTERING** y **DISABLE DUPLICATE-FILTERING**.

Para cambiar los temporizadores, introducir lo siguiente:

```
NetBIOS config> SET GENERAL

WARNING! Setting Duplicate Frame Filter Timeout to zero...
         disables duplicate frame checking!

Duplicate frame filter timeout value in seconds[1.5]?
Duplicate frame detect timeout value in seconds[5.0]?

General parameters set

NetBIOS config>
```

¡Advertencia! Establecer el timeout de Filtro de Trama Duplicada en cero…..desactiva el control de trama duplicada.

Si se activa el DLSw, el router también indica lo siguiente:

```
Command frame retry count [5]?
Command frame retry timeout value in seconds [0.5]?
```

Estos parámetros controlan cuántas tramas de consulta envía el router DLSw de destino durante un período de tiempo que se puede configurar.

2.6. Filtrado de trama de respuesta

Los equipos NetBIOS esperan una trama de respuesta a las tramas Name-Query y Status-Query. Si un equipo no recibe una respuesta, continúa enviando consultas.

Si el router recibe una respuesta a una trama comando que no envió, rechaza la respuesta y no la renvía.

No se puede desactivar el filtrado de trama de respuesta en el router.

2.7. Filtrado de Trama de Respuesta para DLSw

Para el tráfico DLSw, hay que asegurarse de que el temporizador de identificación de trama duplicada esté establecido lo suficientemente alto como para que el encaminador tenga tiempo de establecer la sesión.

Como se describe en el apartado **2.3 "Filtrado de Trama Duplicada"**, un router DLSw de destino asume la responsabilidad de establecer una sesión.

Un router asume la responsabilidad de establecer una sesión si empareja tramas Name-Query y Name-Recognized dentro de los períodos de intervalo de identificación de trama duplicada. Si el router no empareja estas tramas dentro de ese período de tiempo, no envía tramas de respuesta Name-Recognized, y no establece la sesión.

El valor predefinido del intervalo de identificación de trama duplicada es de cinco segundos. No se debe establecer el intervalo de identificación de trama duplicada en cero segundos o el router no tendrá tiempo de establecer la sesión. Se puede aumentar el intervalo de trama duplicada utilizando el comando **SET GENERAL**.

```
NetBIOS config> SET GENERAL

WARNING! Setting Duplicate Frame Filter Timeout to zero...
         disables duplicate frame checking!

Duplicate frame filter timeout value in seconds[1.5]?
Duplicate frame detect timeout value in seconds[5.0]?

General parameters set

NetBIOS config>
```

¡Advertencia! Establecer el timeout de Filtro de Trama Duplicada en cero…..desactiva el control de trama duplicada.

2.8. Name caching y Route caching NetBIOS

El Name caching y el Route caching se pueden aplicar tanto a DLSw como a bridging. Una vez que el router filtra todas las tramas difundidas NetBIOS posibles, utiliza el cache de nombre NetBIOS y el cache de ruta para reducir el número de tramas que envía el encaminador.

Con el Name caching, el router mantiene una base de datos de nombres y rutas NetBIOS. Cada vez que el router recibe una trama Name-Recognized, extrae la dirección MAC y la ruta e introduce esa información en la base de datos.

Cuando el router recibe una Name-Query o Statue-Query, comprueba para ver si el nombre que se requiere ya está en su base de datos. Si está, el Route caching convierte la trama de una trama STE a una SRF (Specifically-Routed Frame). Un temporizador en la entrada invalida la información de la base de datos, si el servidor no responde antes de que venza el temporizador.

2.9. Activación del Caching

El Name caching está siempre activado. No se puede desactivar. Por defecto el Route caching está desactivado. Para activarlo hay que introducir el comando **ENABLE ROUTE-CACHING**.

```
NetBIOS config> ENABLE ROUTE-CACHING

Route caching is                        ON

NetBIOS config>
```

2.10. Tipos de Entradas de Name caching

Hay tres tipos de entradas de Name caching:

- *Permanentes* son aquellas que se añaden al prompt de configuración NetBIOS (`NetBIOS config>`). El router guarda las entradas permanentes y todavía están disponibles cuando se reinicia el router.
- *Estáticas* son aquellas que se introducen en el prompt de monitorización NetBIOS (`NetBIOS>`). El router no guarda las entradas estáticas y no están disponibles tras reiniciar el router.
- *Dinámicas* son aquellas que el router aprende a través del procesamiento de Name-Query y Name-Recognized. Un temporizador quita las entradas dinámicas que no están referenciadas dentro de un período de tiempo que se puede configurar. El router no guarda las entradas dinámicas y no están disponibles tras el reinicio del router.

Hay tres tipos de nombres NetBIOS guardados en el Name caching:

- *Individual* es un nombre individual NetBIOS.
- *Grupo* es un nombre de grupo NetBIOS.
- *Desconocido* significa que el router todavía no tiene la información sobre el nombre, indicando que una búsqueda del nombre no está completa.

El router también distingue entre entradas locales y remotas:

- *Local* es una entrada que el router puede alcanzar localmente a través de la red de bridge. El router guarda la dirección MAC relacionada con el nombre. Si está activado el Route caching, el router también guarda la mejor ruta LLC entre el router y el equipo NetBIOS.
- *Remota* es una entrada que el router puede alcanzar de manera remota a través de una sesión DLSw TCP. El router guarda las mejores sesiones TCP.

2.11. Añadir Entradas de Name caching

Se pueden añadir entradas permanentes o estáticas para vecinos DLSw al Name caching. Aunque el router permite añadir entradas aparte de los vecinos DLSw, ignora esas entradas.

Se pueden introducir nombres NetBIOS en ASCII y hexadecimal, tanto por separado como intermezclados. Por ejemplo, se podría necesitar introducir una dirección de adaptador en modo hexadecimal. El modo de entrada de datos por defecto es ASCII. Para utilizar el modo hexadecimal, escribir un corchete izquierdo (<). Para volver a modo ASCII, escribir un corchete derecho (>).

Introducir el comando **ADD CACHE-ENTRY** en el prompt `NetBIOS config>` para añadir entradas estáticas.

```
NetBIOS config> ADD CACHE-ENTRY

Enter up to 15 characters of NetBIOS name (no wild cards)[]? nbs<F7>
Enter IP Address [0.0.0.0]? 123.45.67.89

Name cache entry has been created

NetBIOS config>
```

2.12. Establecer Parámetro de Cache

Utilizar el comando **SET CACHE-PARMS** para cambiar los siguientes parámetros:

```
NetBIOS config> SET CACHE-PARMS

Significant characters in name[16]? 15
Best path aging timeout value in seconds[60.0]?
Reduced search timeout value in seconds[1.5]?
Unreferenced entry timeout value in minutes[5000]?
Max nbr local name cache entries[500]?
Max nbr remote name cache entries[100]?

Cache parameters set

NetBIOS config>
```

Véase el Capítulo 10, apartado 3.8 SET para más información sobre el comando **SET CACHE-PARMS**.

2.13. Visualización de las Entradas de Cache

El router proporciona los siguientes comandos que permiten nuevas entradas de cache.

Desde el prompt de configuración NetBIOS, se pueden utilizar los comandos **LIST CACHE** en la **Tabla 9.1**

Tabla 9.1 Lista NetBIOS de Comandos de configuración de Cache

Comando	**Visualiza**
LIST CACHE ALL	Todas las entradas activas en el name caching del router incluyendo las entradas permanentes, estáticas y dinámicas.
LIST CACHE ENTRY-NUMBER	Una entrada cache de acuerdo con su número de entrada.
LIST CACHE NAME	Una entrada de cache para un nombre específico NetBIOS.
LIST CACHE IP-ADDRESS	Una entrada de cache para una dirección IP específica.

Desde el prompt de monitorización de NetBIOS, se pueden utilizar los comandos **LIST CACHE** en la **Tabla 9.2**

Tabla 9.2 Lista NetBIOS de Comandos de Monitorización de Cache

Comando	**Visualiza**
LIST CACHE ACTIVE	Todas las entradas activas en el name caching del router incluyendo las entradas permanentes, estáticas y dinámicas.
LIST CACHE CONFIG	Entradas Estáticas y permanentes. No muestra las entradas dinámicas.
LIST CACHE GROUP	Entradas que existen para nombres de grupo NetBIOS.
LIST CACHE LOCAL	Entradas de cache local. Las entradas de cache local son aquellas que aprende el encaminador sobre el bridge.
LIST CACHE NAME	Una entrada cache para un nombre específico NetBIOS.
LIST CACHE REMOTE	Entradas de cache remoto. Las entradas de cache remoto son aquellas que aprende el encaminador sobre el DLSw WAN.
LIST CACHE UNKNOWN	Entradas donde los tipos de entradas NetBIOS son desconocidos.

2.14. Filtrado de Nombre NetBIOS

Los filtros de nombre NetBIOS se aplican tanto al bridging como a DLSw. Se pueden utilizar para filtrar paquetes NetBIOS que tienen nombres específicos de origen NetBIOS. El router examina los campos nombre de origen y nombre de destino de los siguientes tipos de paquetes UI:

- Add-Group-Name-Query (origen)
- Add-Name-Query (origen)
- Datagram (destino)
- Name-Query (origen y destino)

Para información sobre cómo crear filtros de nombres, véase el **Capítulo 11, "Configuración y Monitorización del Filtrado de Nombre y Byte NetBIOS"**

2.15. Filtrado de Byte NetBIOS

Los filtros de byte NetBIOS se aplican tanto al bridging como a DLSw. El filtrado de byte permite filtrar paquetes NetBIOS basados en campos contenidos en el paquete NetBIOS.

Para crear un filtro de byte, especifíquese:

- Un offset (desplazamiento) desde el principio de la cabecera NetBIOS.
- Un patrón de byte para emparejar.
- Una máscara opcional para aplicar a campos seleccionados en la cabecera de NetBIOS.

Para información sobre cómo crear filtros de nombre, véase el **Capítulo 11 "Configuración y Monitorización de Filtrado de Nombre y Byte NetBIOS"**

Capítulo 10
Comandos de Filtrado y de Cache NetBIOS

1. Relativo a los comandos de Configuración y Monitorización NetBIOS

Introducir los comandos de configuración NetBIOS en el prompt `NetBIOS config>`. Este capítulo trata los cambios que hay que hacer en el prompt de configuración como si fueran permanentes. Los cambios que se hacen en este prompt no surten efecto inmediatamente, es necesario reinicializar el router para que los cambios efectuados lleguen a formar parte de la memoria de configuración del router.

Introducir los comandos de monitorización de NetBIOS es en el prompt `NetBIOS>`. Este capítulo trata de los cambios que hay que hacer en el prompt de monitorización como estáticos. Los comandos de monitorización surten efecto inmediatamente, pero el router no los guarda hasta que no se reinicia el router.

2. Configuración del Filtrado y Cache NetBIOS

Se pueden configurar los siguientes parámetros de filtrado y de cache NetBIOS:

- Para configurar los parámetros de cache de nombre, introducir el comando **SET CACHE-PARMS**.
- Para configurar el filtrado de tramas duplicada, introducir el comando **SET GENERAL**.
- Para configurar el filtrado de tipo de trama, introducir los comandos **SET FILTERS BRIDGE** o **SET FILTERS DLSW**.

2.1. Configuración de NetBIOS para DLSw

Si se está enviando tráfico NetBIOS sobre DLSw, también se pueden configurar los siguientes parámetros, de acuerdo con el procedimiento siguiente:

- Añadir entradas de cache de nombre para vecinos DLSw.
- Abrir NetBIOS SAPs.
- Configurar la prioridad para sesiones SNA y NetBIOS.
- Configurar el tamaño máximo de trama NetBIOS.
- Configurar la asignación de memoria para tramas NetBIOS UI.

2.2. Añadir entradas de cache de nombre para vecinos DLSw

Añadir entradas de cache de nombre para vecinos DLSw. Se pueden añadir múltiples entradas con diferentes direcciones IP para un único nombre NetBIOS. Esto permite que el DLSw envíe la trama a múltiples vecinos DLSw.

Se pueden introducir nombres NetBIOS en ASCII y hexadecimal, tanto por separado como intermezclados. Véase el apartado **3.3 ADD** para más información. Los nombres NetBIOS son sensibles a mayúsculas y minúsculas y deben emparejar las mayúsculas y minúsculas de los nombres NetBIOS de la red.

```
NetBIOS config> ADD CACHE-ENTRY

Enter up to 15 characters of NetBIOS name (no wild cards)[]? accounting<000>
Enter IP Address [0.0.0.0]? 135.77.25.2

Name cache entry has been created

NetBIOS config>
```

2.3. Abrir NetBIOS SAPs

En el prompt `DLSw config>`, abrir NetBIOS SAPs en ambos lados del conector para activar el DLSw para transmitir tramas NetBIOS.

```
DLSw config> OPEN-SAP
Interface # [0]?
Enter SAP in hex (range 0-F4), 'SNA', 'NB' or 'LNM' [4]?
SAP 4 opened on interface 0
DLSw config>
```

2.4. Establecer una Prioridad para SNA y Sesiones NetBIOS

Hay que priorizar SNA y el tráfico NetBIOS para prevenir que un tipo de sesión utilice demasiado del ancho de banda disponible durante una congestión de red.

Para hacer esto, hay que introducir en el prompt `DLSw config>` el comando SET PRIORITY para establecer uno de los siguientes tipos de prioridad: Critica (Critical), Alta (High), Media (Médium) o Baja (Low) para sesiones SNA y sesiones NetBIOS. También se establece una asignación de mensajes que corresponde a cada prioridad de sesión.

```
DLSw config> SET PRIORITY
Priority for SNA DLSw sessions (C/H/M/L)[M]? H
Priority for NetBIOS DLSw sessions (C/H/M/L)[M]?
Message allocation by C/H/M/L priority (4 digits)[4/3/2/1]?
Maximum NetBIOS frame size (516, 1470, 2052, or 4399)[2052]?
DLSw config>
```

El router utiliza la prioridad y la asignación de mensaje para limitar selectivamente la longitud por rotura por presión de tipos específicos de tráfico. Por ejemplo, si se asigna al

- tráfico SNA una prioridad de tipo Critica y la sesión Critica tiene una asignación de mensaje de de 4, y al
- tráfico NetBIOS una prioridad de Media y las sesiones Medias tienen una asignación de mensaje de 2, el router procesa 4 tramas SNA antes de procesar 2 tramas NetBIOS. Una vez que el router ha procesado 2 tramas NetBIOS, procesa 4 tramas SNA y así. de esta forma, el router dedica dos tercios del ancho de banda disponible al tráfico SNA (en la proporción de 4 a 2). Obsérvese que el router cuenta tramas, en lugar de bytes, cuando se distribuye la anchura de banda de acuerdo con las prioridades que se le hayan asignado.

Se puede cambiar la asignación de mensajes para sesiones desde el valor por defecto 4/3/2/1. Siempre se deben introducir cuatro cifras, comprendidas entre 1 y 9, en orden descendente. Por ejemplo, si la prioridad SNA es Critica, el tráfico NetBIOS tiene prioridad Media y se cambia la asignación de mensajes a 8/7/6/5, el router procesa 8 tramas SNA antes de procesar 6 tramas NetBIOS, y así.

2.5. Establecer el tamaño máximo de trama NetBIOS

Para cambiar el tamaño máximo de trama NetBIOS, introducir el comando **SET PRIORITY** en el prompt `DLSw config>`. El valor por defecto es 2052. Este parámetro conviene configurarlo para el tamaño más largo de trama que se espera necesitar, y no más largo. Configurar el tamaño de trama más largo de lo que se necesita reduce el número de buffers disponibles.

2.6. Establecer la distribución de memoria para tramas NetBIOS UI

Introducir el comando **SET MEMORY** en el prompt `DLSw config>` para configurar el número de bytes que el router asigna como buffer para tramas NetBIOS UI. Si el buffer de transmisión TCP se llena, el router utiliza este buffer para reunir tramas NetBIOS UI.

Nótese que el número de bytes distribuidos para NetBIOS es global, y no por sesión.

```
DLSw config> SET MEMORY
Number of bytes to allocate for DLSw (at least 26624)[141312]?
Number of bytes to allocate per LLC session[8192]?
Number of bytes to allocate per SDLC session[4096]?
Number of bytes to allocate for NetBIOS UI-frames[40960]?
DLSw config>
```

3. Comandos de Configuración NetBIOS

La Tabla 10.1 contiene una lista de los comandos de configuración NetBIOS

Tabla 10.1. Comandos de Configuración NetBIOS

Comando	Función
? (AYUDA)	Muestra una lista de los comandos u opciones disponibles.
ADD	Añade entradas cache al cache de nombre del router.
DELETE	Borra entradas de cache que se añaden utilizando el comando **ADD CACHE-ENTRY**.
DISABLE	Desactiva el filtrado de trama duplicada y el Route caching.
ENABLE	Activa el filtrado de trama duplicada y el Route caching.
LIST	Visualiza varias entradas de cache e información de configuración.
SET	Configura parámetros para cache de nombre, filtrado de trama duplicada y filtrado de tipo de trama. También visualiza el prompt `NETBIOS Filter config>`.
EXIT	Vuelve al prompt anterior.

3.1. Visualización del prompt de Configuración NetBIOS

Se puede acceder al prompt `NetBIOS config>` tanto desde los entornos de configuración ASRT o DLSw.

Los cambios que se hacen en el prompt `NetBIOS config>` afectan tanto al bridging como al DLSw.

1. Para visualizar el prompt `NetBIOS config>` desde el entorno de configuración ASRT, introducir el comando **PROTOCOL ASRT** en el prompt `Config>` y teclear **NETBIOS** en el prompt `ASRT config>`.

```
Config> PROTOCOL ASRT

-- ASRT Bridge user configuration --
ASRT config> NETBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

2. Para visualizar el prompt `NetBIOS config>` desde el entorno de configuración DLSw, introducir el comando **PROTOCOL DLS** en el prompt `Config>` y teclear **NETBIOS** en el prompt `DLSw config>`.

```
Config> PROTOCOL DLS
DLSw protocol user configuration
DLSw config> NETBIOS

NetBIOS Support User Configuration

NetBIOS config>
```

3.2. ? (AYUDA)

Hace una lista de los comandos u opciones disponibles.

Sintaxis:

```
NetBIOS config> ?
```

Ejemplo:

```
NetBIOS config> ?
ADD
DELETE
DISABLE
ENABLE
LIST
SET
EXIT
```

3.3. ADD

Añade una nueva entrada de cache de nombre a la configuración permanente del router.

Sintaxis:

```
NetBIOS config> ADD ?
CACHE-ENTRY
```

a) *ADD CACHE-ENTRY*

Añade una nueva entrada al cache de nombre del encaminador. Se pueden añadir entradas de cache de nombre sólo para vecinos DLSw. El encaminador ignora entradas que se añaden para tráfico ASRT.

Se pueden añadir múltiples entradas con diferentes direcciones IP para un único nombre NetBIOS. Esto permite enviar la trama a múltiples vecinos DLSw.

Se pueden introducir nombres NetBIOS en ASCII y hexadecimal, tanto por separado como intermezclados. Por ejemplo, se podría necesitar introducir una dirección de adaptador en modo hexadecimal. El modo de entrada de datos por defecto es ASCII. Para utilizar el modo hexadecimal, escribir un corchete izquierdo (<). Para volver a modo ASCII, escribir un corchete derecho (>).

Nota: Los nombres NetBIOS son sensibles a mayúsculas y minúsculas y deben coincidir con las mayúsculas y minúsculas de los nombres NetBIOS de la red.

Ejemplo:

```
NetBIOS config> ADD CACHE-ENTRY

Enter up to 15 characters of NetBIOS name (no wild cards)[]? accounting<000>
Enter IP Address [0.0.0.0]? 135.77.25.2

Name cache entry has been created

NetBIOS config>
```

3.4. DELETE

Borra las entradas de cache de nombre de la configuración permanente del router. El router pide un número, que es el número de entrada que se quiere borrar. Para ver una lista de los números de entrada, introducir el comando **LIST CACHE ALL**.

Sintaxis:

```
NetBIOS config> DELETE CACHE-ENTRY
```

Ejemplo:

```
NetBIOS config> DELETE CACHE-ENTRY

Enter name cache record number[1]?

Name cache entry has been deleted

NetBIOS config>
```

3.5. DISABLE

Desactiva el filtrado de trama duplicada o el Route caching del bridge.

Sintaxis:

```
NetBIOS config> DISABLE ?
DUPLICATE-FILTERING
ROUTE-CACHING
```

a) DISABLE DUPLICATE-FILTERING

Desactiva el filtrado de trama duplicada para el bridging. El filtrado de trama duplicada siempre está activada para el tráfico DLSw. No se puede activar o desactivar.

Ejemplo:

```
NetBIOS config> DISABLE DUPLICATE-FILTERING

Duplicate frame filtering is           OFF

NetBIOS config>
```

b) DISABLE ROUTE-CACHING

Desactiva el Route caching para el bridging. El Route caching es el proceso de convertir tramas difundidas en tramas SRF (Specifically-Routed Frames), utilizando las entradas en el cache de nombre NetBIOS. El Route caching está siempre activado para el tráfico DLSw. No se puede activar o desactivar.

Ejemplo:

```
NetBIOS config> DISABLE ROUTE-CACHING

Route caching is                       OFF

NetBIOS config>
```

3.6. ENABLE

Activa el filtrado de trama duplicada o el Route caching para el bridge.

Sintaxis:

```
NetBIOS config> ENABLE ?
DUPLICATE-FILTERING
ROUTE-CACHING
```

a) ENABLE DUPLICATE-FILTERING

Activa el filtrado de trama duplicada para el bridging. El filtrado de trama duplicada está siempre activada para el tráfico DLSw. No se puede activar o desactivar.

Ejemplo:

```
NetBIOS config> ENABLE DUPLICATE-FILTERING

Duplicate frame filtering is            ON

NetBIOS config>
```

b) ENABLE ROUTE-CACHING

Activa el Route caching para el bridging. El Route caching está siempre activado para el tráfico DLSw. No se puede activar o desactivar. El route caching es el proceso de convertir tramas difundidas en tramas SRF (Specifically-Routed Frames), utilizando las entradas en el cache de nombre NetBIOS.

Ejemplo:

```
NetBIOS config> ENABLE ROUTE-CACHING

Route caching is                        ON

NetBIOS config>
```

3.7. LIST

Visualiza todas las entradas de cache o visualiza las entradas de cache por tipo de entrada. Visualiza la información de configuración de filtro o la información de configuración general.

Sintaxis:

```
NetBIOS config> LIST ?
CACHE
FILTERS
GENERAL
```

a) LIST CACHE

Sintaxis:

```
NetBIOS config> LIST CACHE ?
ALL
ENTRY-NUMBER
IP-ADDRESS
NAME
```

- *LIST CACHE ALL*

Visualiza todas las entradas activas en el cache de nombre permanente del router. No visualiza las entradas dinámicas o estáticas.

El router visualiza todos los datos hexadecimales entre corchetes. El número entre corchetes justo antes de la dirección IP es el décimo sexto carácter del nombre NetBIOS. IBM y Microsoft reservan el décimo sexto carácter del nombre NetBIOS y siempre aparece en hexadecimal.

Ejemplo:

```
NetBIOS config> LIST CACHE ALL

Entry  Name                  IP Address
-----  --------------------  ---------------
    1  test           <00>  1.2.3.4
    2  ejemplo        <00>  145.67.89.10

NetBIOS config>
```

- *LIST CACHE ENTRY-NUMBER*

Visualiza la entrada de cache de acuerdo con su número de entrada. Introducir el comando **LIST CACHE ALL** para ver una lista de todos los números de entrada.

Ejemplo:

```
NetBIOS config> LIST CACHE ENTRY-NUMBER
Enter name cache record number[1]? 2

Entry  Name                  IP Address
-----  --------------------  ---------------
    2  example        <00>  145.67.89.10

NetBIOS config>
```

- *LIST CACHE IP-ADDRESS*

Permite visualizar una entrada para una dirección específica IP.

Ejemplo:

```
NetBIOS config> LIST CACHE IP-ADDRESS
Enter IP Address [0.0.0.0]? 145.67.89.10

Entry  Name                  IP Address
-----  --------------------  ---------------
    2  example        <00>  145.67.89.10

NetBIOS config>
```

- *LIST CACHE NAME*

Visualiza una entrada de cache para un nombre específico NetBIOS. Utilizar los siguientes comodines para simplificar la búsqueda:

***** Significa cualquier cadena de caracteres. Por ejemplo, "San*" podría producir:
San Francisco
Santa Fe
San Juan

? Significa cualquier único carácter.

$ Debe coincidir con el último carácter en un nombre.

Los siguientes ejemplos son utilizaciones válidas de comodines que coinciden con San Francisco:

Fran	S??*?????????
San?Fran?isco	S'*
*S**	S?a?n?F?a?c?s?
**o*	????????????
Isco?	Isco$
*San?F**	*

Utilizar tantos comodines como se quiera, hasta el número máximo de caracteres en nombre NetBIOS (15 o 16 dependiendo de cuántos caracteres significativos se configuran utilizando el comando **SET CACHE-PARMS**).

Nota: Los nombres NetBIOS son sensibles a mayúsculas y minúsculas

Ejemplo:

```
NetBIOS config> LIST CACHE NAME
Enter up to 15 characters of NetBIOS name (wild cards ok)[]? test

Entry  Name                IP Address
-----  ------------------  ---------------
    1  test           <00>  1.2.3.4

NetBIOS config>
```

b) LIST FILTERS

Sintaxis:

```
NetBIOS config> LIST FILTERS ?
ALL
BRIDGE
DLSW
```

- ***LIST FILTERS ALL***

Visualiza si el filtrado de tipo de trama está encendido o apagado tanto para el bridging como para DLSw. Utilizar los comandos **SET FILTERS BRIDGE** y **SET FILTERS DLSW** para activar o desactivar estos filtros.

Ejemplo:

```
NetBIOS config> LIST FILTERS ALL

Bridge name conflict filtering is      OFF
Bridge general bcast filtering is      OFF
Bridge trace control filtering is      OFF

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON

NetBIOS config>
```

- *LIST FILTERS BRIDGE*

Visualiza si el filtrado de tipo de trama está encendida o apagada para el bridging. Utilizar el comando **SET FILTERS DLSW** para activar o desactivar estos filtros.

Ejemplo:

```
NetBIOS config> LIST FILTERS BRIDGE

Bridge name conflict filtering is      OFF
Bridge general bcast filtering is      OFF
Bridge trace control filtering is      OFF

NetBIOS config>
```

- *LIST FILTERS DLSW*

Visualiza si el filtrado de tipo de trama está encendida o apagada para ambos DLSw. Utilizar el comando **SET FILTERS DLSW** para activar o desactivar estos filtros.

Ejemplo:

```
NetBIOS config> LIST FILTERS DLSW

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON

NetBIOS config>
```

c) *LIST GENERAL*

Visualiza el cache actual NetBIOS y la configuración de filtrado.

Sintaxis:

```
NetBIOS config> LIST GENERAL
```

Ejemplo:

```
NetBIOS config> LIST GENERAL

Bridge-only Information:

Bridge duplicate filtering is          OFF
Bridge duplicate frame filter t/o      1.5 seconds

DLS-only Information:

DLS command frame retry count            5
DLS max remote name cache entries      100
DLS command frame retry timeout        0.5 seconds

DLS-Bridge Common Information:

Route caching is                       OFF
Significant characters in name          15
Max local name cache entries           500
Duplicate frame detect timeout         5.0 seconds
Best path aging timeout               60.0 seconds
Reduced search timeout                 1.5 seconds
Unreferenced entry timeout            5000 minutes

NetBIOS config>
```

Nota: La información de solo DLS (DSL-only) solamente aparece si está activado el DLSw.

3.8. SET

Configura los parámetros de name caching, enciende o apaga el filtrado de tipo de trama para el bridging o DLSw, y ajusta los temporizadores del filtrado de trama duplicada y los temporizadores de reintento de trama. También visualiza el nombre NetBIOS y el prompt de filtrado de byte.

Sintaxis:

```
NetBIOS config> SET ?
CACHE-PARMS
FILTERS
GENERAL
```

a) SET CACHE-PARMS

Configura los parámetros de name caching que se aplican al bridging o al DLSw.

Ejemplo:

```
NetBIOS config> SET CACHE-PARMS

Significant characters in name[15]?
Best path aging timeout value in seconds[60.0]?
Reduced search timeout value in seconds[1.5]?
Unreferenced entry timeout value in minutes[5000]?
Max nbr local name cache entries[500]?
Max nbr remote name cache entries[100]?

Cache parameters set

NetBIOS config>
```

Significant characters in name

Determina si el router considera 15 ó 16 caracteres cuando busca el nombre NetBIOS. Si se introducen

- 15, el router ignora el décimo sexto carácter.
- 16, el router incluye el décimo sexto carácter cuando busca entradas de cache.

El valor predeterminado es 15.

Best path aging timeout

Período de tiempo en segundos que el router considera que la dirección y la ruta para una entrada de cache local son la mejor ruta hasta ese equipo. Cuando pasa este tiempo, el router borra la entrada de cache de nombre e intenta descubrir una nueva ruta que sea mejor para el nombre NetBIOS.

Para determinar la mejor ruta, el router considera el tiempo de transmisión entre nodos en todas las posibles rutas que conectan dichos nodos, así como el tamaño más largo de trama. El router no considera una ruta como posible si no puede acomodar la trama más larga NetBIOS que puede ser transmitida por la ruta.

El valor por defecto es 60 segundos. El rango de valores es de 1,0 a 100,0 segundos.

Reduced search timeout

Cuando el router recibe un Name-Query, Status-Query, o Datagram durante el período de vencimiento de temporización, busca basándose en la información actual de cache de nombre NetBIOS.

Si el router recibe una trama duplicada después de que pase este tiempo, presume que la ruta anterior ya no es válida y aumenta su búsqueda. El router envía la trama duplicada tanto a los bridges como a DLSw. El DLSw difunde el correspondiente mensaje SSP a todos los posibles compañeros DLSw.

El valor por defecto es 1,5 segundos. El rango de valores es de 1,0 a 100,0 segundos.

Unreferenced entry timeout

El router mantiene un nombre que no está referenciado en su cache durante este tiempo antes de borrarlo. Si la cache se llena, el router elimina las entradas más rápidamente.

El valor por defecto es de 5000 minutos. El rango de valores es de 1,0 a 100000 minutos.

Max nbr local name cache entries

Número máximo de entradas locales que el router almacena en la cache de nombres. Las entradas locales son aquellas que aprende el encaminador por medio del bridge.

El valor por defecto es 500. El rango de valores es de 1 a 30.000. Para optimizar la utilización memoria, utilización del procesador y la cantidad de tráfico broadcast, hay que establecer este número tan cerca como sea posible del número total de equipos NetBIOS (servidores y clientes) que están activados en esa red de bridge

	local del router.
Max nbr remote name cache entries	Número máximo de las entradas aprendidas remotamente, las entradas de nombre de grupo y las entradas desconocidas. El valor por defecto es 100. El rango de valores es de 1 a 30.000. Para optimizar la utilización de memoria, la utilización del procesador y la cantidad de tráfico broadcast, establecer este número con arreglo al número de clientes NetBIOS remotos en la red de bridge local en este router, y sumarle aproximadamente un 25% adicional.

b) SET FILTERS

Sintaxis:

```
NetBIOS config> SET FILTERS ?
BRIDGE
BYTE
DLSW
NAME
```

- *SET FILTERS BRIDGE*

Enciende o apaga el filtrado de tipo de trama para el bridging.

Ejemplo:

```
NetBIOS config> SET FILTERS BRIDGE

Filter Name Conflict frames(Yes/No)(N)?

Name conflict filtering is             OFF

Filter General Broadcast frames(Yes/No)(N)? y

General broadcast filtering is          ON

Filter Trace Control frames(Yes/No)(N)?

Trace control filtering is             OFF

NetBIOS config>
```

- *SET FILTERS BYTE*

Desde el prompt `NetBIOS config>`, visualiza el prompt de configuración de filtrado NetBIOS (`NETBIOS Filter config>`).

Este prompt permiten establecer el filtrado de byte NetBIOS.

Véase el **Capítulo 11 "Configuración y Monitorización de Filtrado de Nombre y byte NetBIOS"** para más información sobre los comandos disponibles en este prompt.

Ejemplo:

```
NetBIOS config> SET FILTERS BYTE
NETBIOS Filtering configuration
NETBIOS Filter config>
```

- *SET FILTERS DLSW*

Establece los filtros de tipo de trama para tráfico DLSw.

Ejemplo:

```
NetBIOS config> SET FILTERS DLSW

Filter Name Conflict frames(Yes/No)(Y)? y

Name conflict filtering is              ON

Filter General Broadcast frames(Yes/No)(Y)? n

General broadcast filtering is         OFF

Filter Trace Control frames(Yes/No)(Y)? n

Trace control filtering is             OFF

NetBIOS config>
```

- *SET FILTERS NAME*

Desde el prompt `NetBIOS config>`, visualiza el prompt `NETBIOS Filter config>`.

Este prompt permiten establecer el filtrado de nombre NetBIOS.

Véase el **Capítulo 11 "Configuración y Monitorización de Filtrado de Nombre y byte NetBIOS"** para más información sobre los comandos disponibles en este prompt.

Ejemplo:

```
NetBIOS config> SET FILTERS NAME
NETBIOS Filtering configuration
NETBIOS Filter config>
```

c) SET GENERAL

Establece el timeout de la trama duplicada, el timeout de detección de trama duplicada y el contador y timeout de reintento de trama de comando. Véase el apartado **2.3 "Filtrado de Trama Duplicada"** en el Capítulo 9 para más información sobre cómo duplicar el trabajo de los filtros de trama.

Ejemplo:

```
NetBIOS config> SET GENERAL

WARNING! Setting Duplicate Frame Filter Timeout to zero...
         disables duplicate frame checking!

Duplicate frame filter timeout value in seconds[1.5]?
Duplicate frame detect timeout value in seconds[5.0]?
Command frame retry count[5]?
Command frame retry timeout value in seconds[0.5]?

General parameters set

NetBIOS config>
```

¡Advertencia! Establecer el timeout de Filtro de Trama Duplicada en cero…..desactiva el control de trama duplicada.

Si el DLSw NO está activado, el software NO indica la parte:

```
Command frame retry count[5]?
Command frame retry timeout value in seconds[0.5]?
```

Duplicate frame filter timeout	Se dirige sólo a tráfico de bridge si está activada el filtrado de tramas duplicadas. Durante este período de timeout, el router filtra todas las tramas duplicadas que recibe. El rango de valores es de 0,0 a 100,000 segundos. El cero desactiva el control de trama duplicada. El valor por defecto es 1,5 segundos.
Duplicate frame detect timeout	Se dirige tanto al tráfico de bridge como al DLSw. Tiempo durante el que el router almacena entradas en su base de datos de filtro de trama. Cuando pasa este tiempo, el router crea entradas nuevas para las tramas nuevas que recibe. El rango de valores es de 0,0 a 100,000 segundos. El valor por defecto es 5 segundos.
Command frame retry count	Se aplica al tráfico DLSw. Número de tramas duplicadas NetBIOS UI que el router de destino DLSw envía a sus LAN localmente relacionados. El router envía estas tramas en intervalos especificados por el parámetro *command frame retry timeout.* El rango de valores es de 0,0 a 10. El valor por defecto es de 5 segundos.
Command frame retry timeout	Se aplica al tráfico DLSw. Éste es el intervalo en que el router DLSw vecino reintenta enviar tramas duplicadas NetBIOS UI a su red de bridge local. El rango de valores es de 0,0 a 10,00 segundos. El valor por defecto es 5 segundos.

3.9. EXIT

Vuelve al prompt anterior.

Sintaxis:

```
NetBIOS config> EXIT
```

Ejemplo:

```
NetBIOS config> EXIT
ASRT config>
```

4. Comandos de Monitorización NetBIOS

La Tabla 10.2 contiene una lista de los comandos de monitorización NetBIOS.

Tabla 10.2. Comandos de Monitorización NetBIOS

Comando	Función
? (AYUDA)	Hace una lista de los comandos u opciones disponibles.
ADD	Añade entradas cache al cache de nombre del router.
DELETE	Borra entradas de cache que se añaden utilizando el comando **ADD CACHE-ENTRY**.
DISABLE	Desactiva el filtrado de trama duplicada y Route caching.
ENABLE	Activa el filtrado de trama duplicada y el Route caching.
LIST	Visualiza varias entradas de cache e información de monitorización.
SET	Configura parámetros para cache de nombre, filtrado de trama duplicada y filtrado de tipo de trama. También visualiza el prompt `NETBIOS Filter>`.
EXIT	Vuelve al prompt anterior.

4.1. Visualización del prompt de Monitorización NetBIOS

Se puede acceder al prompt `NetBIOS>` tanto desde los entornos de monitorización ASRT o DLSw.

Los cambios que se hacen en el prompt `NetBIOS>` afectan tanto al bridging como a DLSw.

1. Para visualizar el prompt `NetBIOS>` desde el entorno de monitorización ASRT, introducir el comando **PROTOCOL ASRT** en el prompt `+` y teclear **NETBIOS** en el prompt `ASRT>`.

```
+ PROTOCOL ASRT
ASRT> NETBIOS

NetBIOS Support User Console

NetBIOS>
```

2. Para visualizar el prompt `NetBIOS>` desde el entorno de monitorización DLSw, introducir el comando **PROTOCOL DLS** en el prompt `+` y teclear **NETBIOS** en el prompt `DLSw>`.

```
+ PROTOCOL DLS
DLSw> NETBIOS

NetBIOS Support User Console

NetBIOS>
```

4.2. ? (AYUDA)

Hace una lista de los comandos u opciones disponibles.

Sintaxis:

```
NetBIOS> ?
```

Ejemplo:

```
NetBIOS> ?
ADD
DELETE
DISABLE
ENABLE
LIST
SET
EXIT
```

4.3. ADD

Añade una nueva entrada de cache de nombre a la configuración estática del router.

Sintaxis:

```
NetBIOS> ADD ?
CACHE-ENTRY
```

a) *ADD CACHE ENTRY*

Añade una nueva entrada al cache de nombre del router. Se pueden añadir entradas de cache de nombre sólo para vecinos DLSw. El router ignora entradas que se añaden para tráfico ASRT.

Se pueden añadir múltiples entradas con diferentes direcciones IP para un único nombre NetBIOS. Esto permite enviar la trama a múltiples vecinos DLSw.

Se pueden introducir nombres NetBIOS en ASCII y hexadecimal, tanto por separado como intermezclados. Por ejemplo, se necesitaría introducir una dirección de adaptador en modo hexadecimal. El modo por defecto de entrada de datos es ASCII. Para introducir modo hexadecimal, tecléese un corchete izquierdo (<). Para volver a modo ASCII, introdúzcase un corchete derecho (>).

Nota: Los nombres NetBIOS son sensibles a mayúsculas y minúsculas y deben coincidir con las mayúsculas y minúsculas de los nombres NetBIOS de la red.

Ejemplo:

```
NetBIOS> ADD CACHE-ENTRY

Enter up to 15 characters of NetBIOS name (no wild cards)[]? accounting<000>
Enter IP Address [0.0.0.0]? 135.77.25.2

Name cache entry has been created

NetBIOS config>
```

4.4. DELETE

Borra las entradas de cache de nombre de la configuración estática o del cache activo del router. El router pide un nombre de entrada de cache. Para ver una lista de entradas, introducir **LIST CACHE CONF** o **LIST CACHE ACTIVE**.

Nota: Los nombres NetBIOS son sensibles a mayúsculas y minúsculas.

Sintaxis:

```
NetBIOS> DELETE CACHE-ENTRY
```

Ejemplo:

```
NetBIOS> DELETE CACHE-ENTRY

Enter up to 15 characters of NetBIOS name (no wild cards)[]? test

Name cache entry NOT found in Active list for name entered
Name cache entry has NOT been deleted from Active list

Static name cache entry deleted from temporary config list

NetBIOS>
```

4.5. DISABLE

Desactiva el filtrado de trama duplicada o el Route caching del bridge.

Sintaxis:

```
NetBIOS> DISABLE ?
DUPLICATE-FILTERING
ROUTE-CACHING
```

a) DISABLE DUPLICATE-FILTERING

Desactiva el filtrado de trama duplicada para el bridging. El filtrado de trama duplicada siempre está activada para el tráfico DLSw. No se puede activar o desactivar.

Ejemplo:

```
NetBIOS> DISABLE DUPLICATE-FILTERING

Duplicate frame filtering is           OFF

NetBIOS>
```

b) DISABLE ROUTE-CACHING

Desactiva el Route caching de ruta para el bridging. El Route caching es el proceso de convertir tramas difundidas en tramas Specifically-Routed Frames (SRF), utilizando las entradas en el cache de nombre NetBIOS. El Route caching está siempre activado para el tráfico DLSw. No se puede activar o desactivar.

Ejemplo:

```
NetBIOS> DISABLE ROUTE-CACHING

Route caching is                       OFF

NetBIOS>
```

4.6. ENABLE

Activa el filtrado de trama duplicada o el Route caching para el bridge.

Sintaxis:

```
NetBIOS> ENABLE ?
DUPLICATE-FILTERING
ROUTE-CACHING
```

a) ENABLE DUPLICATE-FILTERING

Activa el filtrado de trama duplicada para el bridging. El filtrado de trama duplicada está siempre activada para el tráfico DLSw. No se puede activar o desactivar.

Ejemplo:

```
NetBIOS> ENABLE DUPLICATE-FILTERING

Duplicate frame filtering is            ON

NetBIOS>
```

b) ENABLE ROUTE-CACHING

Activa el Route caching para el bridging. El Route caching está siempre activado para el tráfico DLSw. No se puede activar o desactivar. El Route caching es el proceso de convertir tramas difundidas en tramas Specifically-Routed Frames (SRF), utilizando las entradas en el cache de nombre NetBIOS.

Ejemplo:

```
NetBIOS> ENABLE ROUTE-CACHING

Route caching is                        ON

NetBIOS>
```

4.7. LIST

Visualiza varios tipos de entradas de cache, configuración de filtro, información general de monitorización o estadísticas de cache y filtrado.

Sintaxis:

```
NetBIOS> LIST ?
CACHE
FILTERS
GENERAL
STATISTICS
```

a) LIST CACHE

Sintaxis:

```
NetBIOS> LIST CACHE ?
ACTIVE
CONFIG
GROUP
LOCAL
NAME
REMOTE
UNKNOWN
```

- *LIST CACHE ACTIVE*

Visualiza todas las entradas activas en el cache de nombre del router, incluyendo entradas estáticas, dinámicas o permanentes.

El router visualiza todos los datos hexadecimales entre corchetes. El número entre corchetes justo antes de la dirección IP es el décimo sexto carácter del nombre NetBIOS. IBM y Microsoft reservan el décimo sexto carácter del nombre NetBIOS y siempre aparece en hexadecimal.

Si el campo de Tipo de Nombre no específica que es local, es una entrada remota. Para una descripción de los campos en esta visualización, véase el comando **LIST CACHE NAME** en este mismo apartado.

Ejemplo:

```
NetBIOS> LIST CACHE ACTIVE

Cnt  NetBIOS Name         Name Type          Entry Type
---  ------------------   -----------------  ----------
  1  ADMIN          <00>  INDIVIDUAL LOCAL   DYNAMIC
  2  MAILER         <20>  UNKNOWN            DYNAMIC
  3  DEV            <1b>  UNKNOWN            DYNAMIC
  4  RESEARCH       <1b>  UNKNOWN            DYNAMIC
  5  JOHN           <00>  INDIVIDUAL LOCAL   DYNAMIC
  6  JAXE           <00>  INDIVIDUAL LOCAL   DYNAMIC
  7  LABNT          <00>  INDIVIDUAL LOCAL   DYNAMIC

NetBIOS>
```

- *LIST CACHE CONFIG*

Visualiza todas las entradas de cache de nombre permanentes y estáticas. No muestra las entradas dinámicas.

El router visualiza todos los datos hexadecimales entre corchetes. El número entre corchetes justo antes de la dirección IP es el décimo sexto carácter del nombre NetBIOS. IBM y Microsoft reservan el décimo sexto carácter del nombre NetBIOS y siempre aparece en hexadecimal.

Ejemplo:

```
NetBIOS> LIST CACHE CONFIG

Name                 IP Address       Source     Last Mod
-------------------  ---------------  ---------  ---------
SHEPHERD       <00>  192.9.1.134  PERMANENT  UNCHANGED

NetBIOS>
```

- *LIST CACHE GROUP*

Visualiza las entradas de cache que existen para nombres de grupo NetBIOS. Para una descripción de los campos en esta visualización, véase el comando **LIST CACHE NAME** en esta misma sección.

Ejemplo:

```
NetBIOS> LIST CACHE GROUP

Cnt  NetBIOS Name         Entry Type  Rem Path St  IP Address(es)
---  -------------------  ----------  -----------  ---------------
  1  ID             <1d>  DYNAMIC     GROUP

NetBIOS>
```

- *LIST CACHE LOCAL*

Visualiza las entradas de cache local. Las entradas de cache local son aquellas que aprende el router a través de la red de bridge local. Para una descripción de los campos en esta visualización, véase el comando **LIST CACHE NAME** en esta misma sección.

Para clientes NetBIOS el Estado de Ruta Local (Local Path State) siempre es Uknown (Desconocido) y los campos de Dirección MAC (MAC Address) están siempre vacíos.

Ejemplo:

```
NetBIOS> LIST CACHE LOCAL

Cnt  NetBIOS Name         Loc Path St  MAC Address   Routing Information
---  -------------------  -----------  ------------  -------------------------
  1  MARTINS        <00>  UNKNOWN
  2  LAB486         <00>  UNKNOWN
  3  MABERED        <20>  UNKNOWN
  4  TEL0106        <20>  UNKNOWN
  5  TSERVER        <06>  UNKNOWN

NetBIOS>
```

- *LIST CACHE NAME*

~~Visualiza una entrada de cache para un nombre específico NetBIOS. Utilizar los siguientes comodines para simplificar la búsqueda:~~

*****	Significa cualquier cadena de caracteres. Por ejemplo, “San*” podría producir: San Francisco Santa Fe San Juan
?	Significa cualquier carácter único.
$	Debe coincidir con el último carácter en un nombre.

Los siguientes ejemplos son utilizaciones válidas de comodines que coinciden con San Francisco:

Fran	S??*?????????
San?Fran?isco	S’*
*S**	S?a?n?F?a?c?s?
**o*	????????????

Isco? Isco$

*San?F** *

Utilizar tantos comodines como se quiera, hasta el número máximo de caracteres en un nombre NetBIOS (15 ó 16 dependiendo de cuántos caracteres significativos se configuren con el comando **SET CACHE-PARMS**).

Nota: Los nombres NetBIOS son sensibles a mayúsculas y minúsculas.

Ejemplo:

```
NetBIOS> LIST CACHE NAME
Enter up to 15 characters of NetBIOS name (wild cards ok)[]? TEST

NetBIOS Name         Name Type          Entry Type
-------------------  -----------------  ----------
TEST           <00>  INDIVIDUAL LOCAL   DYNAMIC

    Count of name cache entry hits:     0

    Age of name cache entry:            137535
    Age of name cache last reference:   137536

    Local path information:

        Loc Path St  Timestamp  MAC Address    LFS   Routing Information
        -----------  ---------  ------------  -----  ------------------
        UNKNOWN      254372

    Remote path information:

        Rem Path St  Timestamp   LFS   IP Address(es)
        -----------  ---------  -----  --------------
        UNKNOWN      254374

Do you wish to continue(Yes/No)(Y)? y
NetBIOS>
```

NetBIOS Name El nombre NetBIOS de la entrada.

Name Type Tipo de nombre NetBIOS. Los tipos posibles son:

INDIVIDUAL	Nombre individual NetBIOS.
GROUP	Nombre de grupo NetBIOS.
UNKNOWN	El router no tiene información sobre el nombre, indicando que una búsqueda de un nombre no es completa.
LOCAL	Una entrada que el router puede alcanzar localmente a través de la red de bridge.
REMOTE	Una entrada que el router puede buscar remotamente a través de una sesión DLSw TCP.

Entry Type Los posibles tipos de entrada son:

	PERMANENT	Entradas que se añaden en el prompt `NetBIOS config>` utilizando el comando **ADD CACHE-ENTRY**.
	STATIC	Entradas que se añaden en el prompt `NetBIOS>` utilizando el comando **ADD CACHE ENTRY**.
	DYNAMIC	Entradas que aprende el router a través del procesamiento Name-Query y Name-Recognized.
Count of name cache entry hits	Número de veces que se hizo referencia a la entrada.	
Age of name cache entry	Número de ticks del temporizador desde que se añadió la entrada. Los ticks del temporizador varían de acuerdo con la plataforma de hardware.	
Age of name cache last Reference	Número de ticks del temporizador desde que se añadió una entrada a la plataforma de hardware.	
Local path information:		
Loc Path St	Estado de la Ruta Local. Los mejores estados posibles son:	
	BEST FOUND	El router encontró la mejor ruta posible.
	UNKNOWN	El router todavía no ha encontrado la mejor ruta hacia este equipo.
	GROUP	El router no busca la mejor ruta para nombres de grupo.
	SEARCH LTD	El router está dirigiendo una búsqueda limitada para este nombre NetBIOS. Véase el comando **SET CACHE-PARMS** para más información sobre una búsqueda reducida.
	SEARCH ALL	El router está dirigiendo una búsqueda completa. Cuando expira el temporizador de búsqueda reducida del comando **SET CACHE-PARMS,** el router dirige una búsqueda completa.
Timestamp	Número de ticks del temporizador desde que el software actualizó por última vez una entrada. Los ticks del temporizador varían según la plataforma de hardware.	
MAC Address	Si la entrada es un servidor, visualiza la dirección MAC del servidor.	
LSF	Tamaño Máximo de Trama que puede utilizar el router para la entrada.	
Routing Information	Visualiza la información estándar del Campo de Información de Encaminamiento (Routing Information Field, RIF).	

Remote Path Information:

Rem Path St — Estado de la Ruta Remota. Los posibles estados son los siguientes.

BEST FOUND	El router encontró la mejor ruta posible.
UNKNOWN	El router todavía no ha encontrado la mejor ruta hacia este equipo.
GROUP	El router no busca la mejor ruta para nombres de grupo.
SEARCH LTD	El router está dirigiendo una búsqueda limitada para este nombre NetBIOS. Véase el comando **SET CACHE-PARMS** para más información sobre una búsqueda reducida.
SEARCH ALL	El router está dirigiendo una búsqueda completa. Cuando expira el temporizador de búsqueda reducida del comando **SET CACHE-PARMS,** el router dirige una búsqueda completa.

Timestamp — Número de ticks del temporizador desde que se actualizó por última vez una entrada. Los ticks del temporizador varían según la plataforma de hardware.

LSF — Tamaño Máximo de Trama que puede usar el router para la entrada.

IP Address — Dirección IP del compañero DLSw.

• LIST CACHE REMOTE

Visualiza las entradas de cache que aprende el encaminador sobre el DLSw WAN. Si el router no ha encontrado la mejor ruta, visualiza la dirección IP asociada con el vecino DLSw que puede alcanzar el equipo NetBIOS. Para una descripción de los campos en esta visualización, véase el comando **LIST CACHE NAME** en esta sección.

Ejemplo:

```
NetBIOS> LIST CACHE REMOTE

Cnt  NetBIOS Name         Entry Type  Rem Path St  IP Address(es)
---  -------------------  ----------  -----------  ---------------
  1  FIRMWARE       <1e>  DYNAMIC     BEST FOUND   20.55.27.33

NetBIOS>
```

• LIST CACHE UNKNOWN

Visualiza las entradas de cache donde el tipo de nombre NetBIOS es desconocido. El router introduce todas las entradas dinámicas como Unknown (Desconocidas) hasta que aprende el tipo de nombre. Después marca las entradas como locales, remotas o de grupo. Para una descripción de los campos en esta visualización, véase el comando **LIST CACHE NAME** en esta sección.

Ejemplo:

```
NetBIOS> LIST CACHE UNKNOWN

Cnt  NetBIOS Name         Entry Type  Loc Path St  Rem Path St  IP Address(es)
---  -------------------  ----------  -----------  -----------  ---------------
  1  CBRA           <1d>  DYNAMIC     UNKNOWN      SEARCH ALL
  2  HARDWARE       <1e>  DYNAMIC     UNKNOWN      SEARCH ALL
  3  JSPNRMPTGSBSSDI<52>  DYNAMIC     UNKNOWN      SEARCH ALL
  4  TEL01          <00>  DYNAMIC     UNKNOWN      SEARCH LTD

NetBIOS>
```

b) LIST FILTERS

Sintaxis:

```
NetBIOS> LIST FILTERS ?
ALL
BRIDGE
DLSW
```

- *LIST FILTERS ALL*

Visualiza si el filtrado de tipo de trama está encendido o apagado tanto para el bridging como para DLSw. Utilizar los comandos **SET FILTERS BRIDGE** y **SET FILTERS DLSW** para activar o desactivar estos filtros.

Ejemplo:

```
NetBIOS> LIST FILTERS ALL

Bridge name conflict filtering is      OFF
Bridge general bcast filtering is      OFF
Bridge trace control filtering is      OFF

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON

NetBIOS>
```

- *LIST FILTERS BRIDGE*

Visualiza si el filtrado del tipo de trama está encendido o apagado para el bridging. Utilizar el comando **SET FILTERS BRIDGE** para activar o desactivar estos filtros.

Ejemplo:

```
NetBIOS> LIST FILTERS BRIDGE

Bridge name conflict filtering is      OFF
Bridge general bcast filtering is      OFF
Bridge trace control filtering is      OFF

NetBIOS>
```

- *LIST FILTERS DLSW*

Visualiza si el filtrado de tipo de trama está encendida o apagada para ambos DLSw. Utilizar el comando **SET FILTERS DLSW** para activar o desactivar estos filtros.

Ejemplo:

```
NetBIOS> LIST FILTERS DLSW

DLS name conflict filtering is          ON
DLS general bcast filtering is          ON
DLS trace control filtering is          ON

NetBIOS>
```

c) *LIST GENERAL*

Visualiza el cache actual NetBIOS y la monitorización de filtrado.

Ejemplo:

```
NetBIOS> LIST GENERAL

Bridge-only Information:

Bridge duplicate filtering is          OFF
Bridge duplicate frame filter t/o      1.5 seconds

DLS-only Information:

DLS command frame retry count            5
DLS max remote name cache entries      100
DLS command frame retry timeout        0.5 seconds

DLS-Bridge Common Information:

Route caching is                       OFF
Significant characters in name          15
Max local name cache entries           500
Duplicate frame detect timeout         5.0 seconds
Best path aging timeout               60.0 seconds
Reduced search timeout                 1.5 seconds
Unreferenced entry timeout            5000 minutes

NetBIOS>
```

Nota: La Información solo DLS (DLS-only) solamente aparece si está activado el DLSw.

d) LIST STATISTICS

Sintaxis:

```
NetBIOS> LIST STATISTICS ?
CACHE
FRAMES
GENERAL
```

- *LIST STATISTICS CACHE*

Hace una lista de las estadísticas de cache de nombre.

Ejemplo:

```
NetBIOS> LIST STATISTICS CACHE

Local name cache entries                2
Remote name cache entries               1
Local individual names                  1
Remote individual names                 0
Group names                             0
Unknown names                           1
Name cache hits                         2312
Name cache misses                       3

NetBIOS>
```

- *LIST STATISTICS FRAMES*

Sintaxis:

```
NetBIOS> LIST STATISTICS FRAMES ?
BRIDGE
DLSW
```

LIST STATISTICS FRAMES BRIDGE

Hace una lista de las estadísticas de cache de nombre para el bridging.

Ejemplo:

```
NetBIOS> LIST STATISTICS FRAMES BRIDGE

Frames in cache                          3
Name query frames                        2
Status query frames                      1
Add name frames                          0
Add group name frames                    0
Name in conflict frames                  0
Frames not filtered as duplicates        0

NetBIOS>
```

LIST STATISTICS FRAMES DLSW

Hace una lista de las estadísticas de cache de nombre para DLSw.

Ejemplo:

```
NetBIOS> LIST STATISTICS FRAMES DLSW

Name query frames                        0
Status query frames                      0
Add name frames                          0
Add group name frames                    0
Name in conflict frames                  0
Frames not filtered as duplicates        0

NetBIOS>
```

- *LIST STATISTICS GENERAL*

Sintaxis:

```
NetBIOS> LIST STATISTICS GENERAL ?
BRIDGE
DLSW
```

LIST STATISTICS GENERAL BRIDGE

Visualiza los contadores de trama para el bridging.

Ejemplo:

```
NetBIOS> LIST STATISTICS GENERAL BRIDGE

Frames received                      46705
Frames discarded                         0
Frames forwarded to bridge           46705
Frames forwarded to DLS              43716

NetBIOS>
```

LIST STATISTICS GENERAL DLSW

Visualiza los contadores de trama para DLSw.

Ejemplo:

```
NetBIOS> LIST STATISTICS GENERAL DLSW

Frames received                          0
Frames discarded                         0
Frames forwarded to bridge               0

NetBIOS>
```

4.8. SET

Configura los parámetros de name caching, enciende o apaga el filtrado de tipo de trama para el bridging o DLSw, y ajusta los temporizadores del filtrado de trama duplicada y los temporizadores de reintento de trama. También visualiza el nombre NetBIOS y el prompt de filtrado de byte.

Sintaxis:

```
NetBIOS> SET ?
CACHE-PARMS
FILTERS
GENERAL
```

a) SET CACHE-PARMS

Configura los parámetros de name caching que se aplican al bridging o al DLSw.

Ejemplo:

```
NetBIOS> SET CACHE-PARMS

Significant characters in name[15]?
Best path aging timeout value in seconds[60.0]?
Reduced search timeout value in seconds[1.5]?
Unreferenced entry timeout value in minutes[5000]?
Max nbr local name cache entries[500]?
Max nbr remote name cache entries[100]?

Cache parameters set

NetBIOS>
```

Significant characters in name

Determina si el router considera 15 ó 16 caracteres cuando busca el nombre NetBIOS. Si se introducen

- 15, el router ignora el décimo sexto carácter.
- 16, el router incluye el décimo sexto carácter cuando busca entradas de cache.

El valor predeterminado es 15.

Best path aging timeout	Período de tiempo en segundos que el router considera que la dirección y la ruta para una entrada de cache local son la mejor ruta hasta ese equipo. Cuando pasa este tiempo, el router borra la entrada de cache de nombre e intenta descubrir una nueva ruta que sea mejor para el nombre NetBIOS. Para determinar la mejor ruta, el router considera el tiempo de transmisión entre nodos en todas las posibles rutas que conectan dichos nodos, así como el tamaño más largo de trama. El router no considera una ruta como posible si no puede acomodar la trama más larga NetBIOS que puede ser transmitida por la ruta. El valor por defecto es 60 segundos. El rango de valores es de 1,0 a 100,0 segundos.
Reduced search timeout	Cuando el router recibe un Name-Query, Status-Query, o Datagram durante el período de vencimiento de temporización, busca basándose en la información actual de cache de nombre NetBIOS. Si el router recibe una trama duplicada después de que pase este tiempo, presume que la ruta anterior ya no es válida y aumenta su búsqueda. El router envía la trama duplicada tanto a los bridges como a DLSw. El DLSw difunde el correspondiente mensaje SSP a todos los posibles compañeros DLSw. El valor por defecto es 1,5 segundos. El rango de valores es de 1,0 a 100,0 segundos.
Unreferenced entry timeout	El router mantiene un nombre que no está referenciado en su cache durante este tiempo antes de borrarlo. Si la cache se llena, el router elimina las entradas más rápidamente. El valor por defecto es de 5000 minutos. El rango de valores es de 1,0 a 100000 minutos.
Max nbr local name cache entries	Número máximo de entradas locales que el router almacena en la cache de nombres. Las entradas locales son aquellas que aprende el encaminador por medio del bridge. El valor por defecto es 500. El rango de valores es de 1 a 30.000. Para optimizar la utilización memoria, utilización del procesador y la cantidad de tráfico broadcast, hay que establecer este número tan cerca como sea posible del número total de equipos NetBIOS (servidores y clientes) que están activados en esa red de bridge local del router.
Max nbr remote name cache entries	Número máximo de las entradas aprendidas remotamente, las entradas de nombre de grupo y las entradas desconocidas. El valor por defecto es 100. El rango de valores es de 1 a 30.000. Para optimizar la utilización de memoria, la utilización del procesador y la cantidad de tráfico broadcast, establecer este número con arreglo al número de clientes NetBIOS remotos en la red de bridge local en este router, y sumarle aproximadamente un 25% adicional.

b) SET FILTERS

Sintaxis:

```
NetBIOS> SET FILTERS ?
BRIDGE
BYTE
DLSW
NAME
```

- *SET FILTERS BRIDGE*

Enciende o apaga el filtrado de tipo de trama para el bridging.

Ejemplo:

```
NetBIOS> SET FILTERS BRIDGE

Filter Name Conflict frames(Yes/No)(N)?

Name conflict filtering is             OFF

Filter General Broadcast frames(Yes/No)(N)? y

General broadcast filtering is          ON

Filter Trace Control frames(Yes/No)(N)?

Trace control filtering is             OFF

NetBIOS>
```

- *SET FILTERS BYTE*

Desde el prompt `NetBIOS>`, visualiza el prompt de monitorización de filtrado NetBIOS (`NETBIOS Filter>`).

Este prompt permiten establecer los filtros de byte NetBIOS.

Véase el **Capítulo 11 "Configuración y Monitorización de Filtrado de Nombre y Byte NetBIOS"** para más información sobre los comandos disponibles en este prompt.

Ejemplo:

```
NetBIOS> SET FILTERS BYTE
NETBIOS Filtering configuration
NETBIOS Filter>
```

- *SET FILTERS DLSW*

Establece los filtros de tipo de trama para tráfico DLSw.

Ejemplo:

```
NetBIOS> SET FILTERS DLSW

Filter Name Conflict frames(Yes/No)(Y)? y

Name conflict filtering is              ON

Filter General Broadcast frames(Yes/No)(Y)? n

General broadcast filtering is         OFF

Filter Trace Control frames(Yes/No)(Y)? n

Trace control filtering is              OFF

NetBIOS>
```

- *SET FILTERS NAME*

Desde el prompt `NetBIOS>`, visualiza el prompt de monitorización de filtrado `NETBIOS Filter>`.

Este prompt permiten establecer los filtros de nombre NetBIOS.

Véase el **Capítulo 11 "Configuración y Monitorización del Filtrado de Nombre y Byte NetBIOS"** para más información sobre los comandos disponibles en este prompt.

Ejemplo:

```
NetBIOS> SET FILTERS NAME
NETBIOS Filtering configuration
NETBIOS Filter>
```

c) SET GENERAL

Establece el timeout de la trama duplicada, el timeout de detección de trama duplicada y el contador y timeout de reintento de trama de comando. Véase el apartado 2.3 **"Filtrado de Trama Duplicada"** en el Capítulo 9 para más información sobre cómo duplicar el trabajo de los filtros de trama.

Ejemplo:

```
NetBIOS> SET GENERAL

WARNING! Setting Duplicate Frame Filter Timeout to zero...
         disables duplicate frame checking!

Duplicate frame filter timeout value in seconds[1.5]?
Duplicate frame detect timeout value in seconds[5.0]?
Command frame retry count[5]?
Command frame retry timeout value in seconds[0.5]?

General parameters set

NetBIOS>
```

¡Advertencia! Establecer el timeout de Filtro de Trama Duplicada en cero…..desactiva el control de trama duplicada.

Si el DLSw NO está activado, el software NO indica la parte:

```
Command frame retry count[5]?
Command frame retry timeout value in seconds[0.5]?
```

Duplicate frame filter timeout
Se dirige sólo a tráfico de bridge si está activada el filtrado de tramas duplicadas.
Durante este período de timeout, el router filtra todas las tramas duplicadas que recibe.
El rango de valores es de 0,0 a 100,000 segundos. El cero desactiva el control de trama duplicada. El valor por defecto es 1,5 segundos.

Duplicate frame detect timeout
Se dirige tanto al tráfico de bridge como al DLSw.
Tiempo durante el que el router almacena entradas en su base de datos de filtro de trama. Cuando pasa este tiempo, el router crea entradas nuevas para las tramas nuevas que recibe.
El rango de valores es de 0,0 a 100,000 segundos. El valor por defecto es 5 segundos.

Command frame retry count
Se aplica al tráfico DLSw.
Número de tramas duplicadas NetBIOS UI que el router de destino DLSw envía a sus LAN localmente relacionados. El router envía estas tramas en intervalos especificados por el parámetro *command frame retry timeout.*
El rango de valores es de 0,0 a 10. El valor por defecto es de 5 segundos.

Command frame retry timeout
Se aplica al tráfico DLSw.
Éste es el intervalo en que el router DLSw vecino reintenta enviar tramas duplicadas NetBIOS UI a su red de bridge local.
El rango de valores es de 0,0 a 10,00 segundos. El valor por defecto es 5 segundos.

4.9. EXIT

Vuelve al prompt anterior.

Sintaxis:

```
NetBIOS> EXIT
```

Ejemplo:

```
NetBIOS> EXIT
ASRT>
```

Capítulo 11
Configuración y Monitorización de Filtrado de Nombre y Byte NetBIOS

1. Visualización de los Prompts de Filtrado NetBIOS

Esa sección describe los comandos de configuración y monitorización del Filtrado Nombre y Byte NetBIOS.

Introducir los comandos de configuración en el prompt `NETBIOS Filter config>`. Visualizar este prompt como se describe abajo:

```
Config> PROTOCOL ASRT

-- ASRT Bridge user configuration --
ASRT config> NETBIOS

NetBIOS Support User Configuration

NetBIOS config> SET FILTERS NAME
NETBIOS Filtering configuration
NETBIOS Filter config>
```

Introducir los comandos de monitorización en el prompt `NetBIOS Filter>`. Visualizar este prompt como se describe abajo:

```
ASRT> NETBIOS

NetBIOS Support User Console

NetBIOS> SET FILTERS NAME
NETBIOS Filter>
```

2. Establecimiento de Filtros de Nombre y Byte NetBIOS

Un filtro de nombre o de byte está formado por:

- Listas de filtro, que están compuestas por uno o más elementos de filtro.
- Elementos de filtro, que especifican los nombres NetBIOS que se quieren filtrar.

El router compara cada elemento de filtro con paquetes en el orden en que se introducen los elementos de filtro.

Se configuran el nombre NetBIOS y los filtros de byte para cada puerto y se especifica si el filtro se dirige a paquetes de entrada o salida.

Las siguientes secciones proporcionan ejemplos de cómo establecer un filtro de nombre anfitrión y un filtro de byte. Las secciones "**Comandos de Configuración de Filtros de Nombre y Byte NetBIOS**" "**Comandos de Monitorización de Filtros de Nombre y Byte NetBIOS**" describen los comandos utilizados en estos ejemplos.

Ejemplo 1:

Utilizar el siguientes procedimiento como directriz para crear un filtro de nombre. Antes de comenzar, visualícese el prompt `NETBIOS Filter config>`.

```
Config> PROTOCOL ASRT

-- ASRT Bridge user configuration --
ASRT config> NETBIOS

NetBIOS Support User Configuration

NetBIOS config> SET FILTERS NAME
NETBIOS Filtering configuration
NETBIOS Filter config>
```

1. Crear una lista vacía de filtro de nombre.

   Introducir **CREATE NAME-FILTER-LIST**. El software pide que se le de un nombre a la lista de filtro.

```
NETBIOS Filter config> CREATE NAME-FILTER-LIST
Handle for Name Filter List []? boston
```

2. Visualiza el prompt de configuración para la lista de filtro que se acaba de crear. Introducir **UPDATE**. El router pide el nombre de la lista de filtro.

```
NETBIOS Filter config> UPDATE
Handle for Filter List []? boston
Name Filter List Configuration
NETBIOS Name boston config>
```

3. Añadir elementos de filtro a la lista de filtro.

   Cuando se añade un elemento de filtro, se deben especificar los siguientes parámetros en este orden:

- *Inclusive* (se hace bridge) o *exclusive* (se descarta).
- ASCII o *hex* es cómo se introduce el nombre.
- *Hostname*, es el nombre real en formato ASCII o hexadecimal. Esta entrada es sensible a mayúsculas y minúsculas.
- *Caracter décimo sexto especial* es un parámetro opcional para utilizar con cadenas ASCII que contienen menos de 16 caracteres.

El siguientes ejemplo añade un elemento de filtro a la lista de filtro boston, que permite hacer bridge (*configurados como Inclusive*) con paquetes que contienen el nombre wetsboro (una cadena ASCII). No está configurado el *Caracter décimo sexto especial*.

```
NETBIOS Name boston config> ADD INCLUSIVE ASCII
Hostname[]? westboro
Special 16th character in ASCII hex (<CR> for no special character)[]?
NETBIOS Name boston config>
```

Si no se quiere que aparezcan prompts, introducir todos los parámetros como una cadena en la línea de comando. Dejar un espacio entre cada parámetro.

4. Verificar la entrada de elemento de filtro.

   Introducir **LIST** para verificar la entrada.

```
NETBIOS Name boston config> LIST

NAME Filter List Name: boston
NAME Filter List Default: Inclusive

 Item #   Type    Inc/Ex    Hostname         Last Char

   1      ASCII    Inc      westboro

NETBIOS Name boston config>
```

5. Añadir elementos de filtro adicionales a la lista de filtro.

   Repetir el **paso 3** para añadir elementos de filtro a la lista de filtro.

   El orden en que se introducen los elementos de filtro es importante. Éste determina cómo el router aplica los elementos de filtro a un paquete. La aparición de la primera coincidencia detiene la aplicación de elementos de filtro y el router o envía o descarta los paquetes, dependiendo de si el elemento de filtro es *Inclusive* o *Exclusive*.

   Introducir los elementos de filtro más comunes primero consigue que el proceso de filtrado sea más eficiente porque el software está mas predispuesto a emparejar al principio de la lista.

   Si el paquete no coincide con ningún elemento del filtro, el router utiliza la condición por defecto (*Inclusive* o *Exclusive*) de la lista de filtro. Se puede cambiar la condición por defecto de la lista introduciendo **DEFAULT INCLUSIVE** o **DEFAULT EXCLUSIVE** en el prompt de configuración de la lista de filtro. Por ejemplo:

```
NETBIOS Name boston config> DEFAULT EXCLUSIVE
```

6. Cuando se termina de añadir los elementos de filtro a la lista de filtro, introducir **EXIT** para volver al prompt `NETBIOS Filter config>`.

```
NETBIOS Name boston config> EXIT
NETBIOS Filter config>
```

7. Añadir la lista de filtro a la configuración.

Utilizar el comando **FILTER-ON**. Cuando se enciende un filtro de nombre, se deben especificar los siguientes parámetros en este orden.

- *Input* filtra los paquetes entrantes o *output* filtra los paquetes salientes.
- *Port Number* es el número configurado de puerto de bridge que se desea en el router.
- *Filter-list* es el nombre de la lista de filtro (que contiene los elementos de filtro) que se quiere incluir en este filtro.
- De manera opcional, añadir además la lista de filtros al filtro. Introducir **AND** o **OR** en mayúsculas seguido de un nombre de lista de filtro.

El siguiente ejemplo añade un filtro de nombre que consta de la lista de filtro boston. El router evalúa todos los paquetes entrantes en el puerto 2 de acuerdo con los elementos de filtro en la lista de filtro boston. Esto significa que el router utiliza el bridge en todos los paquetes entrantes en el puerto 3 que contienen el nombre westboro.

```
NETBIOS Filter config> FILTER-ON INPUT
Port Number[1]? 2
Filter List[]? boston
Operator (AND or OR)[]?
NETBIOS Filter config>
```

Otro ejemplo:

```
NETBIOS Filter config> FILTER-ON OUTPUT
Port Number[1]?
Filter List[]? boston
Operator (AND or OR)[]? OR
Filter List[]? newyork
Operator (AND or OR)[]?
NETBIOS Filter config>
```

8. Introducir **LIST** para verificar el nuevo filtro.

```
NETBIOS Filter config> LIST

NETBIOS Filtering: Disabled

NETBIOS Filter Lists
--------------------

    Handle           Type

    boston           Name
    newyork          Name
```

```
NETBIOS Filters
---------------

    Port #      Direction      Filter List Handle(s)

       2          Input        boston
       1          Output       boston OR newyork

NETBIOS Filter config>
```

9. Activar globalmente el filtrado de nombre y Byte NetBIOS en el router.
   Introducir **ENABLE NETBIOS-FILTERING**.

```
NETBIOS Filter config> ENABLE NETBIOS-FILTERING
NETBIOS Filter config>
```

Ejemplo 2: Creación de un filtro de Byte

Utilizar el siguiente procedimiento como directriz para crear un filtro de byte. Antes de comenzar, visualícese el prompt `NETBIOS Filter config>`.

```
Config> PROTOCOL ASRT

-- ASRT Bridge user configuration --
ASRT config> NETBIOS

NetBIOS Support User Configuration

NetBIOS config> SET FILTERS BYTE
NETBIOS Filtering configuration
NETBIOS Filter config>
```

1. Crear una lista de filtro de byte vacía.
   Utilizar el comando **CREATE BYTE-FILTER-LIST**.

```
NETBIOS Filter config> CREATE BYTE-FILTER-LIST
Handle for Byte Filter List[]? westport
NETBIOS Filter config>
```

2. Visualizar el prompt de configuración para la lista de filtro que se acaba de crear.
   Introducir **UPDATE**. El router indica el nombre de la lista de filtro.

```
NETBIOS Filter config> UPDATE
Handle for Filter List[]? westport
Byte Filter List Configuration
NETBIOS Byte westport config>
```

3. Añadir elementos de filtro a la lista de filtro de byte.
   Cuando se añade un elemento de filtro, se deben especificar los siguientes parámetros en este orden:
   - *Inclusive* (se hace bridge) or *exclusive* (se descarta)
   - *Byte offset* es el número de bytes (en decimal) de desplazamiento dentro del paquete que el router está filtrado. Esto comienza en la cabecera NetBIOS del paquete. Cero específica que el router examina todos los bytes del paquete.

- *Hex pattern* es un número hexadecimal que utiliza el router para comparar con los bytes empezando por el byte de desplazamiento (byte offset). Véase los apartados "**Comandos de configuración de Nombre y Byte NetBIOS**" y "**Comandos de Monitorización de Nombre y Byte NetBIOS**"para las normas de sintaxis.
- *Hex mask* si aparece, debe ser de la misma longitud que el patrón hexadecimal. Se efectua una operación lógica AND con los bytes del paquete, empezando con el byte offset, antes de que el router compare el resultado con el patrón hexadecimal. Si se omite la máscara hexadecimal (*Hex mask*), el router considera que son todos 1 binarios.

El siguiente ejemplo añade un elemento de filtro a la lista de filtro de byte westboro que provoca que el router utilice un bridge en los paquetes con un patrón hexadecimal 0x12345678 en un byte offset de 0 (configurado como *Inclusive*). No aparece ningún *Hex mask*.

```
NETBIOS Byte westport config> ADD INCLUSIVE
Byte Offset[0]?
Hex Pattern[]? 12345678
Hex Mask (<CR> for no mask)[]?
NETBIOS Byte westport config>
```

4. Verificar la entrada del elementos de filtro con el comando **LIST**.

```
NETBIOS Byte westport config> LIST

BYTE Filter List Name: westport
BYTE Filter List Default: Inclusive

 Item #   Inc/Ex   Offset  Pattern              Mask

   1       Inc        0    0x12345678           0xffffffff

NETBIOS Byte westport config>
```

5. Añadir elementos de filtro adicionales a la lista de filtro.

   Repetir el **paso 3** para añadir elementos de filtro a la lista de filtro.

   El orden en que se introducen los elementos de filtro es importante. Éste determina cómo el router aplica el filtro a un paquete. La aplicación de la primera coincidencia detiene la aplicación de elementos de filtro y el router o envía o descarta el paquete, dependiendo de si el filtro es *Inclusive* o *Exclusive*.

   Introducir primero los elementos de filtro más comunes provoca que el proceso de filtrado sea más eficiente porque el software está más predispuesto a encontrar una coincidencia al principio de la lista en lugar de tener que comprobar toda las lista antes de hacer un emparejamiento.

   Si el paquete no coincide con ningún elemento de filtro, el router utiliza la condición por defecto (*Inclusive* o *Exclusive*) de la lista de filtro. Se puede cambiar la condición por defecto de la lista introduciendo **DEFAULT INCLUSIVE** o **DEFAULT EXCLUSIVE** en el prompt de configuración de la lista de filtro. Por ejemplo:

```
NETBIOS Byte westport config> DEFAULT EXCLUSIVE
NETBIOS Byte westport config>
```

6. Cuando se ha terminado de añadir los elementos de filtro a la lista, introducir **EXIT** para volver al prompt to the `NetBIOS Filter config>`.

```
NETBIOS Byte westport config> EXIT
NETBIOS Filter config>
```

7. Añadir el filtro a la configuración.

   Utilizar el comando **FILTER-ON**. Cuando se enciende un filtro de byte, se deben especificar los siguientes parámetros en este orden:

- *Input* filtra los paquetes entrantes o *output* filtra los paquetes salientes.
- *Port Number* es el número de puerto de bridging configurado que se requiere.
- *Filter list* es el nombre de la lista de filtro (que contiene los elementos de filtro) que se quiere incluir en este filtro.
- De forma opcional, añadir listas de filtro al filtro. Introducir **AND** o **OR** en letras mayúsculas seguidas por un nombre de lista de filtro.

El siguiente ejemplo añade un filtro de byte a los paquetes salientes del puerto 3. Está formado por la lista de filtro de byte westboro. El router evalúa todos los paquetes que salen del puerto 3, de acuerdo con los elementos de filtro que contiene la lista de filtro westboro.

```
NETBIOS Filter config> FILTER-ON OUTPUT
Port Number[1]? 3
Filter List[]? westport
Operator (AND or OR)[]?
NETBIOS Filter config>
```

8. Verificar el nuevo filtro.

   Introducir **LIST** para verificar el filtro.

```
NETBIOS Filter config> LIST

NETBIOS Filtering: Enabled

NETBIOS Filter Lists
--------------------

    Handle           Type

    boston           Name
    newyork          Name
    westport         Byte

NETBIOS Filters
---------------

    Port #      Direction      Filter List Handle(s)

       2          Input        boston
       1          Output       boston OR newyork
       3          Output       westport

NETBIOS Filter config>
```

9. Activar globalmente el filtro de Nombre y Byte NetBIOS en el router.

   Introducir **ENABLE NETBIOS-FILTERING**.

```
NetBIOS Filter config> ENABLE NETBIOS-FILTERING
```

3. Comandos de Configuración de Filtros de Nombre y Byte NetBIOS

La Tabla 11.1 hace una lista de los comandos de configuración de Filtros de Nombre y Byte NetBIOS.

Tabla 11.1. Comandos de configuración de Filtros de Nombre y Byte NetBIOS

Comando	Función
? (AYUDA)	Hace una lista de los comandos u opciones disponibles.
CREATE	Crea las listas de filtro de byte y de nombre para el filtrado NetBIOS.
DELETE	Borra las listas de filtro de byte y de nombre para el filtrado NetBIOS.
DISABLE	Desactiva el filtrado de nombre NetBIOS y de byte en el encaminador.
ENABLE	Activa el filtrado de nombre NetBIOS y de byte en el encaminador.
FILTER-ON	Asigna un filtro a un puerto específico. Se puede aplicar después este filtro a los paquetes de entrada o salida NetBIOS en el puerto específico.
LIST	Visualiza toda la información relativa a los filtros que se han creado.
UPDATE	Añade información o la borra de una lista de filtro nombre o de byte.
EXIT	Vuelve al prompt anterior.

3.1. ? (AYUDA)

Hace una lista de los comandos u opciones disponibles.

Sintaxis:

```
NETBIOS Filter config> ?
```

Ejemplo:

```
NETBIOS Filter config> ?
CREATE
DELETE
DISABLE
ENABLE
FILTER-ON
LIST
UPDATE
EXIT
NETBIOS Filter config>
```

3.2. CREATE

Crea una lista de filtro de byte o una lista de filtro de nombre.

Sintaxis:

```
NETBIOS Filter config> CREATE ?
BYTE-FILTER-LIST
NAME-FILTER-LIST
```

a) CREATE BYTE-FILTER-LIST

Crea una lista de filtro de byte. Hay que dar a la lista un único nombre de hasta 16 caracteres. Utilizar este nombre para identificar la lista del filtro.

Ejemplo:

```
NETBIOS Filter config> CREATE BYTE-FILTER-LIST
Handle for Byte Filter List[]? westport
NETBIOS Filter config>
```

b) CREATE NAME-FILTER-LIST

Crea una lista de filtro de nombre. Hay que dar a la lista un único nombre de hasta 16 caracteres. Utilizar este nombre para identificar la lista del filtro.

Ejemplo:

```
NETBIOS Filter config> CREATE NAME-FILTER-LIST
Handle for Name Filter List[]? newyork
NETBIOS Filter config>
```

3.3. DELETE

Borra las listas de filtro de byte, las listas de filtro de nombre anfitrión, y filtra. **DELETE** borra toda la información relacionada con las listas de filtro de byte y de filtro de nombre anfitrión.

Sintaxis:

```
NETBIOS Filter config> DELETE ?
FILTER
BYTE-FILTER-LIST
NAME-FILTER-LIST
```

a) DELETE FILTER

Sintaxis:

```
NETBIOS Filter config> DELETE FILTER ?
INPUT
OUTPUT
```

- ***DELETE FILTER INPUT***

Borra un filtro creado con el comando **FILTER-ON INPUT**.

Borra toda la información relacionada con el filtro y llena cualquier vacío que aparezca entre los números del filtro.

Ejemplo:

```
NETBIOS Filter config> DELETE FILTER INPUT
Port Number[1]? 2
NETBIOS Filter config>
```

- ***DELETE FILTER OUTPUT***

Borra un filtro creado con el comando **FILTER-ON OUTPUT**.

Borra toda la información relacionada con el filtro y llena cualquier vacío que aparezca entre los números del filtro.

Ejemplo:

```
NETBIOS Filter config> DELETE FILTER OUTPUT
Port Number[1]? 3
NETBIOS Filter config>
```

b) DELETE BYTE-FILTER-LIST

Borra una lista de filtro de byte.

Ejemplo:

```
NETBIOS Filter config> DELETE BYTE-FILTER-LIST
Handle for Byte Filter List[]? seattle
NETBIOS Filter config>
```

c) DELETE NAME-FILTER-LIST

Borra una lista de filtro de nombre anfitrión.

Ejemplo:

```
NETBIOS Filter config> DELETE NAME-FILTER-LIST
Handle for Name Filter List[]? alaska
NETBIOS Filter config>
```

3.4. DISABLE

Desactiva globalmente el filtrado de Nombre y Byte NetBIOS en el router.

Sintaxis:

```
NETBIOS Filter config> DISABLE NETBIOS-FILTERING
```

Ejemplo:

```
NETBIOS Filter config> DISABLE NETBIOS-FILTERING
NETBIOS Filter config>
```

3.5. ENABLE

Activa globalmente el filtrado de Nombre y Byte NetBIOS en el router.

Sintaxis:

```
NETBIOS Filter config> ENABLE NETBIOS-FILTERING
```

Ejemplo:

```
NETBIOS Filter config> ENABLE NETBIOS-FILTERING
NETBIOS Filter config>
```

3.6. FILTER-ON

Asigna una o más listas de filtro asignados anteriormente a la salida o entrada de un puerto específico.

Sintaxis:

```
NETBIOS Filter config> FILTER-ON ?
INPUT
OUTPUT
```

a) FILTER-ON INPUT

Asigna una o más listas de filtro a los paquetes entrantes en un puerto. El router aplica el filtro que resulta a todos los paquetes NetBIOS entrantes en un puerto específico.

Port Number es el número de puerto de bridging configurado en el router. El número de puerto identifica este filtro. Introducir el comando **LIST** para ver una lista de números de puerto. Utilizar el comando **CREATE** para hacer una lista de filtro. Para añadir listas de filtros adicionales a este puerto, introducir **AND** o **OR** en letras mayúsculas seguido por el nombre de la lista de filtro.

El router aplica el filtro que se ha creado con este comando a todos los paquetes NetBIOS entrantes en el puerto específico. El router evalúa cada lista de filtro en la línea de comando de izquierda a derecha. Si un paquete coincide con un filtro *Inclusive* el router hace bridge con el paquete. Si el paquete coincide con un filtro *Exclusive*, el router descarta el paquete.

Si el paquete no es uno de los tipos que soportan el filtrado de Nombre o Byte NetBIOS, el router hace bridge con el paquete.

Ejemplo:

```
NETBIOS Filter config> FILTER-ON INPUT
Port Number[1]? 2
Filter List[]? boston
Operator (AND or OR)[]?
NETBIOS Filter config>
```

b) FILTER-ON OUTPUT

Asigna una o más listas de filtro a los paquetes salientes de un puerto. El router aplica el filtro que resulta a todos los paquetes salientes NetBIOS de un puerto específico.

Port Number es un número de puerto de bridging configurado en el encaminador. El número de puerto identifica este filtro. Introducir el comando **LIST** para ver una lista de números de puerto. Utilizar el comando **CREATE** para hacer una lista de filtro. Para añadir listas de filtros adicionales a este puerto, introducir **AND** o **OR** en letras mayúsculas seguido por el nombre de la lista de filtro.

El router aplica el filtro que se ha creado con este comando a todos los paquetes NetBIOS salientes de un puerto específico. El router evalúa cada lista de filtro en la línea de comando de izquierda a derecha. Si un paquete coincide con un filtro *Inclusive*, el router hace bridge con el paquete. Si el paquete coincide con un filtro *Exclusive*, el router descarta el paquete.

Si el paquete no es de uno de los tipos que soportan el filtrado de Nombre o Byte NetBIOS, el router hace bridge con el paquete.

Ejemplo:

```
NETBIOS Filter config> FILTER-ON OUTPUT
Port Number[1]?
Filter List[]? boston
Operator (AND or OR)[]? OR
Filter List[]? newyork
Operator (AND or OR)[]?
NETBIOS Filter config>
```

3.7. LIST

Visualiza información de todos los filtros de nombre y de byte.

Sintaxis:

```
NETBIOS Filter config> LIST
```

Ejemplo:

```
NETBIOS Filter config> LIST

NETBIOS Filtering: Enabled

NETBIOS Filter Lists
--------------------

    Handle           Type

    boston           Name
    newyork          Name
    westport         Byte

NETBIOS Filters
---------------

    Port #      Direction      Filter List Handle(s)

       2          Input        boston
       1          Output       boston OR newyork
       3          Output       westport

NETBIOS Filter config>
```

NetBIOS Filtering	Visualiza si el filtrado NetBIOS está activado o no.
NetBIOS Filter Lists	Muestra el nombre (identificador) de las listas de filtro, así como el tipo, tanto de Nombre como de Byte.
NetBIOS Filters	Número de puerto asignado y dirección (entrada o salida) de cada filtro. El Identificador(es) de Lista de Filtro visualiza el nombre(s) de la(s) lista(s) que compone el filtro.

3.8. UPDATE

Visualiza el prompt `NETBIOS Byte (or Name) filter-list config>`, lo que permite actualizar la lista de filtro específico. En este prompt se puede añadir, borrar, hacer una lista o mover elementos en las listas de filtro de Nombre o de Byte. También se puede establecer el valor por defecto de cada lista de filtro como *Inclusive* o *Exclusive*.

Sintaxis:

```
NETBIOS Filter config> UPDATE <lista-de-filtros>
```

Ejemplo:

```
NETBIOS Filter config> UPDATE
Handle for Filter List[]? newyork
Name Filter List Configuration
NETBIOS Name newyork config>
```

En este nuevo prompt, se pueden introducir varios comandos.

3.9. EXIT

Vuelve al prompt anterior.

Sintaxis:

```
NETBIOS Filter config> EXIT
```

Ejemplo:

```
NETBIOS Filter config> EXIT

NetBIOS config>
```

4. Comandos de Monitorización de Filtros de Nombre y Byte NetBIOS

La Tabla 11.2 hace una lista de los comandos de Monitorización de Filtros de Nombre y Byte NetBIOS.

Tabla 11.2. Comandos de Filtros de Nombre y Byte NetBIOS

Comando	Función
? (AYUDA)	Hace una lista de los comandos u opciones disponibles.
LIST	Visualiza toda la información relativa a los filtros que se han creado.
EXIT	Vuelve al prompt anterior.

4.1. ? (AYUDA)

Hace una lista de los comandos u opciones disponibles.

Sintaxis:

```
NETBIOS Filter> ?
```

Ejemplo:

```
NETBIOS Filter> ?
LIST
EXIT
NETBIOS Filter>
```

4.2. LIST

Visualiza la información de todos los filtros, filtros de byte o filtros de nombre.

Sintaxis:

```
NETBIOS Filter> LIST ?
BYTE-FILTER-LISTS
NAME-FILTER-LISTS
FILTERS
```

a) LIST BYTE-FILTER-LISTS

Visualiza todas las listas de filtro de byte que se han creado.

Ejemplo:

```
NETBIOS Filter> LIST BYTE-FILTER-LIST

BYTE Filter List Name: westport
BYTE Filter List Default: Exclusive

 Filter Item #   Inc/Ex    Byte Offset  Pattern        Mask

      1        Inclusive       0        0x12345678     0xffffffff

NETBIOS Filter>
```

b) LIST NAME-FILTER-LISTS

Visualiza todas las listas de filtro de nombre que se han creado.

Ejemplo:

```
NETBIOS Filter> LIST NAME-FILTER-LISTS

NAME Filter List Name: boston
NAME Filter List Default: Inclusive

 Filter Item #   Type    Inc/Ex        Hostname       Last Char

       1         ASCII   Inclusive     westboro
       2         ASCII   Inclusive     seattle


NAME Filter List Name: newyork
NAME Filter List Default: Inclusive

 Filter Item #   Type    Inc/Ex        Hostname       Last Char

       1         ASCII   Inclusive     jersey

NETBIOS Filter>
```

c) LIST FILTERS

Hace una lista de todos los filtros que se han creado y el número de paquetes que el router ha filtrado como resultado de estos filtros.

Ejemplo:

```
NETBIOS Filter> LIST FILTERS

NETBIOS Filtering: Enabled

    Port #      Direction      Filter List Handle(s)   Pkts Filtered

       2          Input        boston                          0
       1          Output       boston OR newyork               0
       3          Output       westport                        0

NETBIOS Filter>
```

4.3. EXIT

Vuelve al prompt anterior.

Sintaxis:

```
NETBIOS Filter> EXIT
```

Ejemplo:

```
NETBIOS Filter> EXIT
NETBIOS>
```

5. Comandos de Actualización de la Lista de Filtro de Byte

En este apartado se describen los comandos disponibles en el prompt `NETBIOS Byte filter-list config>`.

`add` *inclusive* or *exclusive byte-offset hex-pattern hex-mask*

Añade un elemento de filtro a la lista de filtro. Cuando se añade un elemento de filtro, el router numera el elemento y visualiza el número del elemento de filtro que se acaba de añadir.

> ***Nota: Añadir elementos de filtro a las listas de filtro aumenta el tiempo de procesamiento de acuerdo con el tiempo que tarda en evaluar cada elemento de la lista. Puede afectar al rendimiento en tráfico NetBIOS intenso.***

El orden en que se introducen los elementos de filtro es importante en tanto que determina cómo el router aplica los elementos de filtro a un paquete. El router deja de comparar el paquete con el filtro cuando encuentra la primera coincidencia.

- *Inclusive* (se hace bridge) o *Exclusive* (se descarta).
- *Byte Offset* es el número de bytes (en decimal) de desplazamiento (offset) dentro del paquete que el router está filtrado. Esto comienza en la cabecera NetBIOS del paquete. El Cero especifica que el router examina todos los bytes del paquete.
- *Hex pattern* es un número hexadecimal que utiliza el router para comparar con los bytes empezando por el byte de desplazamiento (byte offset). Las normas de sintaxis para el *hex-pattern* incluyen hacerlo sin 0x en el frente, un máximo de 32 números, y un número par de números hexadecimales.
- *Hex mask* si aparece, debe ser de la misma longitud que el patrón hexadecimal. Se efectua una operación **AND** lógica con los bytes del paquete, empezando con el byte de offset, antes de que el router compare el resultado con el patrón hexadecimal. Si se omite la máscara hexadecimal (*Hex mask*), el router considera que son todos 1 binarios.

Si el offset y el patrón de un elemento de filtro de byte representa bytes que no existen en un paquete NetBIOS (por ejemplo, si el paquete es más corto de lo que se pensó cuando se estableció la lista de filtro de byte), el router no aplica el filtro al paquete. Si se utiliza una serie de elementos de filtro de byte para establecer una única lista de filtro NetBIOS, entonces no se prueba un paquete para el filtrado si cualquiera de los elementos de filtro de byte dentro de la lista de filtro NetBIOS representa bytes que no existen en el paquete NetBIOS.

Ejemplo:

```
NETBIOS Byte westport config> ADD INCLUSIVE
Byte Offset[0]?
Hex Pattern[]? 12345678
Hex Mask (<CR> for no mask)[]?
NETBIOS Byte westport config>
```

El siguiente ejemplo muestra cómo filtrar los Datagram Broadcast Packets.

Ejemplo:

```
NETBIOS Byte westport config> ADD INCLUSIVE
Byte Offset[0]? 4
Hex Pattern[]? 09
Hex Mask (<CR> for no mask)[]?
NETBIOS Byte westport config>
```

default inclusive or exclusive

Cambia el valor por defecto que se estableció por *Inclusive* o *Exclusive*. Si ninguno de los elementos de filtro coincide con los contenidos del paquete que el router considera para el filtrado, el router envía o descarta el paquete, dependiendo de lo establecido.

Sintaxis:

```
NETBIOS Byte filter-list config> DEFAULT
INCLUSIVE
EXCLUSIVE
```

Ejemplo 1:

```
NETBIOS Byte westport config> DEFAULT INCLUSIVE
NETBIOS Byte westport config>
```

Ejemplo 2:

```
NETBIOS Byte westport config> DEFAULT INCLUSIVE
NETBIOS Byte westport config>
```

delete filter-number

Borra un elemento de filtro de la lista de filtro. El software renumera inmediatamente la lista. Para ver una lista de los números elementos, hay que introducir el comando **LIST**.

Sintaxis:

```
NETBIOS Byte filter-list config> DELETE <nº filtro>
```

Ejemplo:

```
NETBIOS Byte westport config> DELETE
Filter Item Number[1]? 2
NETBIOS Byte westport config>
```

exit

Vuelve al nivel anterior de prompt de comando.

Sintaxis:

```
NETBIOS Byte filter-list config> EXIT
```

Ejemplo:

```
NETBIOS Byte westport config> EXIT
NETBIOS Filter config>
```

list

Visualiza la información relacionada con los elementos de filtro de la lista de filtro.

Sintaxis:

```
NETBIOS Byte filter-list config> LIST
```

Ejemplo:

```
NETBIOS Byte westport config> LIST

BYTE Filter List Name: westport
BYTE Filter List Default: Inclusive

 Item #   Inc/Ex   Offset  Pattern              Mask

   1       Inc        4    0x09                 0xff
   2       Ex         2    0x3344               0xffff

NETBIOS Byte westport config>
```

move *nº origen nº final*

Reordena los elementos de filtro dentro de la lista de filtro. Para ver una lista de los números de elementos, hay que introducir el comando **LIST**.

Sintaxis:

```
NETBIOS Byte filter-list config> MOVE <nº origen, nº final>
```

Ejemplo:

```
NETBIOS Byte filter-list config> MOVE
Source Filter Item Number [1] ?  3
After Destination Filter Item Number [0] ?  1
NETBIOS Byte filter-list config>
```

6. Actualizar los Comandos de la Lista de filtro de nombre

En este apartado se hace una lista de los comandos disponibles en el prompt `NETBIOS Name filter-list config>`.

Los comandos disponibles son:

- ADD
- DEFAULT
- DELETE
- EXIT
- LIST
- MOVE

add *inclusive* or *exclusive* ASCII *host-name special-16th-char*

Añade un elemento de filtro a la lista de filtro de nombre. El router compara las siguientes tramas y campos con la información que se introduce con este comando:

- ADD_GROUP_NAME_QUERY: Campo de nombre NetBIOS de origen.
- ADD_NAME_QUERY: Campo de nombre NetBIOS de origen.
- DATAGRAM: Campo de nombre NetBIOS de destino.
- NAME_QUERY: Campo de nombre NetBIOS de destino.

Introducir la siguiente información con este comando:

- *Inclusive* (se hace bridge) o *Exclusive* (se descarta).
- *Hostname* es una cadena ASCII de hasta 16 caracteres. Puede contener cualquier carácter excepto los siguientes:**. / \ [ ] : | < > + = ; ,** espacio. Utilizar ? para indicar un único carácter comodín. Utilizar * como carácter final del nombre para indicar un comodín para el resto del nombre. Si el nombre contiene menos de 15 caracteres, se rellena hasta el carácter 15º con espacios ASCII.
- *Special 16th character* puede usarse si el host name contiene menos de 16 caracteres. Es un números hexadecimal (sin 0x en el frente) que indica el valor para el último carácter. Si no se especifica un caracter décimo sexto en un nombre de menos de dieciseis caracteres, el router utiliza un comodín ? para el carácter décimo sexto.

Ejemplo:

```
NETBIOS Name boston config> ADD INCLUSIVE ASCII
Hostname[]? qwerty
Special 16th character in ASCII hex (<CR> for no special character)[]?
NETBIOS Name boston config>
```

add *inclusive* or *exclusive* HEX hexstring

Añade un elemento de filtro al filtro de nombre. Este comando es funcionalmente el mismo que **ADD INCLUSIVE ASCII**. De cualquier modo, se introduce el nombre como una serie de números hexadecimales (sin 0x en el frente).

Hex String debe constar de un número par de números hexadecimales. Se especifica un comodín para un único byte con ??. Si no se proporcionan 32 números hexadecimales completos, el router rellena los huecos ASCII en los números 29º y 30º y proporciona un comodín como los números 31º y 32º (16º byte).

Ejemplo:

```
NETBIOS Name boston config> ADD EXCLUSIVE HEX
Hex String[]? abc123987fed
NETBIOS Name boston config>
```

default *inclusive* or *exclusive*

Cambia el valor por defecto establecido de la lista de filtro por *Inclusive* o *Exclusive*. Si ningún elemento del filtro coincide con el paquete que el router considera para el filtrado, el router envía o descarta el paquete, dependiendo de lo establecido.

Sintaxis:

```
NETBIOS Name filter-list config> DEFAULT ?
INCLUSIVE
EXCLUSIVE
```

Ejemplo:

```
NETBIOS Name filter-list config> DEFAULT INCLUSIVE
NETBIOS Name filter-list config>
```

delete *filter-item*

Borra un elemento de filtro de la lista. Para ver una lista de los números de elemento, hay que introducir el comando **LIST**.

Sintaxis:

```
NETBIOS Name filter-list config> DELETE <nº filtro>
```

Ejemplo:

```
NETBIOS Name filter-list config> DELETE
Filter Item Number [1] ? 4
NETBIOS Name filter-list config>
```

exit

Vuelve al nivel de prompt anterior.

Sintaxis:

```
NETBIOS Name filter-list config> EXIT
```

Ejemplo:

```
NETBIOS Name filter-list config> EXIT
NETBIOS Filter config>
```

list

Visualiza la información relacionada con los elementos de la lista de filtro especificada.

Sintaxis:

```
NETBIOS Name filter-list config> LIST
```

Ejemplo:

```
NETBIOS Name boston config> LIST

NAME Filter List Name: boston
NAME Filter List Default: Inclusive

 Item #   Type    Inc/Ex    Hostname         Last Char

   1      ASCII    Inc      westboro
   2      ASCII    Inc      seattle
   3      HEX      Ex       abc123987fed

NETBIOS Name boston config>
```

move *filter-item 1 filter-item 2*

Reordena los elementos del filtro dentro de la lista de filtro. Para ver una lista de los números de elemento, hay que introducir el comando **LIST**.

Sintaxis:

```
NETBIOS Name filter-list config> MOVE <nº origen, nº final>
```

Ejemplo:

```
NETBIOS Name boston config> MOVE
Source Filter Item Number[1]? 1
After Destination Filter Item Number[0]? 3
NETBIOS Name boston config>
```

Capítulo 12
Utilización del Filtrado MAC

1. Relativo al Filtrado MAC

El filtrado MAC permite establecer filtros de paquete. Los filtros son grupos de normas aplicadas a un paquete para determinar cómo se maneja.

> ***Nota: El filtrado MAC está permitido en el tráfico de túnel.***

Durante el proceso de filtrado, los paquetes son procesados, o filtrados o etiquetados.

- *Procesados*- Se permite pasar a los paquetes a través del bridge sin resultar afectados.
- *Filtrados* - No se permite pasar a los paquetes a través del bridge.
- *Etiquetados* - Se permite pasar a los paquetes a través del bridge, pero se marcan con un número comprendido en el rango de 1 a 64 basándose en un parámetro configurable.

Un filtro MAC está formado por tres objetos:

- *Elemento de filtro* – Una única norma para el campo de dirección de un paquete. El resultado es o TRUE (coincide) o FALSE (no coincide).
- *Lista de filtro* – Contiene una lista de uno o más elementos de filtro.
- *Filtro* – Contiene un conjunto de listas de filtro.

1.1. Filtrado MAC y Tráfico DLSw

Se puede establecer el filtrado MAC para encaminar tráfico elegible DLSw a rutas de bridge alternas en una base de equipo MAC.

Para establecer un filtro para LLC, utilícese el *Bridge Net* como el número de interfaz para el filtro. Calcúlese el número de Bridge Net añadiendo dos al número de interfaces configuradas por su router. Introducir el comando **LIST DEVICES** en el prompt `Config>` o introducir el comando **CONFIGURATION** en el prompt + para ver una lista de las interfaces.

Cuando se establece un filtro para el Bridge Net, por ejemplo, el router no tira las tramas que coinciden con filtros *Exclusive*. En cambio, envía esas tramas al bridge.

2. Utilización de los Parámetros de filtrado MAC

Se pueden especificar algunos o todos los siguientes parámetros cuando se crea un filtro.

- Dirección MAC de origen o dirección MAC de destino
- Máscara que va a ser aplicada a los campos de los paquetes que van a filtrarse
- Número de interfaz
- Denominación de entrada/salida
- Denominación incluir/excluir/etiquetar
- Valor de la etiqueta (si se designa una etiqueta)

2.1. Parámetros de Elemento de filtro

Se especifican los siguientes parámetros para construir un elemento de filtro.

- Tipo de Dirección: *origen o destino*
- Etiqueta: *Valor de etiqueta*
- Máscara de dirección: *Máscara hexadecimal*

Cada elemento de filtro especifica un tipo de dirección (origen o destino) para comparar el tipo del paquete con las señales.

La *máscara de dirección* es una dirección MAC en hexadecimal que compara las direcciones de paquetes. La máscara se aplica a la dirección de origen/destino MAC antes de compararla con la dirección MAC especificada.

La máscara especifica los bytes que se van a utilizar en la operación lógica AND con los bytes de la dirección MAC. Tiene que ser de igual longitud que la dirección MAC especificada. Si no se especifica una máscara, se supone que son todos 1.

2.2. Parámetros de Lista de Filtro

Los siguientes parámetros se utilizan para construir una lista de filtro:

- Nombre: *Cadena ASCII*
- Lista de elemento de filtro: *elemento de filtro 1, …, elemento de filtro n*
- Acción: INCLUDE, EXCLUDE, TAG (n)

Una lista de filtro se construye desde uno o más elementos de filtro. A cada lista de filtro se le da un nombre único.

La aplicación de una lista de filtro a un paquete consiste en comparar cada elemento del filtro en el orden en que el elemento del filtro se añadió a la lista. Si cualquiera de los elementos de filtro de la lista vuelve con el valor lógico TRUE entonces la lista de filtro vuelve su acción designada.

2.3 Parámetros de Filtro

Los siguientes parámetros se utilizan para construir un filtro:

- Nombres de lista de filtro: *Cadena ASCII, …,cadena ASCII*
- Números de interfaz: Número *IFC*
- Dirección de Puerto: *entrada* o *salida*
- Acción por defecto: *incluir*, *excluir*, o *etiquetar*
- Etiqueta por defecto: *valor de etiqueta*

Un *filtro* se construye mediante la asociación de un grupo de nombres de filtro con un número de interfaz y la asignación de una denominación de entrada o salida. La aplicación de un filtro a un paquete significa que cada uno de las listas de filtro asociadas deben aplicarse a paquetes que se están recibiendo (entrada) o enviando (salida) en la interfaz especificada.

Cuando un filtro evalúa un paquete con condición *incluir*, el paquete se envía. Cuando un filtro evalúa un paquete con condición *excluir*, el paquete se descarta. Cuando un filtro evalúa una condición *etiquetar*, el paquete que está siendo considerado se envía con una etiqueta.

Un parámetro adicional de cada filtro es la acción por defecto que es el resultado que no haya ninguna coincidencia para todos de sus listas de filtro. Esta acción por defecto es incluir. Puede establecerse como incluir, excluir o etiquetar. Además, si la acción por defecto es etiquetar, también se da un valor de etiqueta.

3. Utilización de las Etiquetas de Filtrado MAC

- El filtrado de direcciones MAC se maneja mediante un esfuerzo común entre la reserva del ancho de banda y la característica de filtrado MAC (MCF) utilizando *etiquetas*. Un usuario con reserva de ancho de banda es capaz de categorizar tráfico de bridge, por ejemplo, asignándole una etiqueta.
- La etiquetación se hace mediante la creación de un elemento de filtro en el prompt de configuración de filtrado MAC y asignándole una etiqueta. Esta etiqueta se usa para establecer una clase de ancho de banda para todos los paquetes asociados a esa etiqueta. Los valores de deben estar en una escala de 1 a 64.

  Soporta la aplicación de etiquetas sólo a paquetes de bridge y permite sólo usar los campos de dirección MAC de los paquetes en la aplicación de la etiqueta.
- Se pueden enviar hasta cinco direcciones MAC etiquetadas, desde 1 a 5. La ETIQUETA1 se busca primero, luego la ETIQUETA2 y así.
- Una vez que un filtro etiquetado se crea, se le asigna una clase y prioridad en el proceso de configuración de la Reserva de Ancho de Banda. Utilícese **TAG** en la Reserva de Ancho de Banda para referirse a la etiqueta.

Las etiquetas pueden también referirse a grupos como en el Túnel IP. Los puntos extremos del túnel pertenecen a cualquier número de grupos, y después los paquetes se asignan a un grupo en particular a través de la característica de etiquetación del filtrado de direcciones MAC.

Capítulo 13
Configuración y Monitorización del Filtrado MAC

1. Acceso a los Prompts de Filtrado MAC

Para visualizar el prompt de configuración de filtrado MAC hay que introducir en el prompt `Config>` el comando **FEATURE MAC-FILTERING**. Por ejemplo:

```
Config> FEATURE MAC-FILTERING

-- MAC Filtering user configuration --
Filter Config>
```

Para visualizar el prompt de monitorización de filtrado MAC hay que introducir en el prompt + el comando **FEATURE MAC-FILTERING**. Por ejemplo:

```
+ FEATURE MAC-FILTERING

-- MAC Filtering user console --
Filter>
```

2. Comandos de Configuración de Filtrado MAC

Este apartado describe los comandos de configuración del filtrado MAC. Introducir los comandos de configuración en el prompt `Filter config>`. La Tabla 13.1 hace una lista de los comandos de configuración de filtrado MAC.

Tabla 13.1 Comandos de Filtrado MAC.

Comando	Función
? (AYUDA)	Visualiza los comandos u opciones disponibles.
ATTACH	Añade una lista de filtro a un filtro.
CREATE	Crea una lista de filtro o un filtro de *entrada* o de *salida*.
DEFAULT	Establece la acción por defecto para el filtro con un *número de filtro* específico a *excluir*, *incluir* o *etiquetar*.
DELETE	Elimina toda la información asociada con una lista de filtro y libera una cadena asignada como un nombre para una lista de filtro nueva. También borra un filtro creado.
DETACH	Borra un nombre de lista de filtro de un filtro.
DISABLE	Desactiva el filtrado MAC globalmente o en base a cada filtro.
ENABLE	Activa el filtrado MAC globalmente o en base a cada filtro.
LIST	Hace una lista resumen de las estadísticas y de lo establecido para cada filtro que actualmente se está ejecutando.
MOVE	Reordena las listas de filtro ligadas a un filtro específico.
REINIT	Reinicializa el sistema completo de filtrado MAC sin afectar al resto del router.
SET-CACHE	Cambia el tamaño de la cache para un filtro.
UPDATE	Añade o borra información de la lista de filtro. Ofrece un menú de subcomandos apropiados.
EXIT	Sale del proceso de configuración o monitorización de filtrado MAC.

2.1. ? (AYUDA)

Visualiza una lista de los comandos u opciones disponibles.

Sintaxis:

```
Filter Config> ?
```

Ejemplo:

```
Filter Config> ?
ATTACH
CREATE
DEFAULT
DELETE
DETACH
DISABLE
ENABLE
LIST
MOVE
REINIT
SET-CACHE
UPDATE
EXIT
```

2.2. ATTACH

Añade una lista de filtro a un filtro. Un filtro se construye mediante la asociación de un grupo de listas de filtro con un número de interfaz. Una lista de filtro se construye desde uno o más elementos de filtro.

Sintaxis:

```
Filter Config> ATTACH <filter-list-name, filter-number>
```

Ejemplo:

```
Filter Config> ATTACH
Enter a filter-list name[]? paris
Enter a filter number[1]?
Filter Config>
```

2.3. CREATE

Crea una lista de filtro o un filtro de entrada o de salida.

Sintaxis:

```
Filter Config> CREATE ?
LIST
FILTER
```

a) CREATE LIST

Crea una lista de filtro. Nombra una lista con una única cadena (*Filter-list name*) de hasta 16 caracteres. Este nombre se usa para identificar una lista de filtro que está siendo construida. Este nombre también se utiliza con otros comandos relacionados con la lista de filtro.

Ejemplo:

```
Filter Config> CREATE LIST
Enter a filter-list name[]? probe-list
Filter Config>
```

b) CREATE FILTER

Crea un filtro y lo pone en la red relacionada con la dirección de *entrada* o de *salida* en la interfaz dada por un número de interfaz. Por defecto este filtro se crea con listas de filtro no añadidas y tiene una acción predeterminada de *incluir* y *activada*.

Ejemplo:

```
Filter Config> CREATE FILTER
Enter a direction to filter (INPUT or OUTPUT)[INPUT]?
Enter an interface to filter[0]? 2
Filter Config>
```

2.4. DEFAULT

Establece la acción por defecto para el filtro con un *número de filtro* específico para *excluir*, *incluir* o *etiquetar*.

Sintaxis:

```
Filter Config> DEFAULT ?
EXCLUDE
INCLUDE
TAG
```

a) DEFAULT EXCLUDE

Establece la acción por defecto para el filtro con un *número de filtro* específico para *excluir*.

Ejemplo:

```
Filter Config> DEFAULT EXCLUDE
Enter a filter number[1]? 2
Filter Config>
```

b) DEFAULT INCLUDE

Establece la acción por defecto para el filtro con un *número de filtro* específico para *incluir*.

Ejemplo:

```
Filter Config> DEFAULT INCLUDE
Enter a filter number[1]? 3
Filter Config>
```

c) DEFAULT TAG

Establece la acción por defecto para el filtro con un *número de filtro* específico para *etiquetar* y establece el valor de etiqueta relacionado con el *número de etiqueta*.

Ejemplo:

```
Filter Config> DEFAULT TAG
Enter a tag value[1]? 2
Enter a filter number[1]? 1
Filter Config> CONFIG>
```

2.5. DELETE

Borra toda la información relacionada con la lista de filtro y libera una cadena asignada como nombre de una nueva lista de filtro. Si la lista de filtro está añadida a un filtro que ya ha sido creado, este comando visualiza un mensaje de error sin borrar nada, Además, todos los elementos de filtro pertenecientes a esta lista también se borran.

Este comando también borra un filtro creado con el comando **CREATE FILTER**.

Sintaxis:

```
Filter Config> DELETE ?
LIST
FILTER
```

a) DELETE LIST

Borra toda la información relacionada con una lista de filtro y libera una cadena asignada como nombre para una nueva lista de filtro. La lista de filtro debe ser una cadena introducida por un comando anterior **CREATE LIST**.

Si la lista de filtro está añadida a un filtro que ya ha sido creado, este comando visualiza un mensaje de error sin borrar nada. Todos los elementos de filtro que pertenecen a esta lista también se borran cuando se usa este comando.

Ejemplo:

```
Filter Config> DELETE LIST
Enter a filter-list name[]? probe-list
Filter Config>
```

b) DELETE FILTER

Borra un filtro creado con el comando **CREATE FILTER**.

Ejemplo:

```
Filter Config> DELETE FILTER
Enter a filter number[1]? 1
Filter Config>
```

2.6. DETACH

Borra un nombre de lista de filtro (parámetro *filter-list name*) de un filtro (parámetro *filter-number*).

Sintaxis:

```
Filter Config> DETACH <filter-list-name, filter-number>
```

Ejemplo:

```
Filter Config> DETACH
Enter a filter-list name[]? paris
Enter a filter number[1]? 2
Filter Config>
```

2.7. DISABLE

Desactiva el filtrado MAC por completo o desactiva un filtro en particular.

Sintaxis:

```
Filter Config> DISABLE ?
ALL
FILTER
```

a) DISABLE ALL

Desactiva el filtrado MAC por completo. De cualquier modo, los filtros todavía están establecidos como *enabled* si previamente fueron activados.

Ejemplo:

```
Filter Config> DISABLE ALL
Filter Config>
```

b) DISABLE FILTER

Desactiva un filtro en particular. El parámetro *filter number* corresponde a los números visualizados con el comando **LIST FILTERS**.

Ejemplo:

```
Filter Config> DISABLE FILTER
Enter a filter number[1]? 2
Filter Config>
```

2.8. ENABLE

Activa el filtrado MAC por completo o activa un filtro en particular.

Sintaxis:

```
Filter Config> ENABLE ?
ALL
FILTER
```

a) ENABLE ALL

Activa el filtrado MAC por completo aunque los propios filtros pueden seguir establecidos como desactivados.

Ejemplo:

```
Filter Config> ENABLE ALL
Filter Config>
```

b) ENABLE FILTER

Activa un filtro en particular. El parámetro *filter number* corresponde a los números visualizados con el comando **LIST FILTERS**.

Ejemplo:

```
Filter> ENABLE FILTER
Enter a filter number[1]? 1
Filter>
```

2.9. LIST

Sintaxis:

```
Filter Config> LIST ?
ALL
FILTER
```

a) LIST ALL

Hace una lista de todas las listas de filtro y filtros que han sido configuradas. No se proporciona una lista de todas las listas de filtro añadidas a un filtro. La demás información visualizada incluye:

- Si el filtrado está activada o desactivada.
- Una lista con el estado del sistema de filtrado (activar, desactivar).
- El conjunto de registros de la lista de filtro configurada.
- Cada uno de los registros del filtro configurado.

Además, se visualiza la siguiente información para cada filtro:

- Número de filtro.
- Número de interfaz.
- Dirección de filtro (input, output).
- Estado del filtro (enabled, disabled).
- Acción por defecto del filtro (tag, include, exclude).

Ejemplo:

```
Filter Config> LIST ALL
Filtering: enabled
Filter List                    Action
-----------                    ------
paris                          INCLUDE

Filters
-------
Id   Default  State         Ifc  Dir       Cache
--   -------  -----         ---  ---       ------
1    INCLUDE  enabled       2    INPUT     16
2    INCLUDE  disabled      1    OUTPUT    16
3    INCLUDE  enabled       0    INPUT     16
Filter Config>
```

b) LIST FILTER

Genera una lista de las listas de filtro ligadas a un filtro específico y toda la información subsiguiente del filtro.

Ejemplo:

```
Filter Config> LIST FILTER
Enter a filter number[1]?
Id   Default  State         Ifc  Dir       Cache
--   -------  -----         ---  ---       ------
1    INCLUDE  enabled       2    INPUT     16

Filter List                  Action
-----------                  ------
paris                        INCLUDE
Filter Config>
```

2.10. MOVE

Utilizar el comando **MOVE** para reordenar las listas de filtro añadidos a un filtro específico (dado por el parámetro *filter-number*). La lista dada por *Filter-list-name1* se coloca inmediatamente antes que la lista dada por *Filter-list-name2*.

Sintaxis:

```
Filter Config> MOVE <filter-list-name1, filter-list-name2, filter-number>
```

Ejemplo:

```
Filter Config> MOVE
Enter a filter-list name from[]? paris
Enter a filter-list name to[]? rome
Enter a filter number[1]? 1
Filter Config>
```

2.11. REINIT

Reinicializa el sistema completo de filtrado MAC desde una configuración existente sin afectar al resto del encaminador.

Sintaxis:

```
Filter Config> REINIT
```

Ejemplo:

```
Filter Config> REINIT
Reinitialize MAC Filtering? (Yes/No)? y
Filter Config>
```

2.12. SET-CACHE

Cambia el tamaño de la cache a un valor comprendido entre 4 y 32768. El valor por defecto es 16.

Sintaxis:

```
Filter Config> SET-CACHE <filter-number, cache-size>
```

Ejemplo:

```
Filter Config> SET-CACHE
Enter a filter number[1]?
Enter the new cache size[16]? 32
Filter Config>
```

2.13. UPDATE

Utilizar el comando **UPDATE** para añadir información o borrar información de una lista de filtro específica. Utilizando este comando con el parámetro *filter-list-name* deseado lleva al prompt requerido `Filter filter-list-name Config>` para esa lista de filtro. Desde este nuevo prompt se puede cambiar información de la lista.

El orden en que se especifican los elementos de filtro para una lista de filtro es importante ya que determina el orden en que éstos se aplican al paquete.

Sintaxis:

```
Filter Config> UPDATE <filter-list-name>
```

Ejemplo:

```
Filter Config> UPDATE PROBE
Filter 'probe' Config>
```

2.14. EXIT

Utilizar el comando **EXIT** para volver al prompt `Config>`.

Sintaxis:

```
Filter Config> EXIT
```

Ejemplo:

```
Filter Config> EXIT
Config>
```

3. Comandos de Monitorización de Filtrado MAC

Esta sección describe los comandos de monitorización del filtrado MAC. Introducir los comandos de monitorización en el prompt `Filter>`. La Tabla 13.2 muestra una lista de los comandos de monitorización de filtrado MAC.

Tabla 13.2. Comandos de Monitorización de Filtrado MAC

Comando	Función
? (AYUDA)	Visualiza los comandos u opciones disponibles.
CLEAR	Borra las estadísticas por filtro de las que se ha hecho una lista en el comando **LIST FILTER**.
DISABLE	Desactiva el filtrado MAC globalmente o en base a cada filtro.
ENABLE	Activa el filtrado MAC globalmente o en base a cada filtro.
LIST	Hace una lista resumen de las estadísticas y de lo establecido para cada filtro que actualmente se está ejecutando.
REINIT	Reinicializa el sistema completo de filtrado MAC sin afectar al resto del router.
EXIT	Sale al proceso de configuración o monitorización de filtrado MAC.

3.1. ? (AYUDA)

Visualiza una lista de los comandos u opciones disponibles.

Sintaxis:

```
Filter> ?
```

Ejemplo:

```
Filter> ?
CLEAR
DISABLE
ENABLE
LIST
REINIT
EXIT
```

3.2. CLEAR

Borra todas las estadísticas por filtro que aparecen en el comando **LIST FILTER** para todos los objetos del filtro y todas las estadísticas que aparecen para cada lista de filtro.

El comando también borra las estadísticas por filtro que aparecen en el comando **LIST FILTER** para el filtro asociado con el *filter number* más todas las estadísticas de las que se ha hecho una lista para cada lista de filtro en este filtro.

Sintaxis:

```
Filter> CLEAR ?
ALL
FILTER
```

a) CLEAR ALL

Borra todas las estadísticas que aparecen en el comando **LIST FILTER** para cada objeto de filtro y cada lista de filtro.

Ejemplo:

```
Filter> CLEAR ALL
Filter>
```

b) CLEAR FILTER

Borra las estadísticas por filtro que aparecen en el comando **LIST FILTER** para el filtro asociado con el *filter number* más todas las estadísticas de las que se ha hecho una listan para cada lista de filtro en este filtro.

Ejemplo:

```
Filter> CLEAR FILTER
Enter a filter number[1]?
Filter>
```

3.3. DISABLE

Desactiva el filtrado MAC por completo o desactiva un filtro en particular.

Sintaxis:

```
Filter> DISABLE ?
ALL
FILTER
```

a) DISABLE ALL

Desactiva el filtrado MAC por completo. De cualquier modo, los filtros todavía están establecidos como *enabled* si previamente fueron activados.

Ejemplo:

```
Filter Config> DISABLE ALL
Filter Config>
```

b) DISABLE FILTER

Desactiva un filtro en particular. El parámetro *filter number* corresponde a los números visualizados con el comando **LIST FILTERS**.

Ejemplo:

```
Filter Config> DISABLE FILTER
Enter a filter number[1]? 2
Filter Config>
```

3.4. ENABLE

Activa el filtrado MAC por completo o activa un filtro en particular.

Sintaxis:

```
Filter> ENABLE ?
ALL
FILTER
```

a) ENABLE ALL

Activa el filtrado MAC por completo aunque los propios filtros pueden seguir establecidos como desactivados.

Ejemplo:

```
Filter Config> ENABLE ALL
Filter Config>
```

b) ENABLE FILTER

Activa un filtro en particular. El parámetro *filter number* corresponde a los números visualizados con el comando **LIST FILTERS**.

Ejemplo:

```
Filter> ENABLE FILTER
Enter a filter number[1]? 1
Filter>
```

3.5. LIST

Sintaxis:

```
Filter> LIST ?
ALL
FILTER
```

a) LIST ALL

Hace una lista de todas las listas de filtro y filtros que han sido configuradas. No se proporciona una lista de todas las listas de filtro añadidas a un filtro. El resto de la información visualizada incluye:

- Si el filtrado está activado o desactivado.
- Una lista con el estado del sistema de filtrado (enable, disable)
- El conjunto de registros de la lista de filtro configurada.
- Cada uno de los registros del filtro configurado.

Además, se visualiza la siguiente información para cada filtro:

- Número de filtro
- Número de interfaz
- Dirección de filtro (input, output)
- Estado del filtro (enable, disable)
- Acción por defecto del filtro (tag, include, exclude)

Ejemplo:

```
Filter> LIST ALL
Filtering: enabled
Filter List                    Action
-----------                    ------
paris                          INCLUDE

Filters
-------
Id   Default  State         Ifc  Dir       Cache
--   -------  -----         ---  ---       ------
1    INCLUDE  enabled       2    INPUT     16
2    INCLUDE  disabled      1    OUTPUT    16
3    INCLUDE  enabled       0    INPUT     16
Filter>
```

b) LIST FILTER

Genera una lista de las listas de filtro añadidas a un filtro específico y toda la información subsiguiente del filtro.

Ejemplo:

```
Filter> LIST FILTER
Enter a filter number[1]?
Id   Default  State         Ifc  Dir       Cache
--   -------  -----         ---  ---       ------
1    INCLUDE  enabled       2    INPUT     16

Filter List                  Action
-----------                  ------
paris                        INCLUDE
Filter>
```

3.6. REINIT

Reinicializa el sistema completo de filtrado MAC desde una configuración existente sin afectar al resto del router.

Sintaxis:

```
Filter> REINIT
```

Ejemplo:

```
Filter> REINIT
Reinitialize MAC Filtering? (Yes/No)? y
Filter Config>
```

3.7. EXIT

Utilizar el comando **EXIT** para volver al prompt +.

Sintaxis:

```
Filter> EXIT
```

Ejemplo:

```
Filter> EXIT
+
```

4. Comandos de Actualización del Filtrado MAC

La Tabla 13.3 hace una lista de los comandos de actualización del filtrado MAC. Introducir estos comandos en el prompt `Filter 'filter-list-name' Config>.`

Tabla 13.3 Comandos de Actualización del Filtrado MAC

Comando	Función
? (AYUDA)	Visualiza los comandos u opciones disponibles.
ADD	Añade un número hexadecimal para comparar con la dirección MAC de origen o destino. Añade elementos de filtro a una lista de filtro. Añade una lista de filtro a un filtro.
DELETE	Borra elementos de filtro de una lista de filtro.
LIST	Hace una lista resumen de todas las listas de filtro y filtros configurados por el usuario. También genera una lista de las listas de filtro añadidas a este filtro y toda la subsiguiente información del filtro.
MOVE	Reordena las listas de filtro relacionadas con un filtro específico.
SET-ACTION	Establece un elemento de filtro para evaluar si es *include*, *exclude* o *tag* (con una opción *tag-number*).
EXIT	Sale del proceso de configuración de actualización del subcomando.

4.1. ? AYUDA

Visualiza una lista de los comandos u opciones disponibles.

Sintaxis:

```
Filter 'filter-list-name' Config> ?
```

Ejemplo:

```
Filter 'probe' Config> ?
ADD
DELETE
LIST
MOVE
SET-ACTION
EXIT
Filter 'probe' Config>
```

4.2. ADD

Añade elementos de filtro a una lista de filtro. Este comando específicamente permite añadir un número hexadecimal para comparar con la dirección MAC de origen o destino.

El orden en que se añaden los elementos de filtro a la lista de filtro es importante ya que determina el orden en que los elementos de filtro se aplican a un paquete.

Cada utilización del subcomando **ADD** crea un elemento de filtro dentro de la lista de filtro. El primer elemento de filtro se designa como *filter-item-number* 1, el siguiente como *number 2*, y así sucesivamente. Después de un **ADD**, el router visualiza el número del elemento de filtro que se acaba de añadir.

La primera coincidencia que se produzca detiene la aplicación de los elementos de filtro, y la lista de filtro evalúa si *include*, *exclude* o *tag*, dependiendo de la acción designada de la lista de filtro. Si ninguno de los elementos de filtro de una lista de filtro produce una coincidencia, se devuelve la acción por defcto (*include*, *exclude* o *tag*) o el filtro.

Sintaxis:

```
Filter 'filter-list-name' Config> ADD ?
SOURCE
DESTINATION
```

a) ADD SOURCE

Añade un número hexadecimal (sin 0x en el frente, un máximo de 16 numeros, y un número par de números hexadecimales) para comparar con la dirección MAC de origen.

El parámetro *hex-mask* debe ser de la misma longitud que *hex-MAC-address* y se efectua una operación AND lógica con la dirección MAC designada en el paquete. El argumento predeterminado *hex-mask* es de todo 1s binarios.

Se puede introducir el *hex-MAC-addr* en forma canónica o no canónica. La forma canónica es simplemente un número hexadecimal (por ejemplo, 000003001234) o una serie de dígitos hexadecimales con un guión entre cada dos dígitos (por ejemplo, 00-00-03-00-12-34).

La forma no canónica es una serie de dígitos hexadecimales con dos puntos entre cada dos dígitos (por ejemplo, 00:00:C9:09:66:49). Las direcciones MAC de elementos de filtro siempre se visualizan utilizando un guión o dos puntos para distinguir las representaciones canónicas de las no canónicas.

Ejemplo:

```
Filter 'paris' Config> ADD SOURCE
Enter MAC Address[]? 00-11-22-33-44-55
Enter MAC Mask[ffffffffffff]?
Filter 'paris' Config>
```

b) ADD DESTINATION

Actúa exactamente como **ADD SOURCE**, con la excepción de que la coincidencia se busca con la dirección de destino en lugar de con la dirección MAC de origen del paquete.

Ejemplo:

```
Filter 'sample' Config> ADD DESTINATION
Enter MAC Address[]? 00-00-a0-bb-0f-13
Enter MAC Mask[ffffffffffff]?
Filter 'sample' Config>
```

4.3. DELETE

Borra elementos de filtro de una lista de filtro. Se borran elementos de filtro especificando el número de elemento de filtro asignado al elemento cuando se añadió.

Cuando se borra un elemento de filtro, cualquier hueco creado en la secuencia numérica se llena. Por ejemplo, si los elementos de filtro 1, 2, 3 y 4 existen y se borra el elemento de filtro 3, el elemento de filtro 4 se vuelve a numerar como 3.

Sintaxis:

```
Filter 'filter-list-name' Config> DELETE <filter-item-number>
```

Ejemplo:

```
Filter 'sample' Config> DELETE 2
Filter 'sample' Config>
```

4.4. LIST

Hace una lista de todos los registros de elemento de filtro representados en forma canónica y no canónica. Visualiza la siguiente información sobre cada elemento de filtro.

- Dirección MAC y máscara de dirección en forma canónica y no canónica
- Números de elementos de filtro
- Tipo de dirección (*source* o *destination*)
- Acción de lista de filtro

Sintaxis:

```
Filter 'filter-list-name' Config> LIST ?
CANONICAL
NONCANONICAL
```

a) LIST CANONICAL

Hace una lista de todos los registros de elementos de filtro en una lista de filtro, dando los números de elementos, el tipo de dirección (SRC, DST), la dirección MAC en forma canónica, y la máscara de dirección en forma canónica. Además, da la acción de la lista de filtro.

Ejemplo:

```
Filter 'sample' Config> LIST CANONICAL
Action: INCLUDE
Id  Type  MAC Address                Mask
--  ----  -----------                ----
1   SRC   01-02-03-04-05-06          ff-ff-ff-ff-ff-ff
2   DST   00-00-11-11-22-22          ff-ff-ff-ff-ff-ff
Filter 'sample' Config>
```

b) LIST NON-CANONICAL

Hace una lista de todos los registros de elementos de filtro en una lista de filtro, dando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en forma no canónica, y la máscara de dirección en forma no canónica. Además, da la acción de lista de filtro.

Ejemplo:

```
Filter 'sample' Config> LIST NONCANONICAL
Action: INCLUDE
Id  Type  MAC Address                Mask
--  ----  -----------                ----
1   SRC   80:40:c0:20:a0:60          ff:ff:ff:ff:ff:ff
2   DST   00:00:88:88:44:44          ff:ff:ff:ff:ff:ff
Filter 'sample' Config>
```

4.5. MOVE

Reordena los elementos de filtro de una lista de filtro. El elemento de filtro cuyo número está especificado por *filter-item-name 1* se mueve y se vuelve a numerar para estar justo antes de *filter-item-name 2*.

Sintaxis:

```
Filter 'filter-list-name' Config> MOVE <filter-item-name1, filter-item-name2>
```

Ejemplo:

```
Filter 'sample' Config> MOVE
Item number to move[1]? 2
Item number before which to insert[1]?
Filter 'sample' Config>
```

4.6. SET-ACTION

Permite establecer una lista de filtro como *include*, *exclude* o *tag* (con una opción *tag-number*). Si ninguno de los elementos de filtro de la lista de filtro coincide con los contenidos del paquete que está siendo considerados para el filtrado, la lista de filtro evalúa esta condición. El valor por defecto es *include*.

Sintaxis:

```
Filter 'filter-list-name' Config> SET-ACTION ?
INCLUDE
EXCLUDE
TAG
```

a) SET-ACTION INCLUDE

Ejemplo:

```
Filter 'sample' Config> SET-ACTION INCLUDE
Filter 'sample' Config>
```

b) SET-ACTION EXCLUDE

Ejemplo:

```
Filter 'sample' Config> SET-ACTION EXCLUDE
Filter 'sample' Config>
```

c) SET-ACTION TAG

Ejemplo:

```
Filter 'sample' Config> SET-ACTION TAG
Enter a tag value[1]? 3
Filter 'sample' Config>
```

4.7. EXIT

Utilizar el comando **EXIT** para volver al prompt anterior.

Sintaxis:

```
Filter 'filter-list-name' Config> EXIT
```

Ejemplo:

```
Filter 'sample' Config> EXIT
Filter Config>
```

Capítulo 14
Utilización del Threading de Protocolo a través de una Red de Bridge

1. Relativo al Threading

El threading es el proceso mediante el cual el protocolo de red (IPX, DNA, IP, AppleTalk y Apollo) del equipo final Token Ring descubre una ruta sobre segmentos de una red SRB.

El threading no es diferente de la operación SRB. La diferencia consiste en cómo el threading es implementado por el equipo final. Las siguientes secciones describen el threading para IP, DNA, IPX, Apple Talk y Apollo.

2. Threading IP con ARP

Los equipos finales IP utilizan paquetes REQUEST y REPLY del Protocolo de Resolución de Direcciones (ARP -Address Resolution Protocol-) para descubrir un RIF. Ambos equipos finales IP y los bridges participan en el proceso de descubrimiento de ruta y proceso de encaminamiento. Los siguientes pasos describen el threading IP.

1. Un equipo final IP mantiene una tabla ARP y una tabla RIF. Utiliza la dirección MAC en la tabla ARP como una referencia cruzada para el RIF de destino en la tabla RIF. Si un RIF no existe para esa dirección MAC específica, el equipo final transmite un paquete ARP REQUEST con un ARE (All Routes Explore) o con un STE (Spanning Tree Explore) al segmento local.
2. Todos los bridges del segmento local capturan el paquete ARP REQUEST y lo envían a sus redes conectadas.
3. Mientras que el paquete ARP REQUEST continua su búsqueda del equipo final de destino, cada bridge que lo envía añade su propio número de bridge y número de segmento al RIF del paquete. Mientras que la trama continúa pasando a través de la red de bridge, el RIF actúa de acuerdo con una lista de parejas de bridges y números de segmento que describen la ruta hasta el destino.
4. Cuando el paquete ARP REQUEST finalmente alcanza su destino, contiene la secuencia exacta de bridge y números de segmento desde el origen hasta el destino.
5. Cuando el equipo final de destino recibe la trama, pone la dirección MAC y su RIF en sus propias tablas ARP y RIF. Si el equipo final de destino recibe cualquier otro paquete ARP REQUEST procedente del mismo origen, descarta ese paquete.
6. El equipo final de destino genera entonces un paquete ARP REPLY que incluye el RIF y lo envía de regreso al equipo final de origen.
7. El equipo final de origen recibe una ruta aprendida. Pone la dirección MAC y su RIF en las tablas ARP y RIF. Después el RIF se añade al paquete de datos y se envía el destino.
8. La duración de las entradas RIF la maneja el temporizador de refresco IP ARP.

3. Threading DNA

Los equipos finales Digital Network Architecture (DNA) utilizan ARE (All Routes Explore) para descubrir una ruta. Ambos equipos finales DNA y los bridges participan en el proceso de descubrimiento de rutas y encaminamiento. Los siguientes pasos describen el proceso de threading DNA.

1. Si no hay una entrada en la tabla RIF para la dirección MAC, se crea una entrada con el estado *NO_ROUTE*. Cuando esto ocurre el equipo final envía el paquete de datos con un STE añadido. El STE se utiliza para descubrir sin intentar llenar la red con ARE.
2. El equipo final transmite después una ARE en una trama sin bucles a la dirección MAC de destino.
3. Todos los bridges del segmento local capturan el STE y la trama sin bucles y lo envían a sus redes conectadas.
4. Mientras que los paquetes continúan su búsqueda del equipo final de destino, cada bridge que lo envía añade su propio número de bridge y número de segmento al RIF en el STE y al ARE. Mientras que las tramas pasan a través de la red de bridge, el RIF actúa de acuerdo con una lista de parejas de bridges y números de segmento que describe la ruta hasta el destino.
5. Cuando el STE y la trama sin bucles alcanzan finalmente el destino, contienen la secuencia exacta de bridges y números de segmento desde el origen hasta el destino.
6. Cuando el equipo final de destino recibe la trama sin bucles pone la dirección MAC y el RIF del equipo de origen en su propia tabla RIF. Si ya existe un RIF para esa entrada, bien actualiza el RIF si esa entrada previa es una *ST_ROUTE* o bien ignora el RIF. En cualquier caso el estado de entrada se cambia a *HAVE_ROUTE*.
7. El equipo final de destino envía entonces la trama de réplica sin bucles incluyendo el RIF específico de regreso al equipo final de origen.
8. El equipo final de origen recibe la ruta aprendida específica. Pone el RIF en la tabla RIF y la entrada cambia por *HAVE_ROUTE*.
9. Los paquetes destinados a una dirección funcional se envían con un STE. Los equipos finales DNA pueden crear una entrada RIF utilizando esta trama STE. Cuando esto ocurre el estado de la entrada se cambia por *ST_ROUTE*.

Los equipos finales DNA contienen un temporizador RIF independiente. Cuando este temporizador se agota para una entrada RIF específica, se envía un ARE en un paquete sin bucles a ese destino específico. Cuando regresa la trama sin bucles, se actualiza la entrada RIF. Si el equipo final de destino está en el mismo anillo y la trama sin bucles no contiene un RIF, el paquete sin bucles se devuelve sin entrada RIF.

4. Threading Apollo

Los equipos finales Apollo usan tramas STE para descubrir una ruta. Ambos equipos finales Apollo y los bridges participan en el proceso de descubrimiento de rutas y encaminamiento. Los siguientes pasos describen el proceso de threading Apollo.

1. Si no hay una entrada en la tabla RIF para la dirección MAC se envía el paquete de datos con un STE. Se añade una entrada a la tabla RIF designándola como NO_ROUTE.
2. El equipo final transmite entonces otro STE con XID para la dirección MAC de destino.
3. Todos los bridges del segmento local capturan el STE y lo envían a sus redes conectadas.
4. Mientras que los paquetes continúan su búsqueda del equipo final de destino, cada bridge que lo envía añade su propio número de bridge y número de segmento al RIF en el STE. Mientras que las tramas pasan a través de la red de bridge, el RIF actúa de acuerdo con una lista de parejas de bridges y números de segmento que describen la ruta hasta el destino.
5. Cuando el STE alcanza finalmente el destino, contiene la secuencia exacta de bridges y números de segmento desde el origen hasta el destino.
6. Cuando el equipo final de destino recibe el STE con XID, pone la dirección MAC y el RIF del equipo de origen en su propia tabla RIF. Si ya existe un RIF para esa entrada, bien actualiza el RIF si esa entrada previa es una *ST_ROUTE* o bien ignora el RIF. En cualquier caso el estado de entrada se cambia a *HAVE_ROUTE*.
7. El equipo final de destino envía entonces la trama de réplica XID incluyendo el RIF específico de regreso al equipo final de origen.
8. El equipo final de origen recibe la ruta aprendida específica. Pone el RIF en la tabla RIF y la entrada cambia a *HAVE_ROUTE*.
9. Los paquetes destinados a una dirección funcional se envían con un STE sin XID. Los equipos finales Apollo pueden crear una entrada RIF utilizando esta trama STE. Cuando esto ocurre el estado de la entrada se cambia por *ST_ROUTE*.

Los equipos finales Apollo contienen un temporizador RIF independiente. Cuando este temporizador se agota para una entrada RIF específica, se envía un STE con paquete XID a ese destino específico. Cuando regresa la trama de réplica XID, se actualiza la entrada RIF. Si el equipo final de destino está en el mismo anillo, la trama sin bucles se envía y retorna sin entrada RIF.

5. Threading IPX

Los equipos finales IPX comprueban cada paquete que reciben por un RIF. Si el RIF no existe en la tabla, añaden el RIF a la tabla y designan esa ruta como HAVE_ROUTE. Si el RIF indica que el paquete procede de un equipo final en el anillo local, se designa la ruta como ON_RING.

Si el equipo final necesita enviar un paquete y no hay entrada en la tabla RIF para la dirección MAC, el equipo final transmite los datos como un STE.

Cuando el temporizador RIF se agota, la entrada de la tabla se borra y no será reintroducida hasta que llegue otro paquete que contenga un RIF para esa entrada.

6. Threading AppleTalk 1 y 2

Los equipos finales Apple Talk usan paquetes ARP y XID para descubrir una ruta. Ambos equipos finales Apple Talk y los bridges participan en el proceso de descubrimiento de rutas y encaminamiento. Los siguientes pasos describen el proceso de threading Apple Talk.

1. Si no existe un RIF para una dirección MAC específica, el equipo final transmite un paquete ARP REQUEST con un ARE (All Route Explore) al segmento local.
2. Todos los bridges del segmento local capturan el paquete ARP REQUEST y lo envían a sus redes conectadas.
3. Mientras que el paquete ARP REQUEST continúa su búsqueda del equipo final de destino, cada bridge que lo envía añade su propio número de bridge y número de segmento al RIF en el paquete. Mientras que las tramas pasan a través de la red de bridge, el RIF actúa de acuerdo con una lista de parejas de bridges y números de segmento que describen la ruta hasta el destino.
4. Cuando el equipo final de destino recibe la trama, pone la dirección MAC y su RIF en sus propias tablas ARP y RIF y el estado de la entrada se designa como *HAVE_ROUTE*. Si el equipo final de destino recibe cualquier otro paquete ARP REQUEST del mismo origen, descarta el paquete.
5. El equipo final de destino genera entonces un paquete ARP REPLY que incluye el RIF y lo envía de regreso al equipo final de origen con el bit de dirección en el RIF revisado.
6. El equipo final de origen recibe la ruta aprendida. Entonces se introducen la dirección MAC y su RIF en las tablas ARP y RIF y el estado se designa como *HAVE_ROUTE*. Si el RIF indica que el paquete procede de un equipo final del anillo local, se designa la ruta como *ON_RING*.
7. Si se agota el temporizador RIF, se envía un XID con un RE y se cambia el estado por *DISCOVERING*. Si no se recibe una réplica XID, se descarta la entrada.