3Com® Corporation

PathBuilder™ S200 Series Switch Bridging

Notice

Restricted Rights Notification for U.S. Government Users

The software (including firmware) addressed in this manual is provided to the U.S. Government under agreement which grants the government the minimum “restricted rights” in the software, as defined in the Federal Acquisition Regulation (FAR) or the Defense Federal Acquisition Regulation Supplement (DFARS), whichever is applicable.

If the software is procured for use by the Department of Defense, the following legend applies:

Restricted Rights Legend

Use, duplication, or disclosure by the Government
is subject to restrictions as set forth in
subparagraph (c)(1)(ii) of the
Rights in Technical Data and Computer Software
clause at DFARS 252.227-7013.

If the software is procured for use by any U.S. Government entity other than the Department of Defense, the following notice applies:

Notice

Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in FAR 52.227-19(C).

Proprietary Material

Part No. T0008-16, Rev. F
First Printing October 1998

Manual is current for Release 5.2M.

Overview

Functionality

PathBuilder S200 series switches support bridging of data traffic for Ethernet LANs. Bridging LAN traffic minimizes your networking costs by eliminating the need for redundant networks and maximizes the availability of dedicated facilities such as servers and printers, as well as public Frame Relay and X.25 services, across multiple LANs.

Remote Bridging Solutions

PathBuilder S200 series switches are intended for use in remote bridging solutions. This means the PathBuilder S200 series switch is best used to connect a remote LAN to the WAN to connect to other remote LANs in your network, as shown in Figure 1.

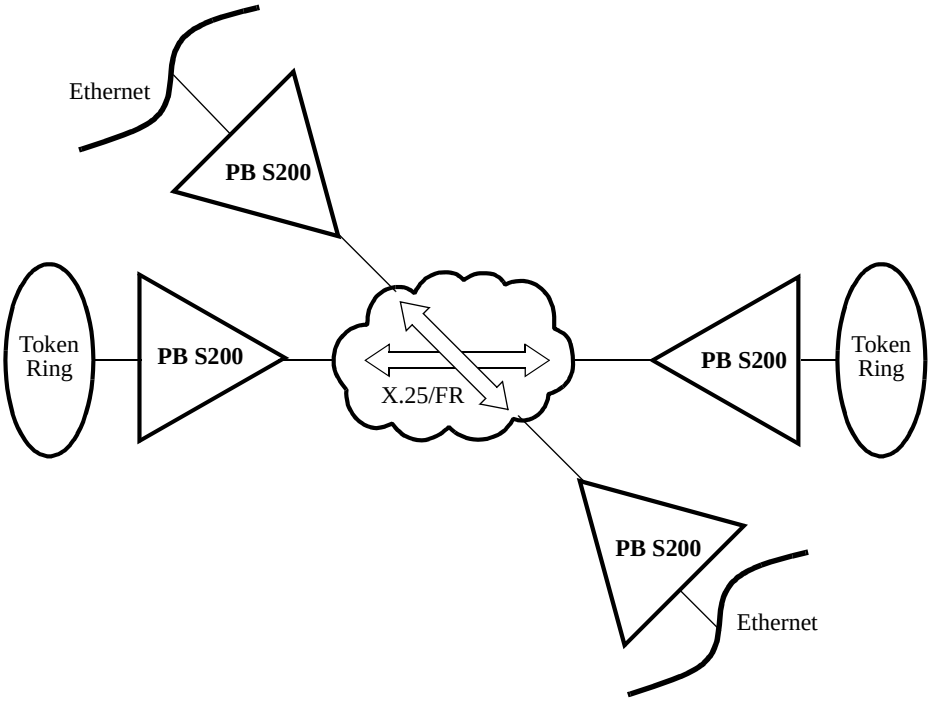


Figure 1. PathBuilder S200 Series Switch Bridge Combining Traffic from Serial Devices

Figure 1 shows PathBuilder S200 series switches acting as remote bridges to combine data traffic from Ethernet LANs to the WAN to connect to other remote LANs in the network.

Mixed LAN Support

PathBuilder S200 series switches support mixed LAN bridging, meaning you can configure an Ethernet interface in the same node. Refer to the “Mixed LAN Bridging” section on page 8 for more details.

Translational Bridging

PathBuilder S200 series switches can use the Translational Bridging feature to bridge traffic between Ethernet Networks. Translational Bridging provides a PathBuilder S200 series switch with the capability to bridge non-routable protocols. For information about enabling and configuring Translational Bridging, refer to the “Configuring Translational Bridging” section on page 37.

No Local Bridging

As mentioned earlier, PathBuilder S200 series switches are not intended for use in local bridging applications where one LAN is connected directly to another LAN. It is not recommended you use PathBuilder S200 series switches to perform local bridging.

Transparent Bridging

Transparent Bridging (TB) is the method used by PathBuilder S200 series switches to bridge Ethernet LAN traffic from one Ethernet LAN to another one across a WAN.

Refer to Transparent Bridging for Ethernet LANs on page 48 for more details on these bridging operations.

Supported Traffic

The PathBuilder S200 series switch family supports many types of protocols for bridging operations. Some of the supported protocols include:

- Async
- SDLC
- Bisync
- Transparent Polled Async
- HDLC
- X.25
- Frame Relay
- Burroughs Poll Select
- NCR Bisync

In This Manual

Topic	See Page

In This Notice
(continued)

Topic	See Page

Bridging Features and Capabilities

Introduction

This section describes bridging features and capabilities of PathBuilder S200 series switches.

Bridging Primer

As mentioned earlier, Bridging extends the size and coverage of a Local Area Network (LAN). PathBuilder S200 series switches provide bridging support for up to two 802.3 (Ethernet) LAN interfaces per node or one 802.5 (Token Ring) LAN interface) per node, and up to 32 remote bridge connections.

A PathBuilder S200 series switch bridge can be connected to a WAN backbone made up of X.25, Frame Relay, or both, as shown in Figure 2.

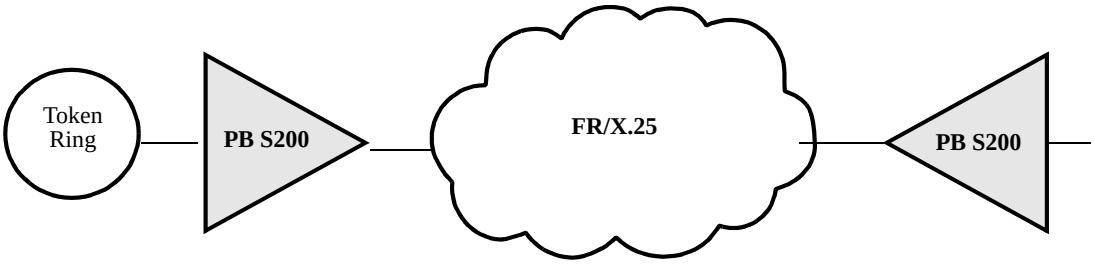


Figure 2. Example of Typical PathBuilder S200 Series Switch Bridging Application

PathBuilder S200 series switches are best suited for remote bridging operations where traffic flows from one LAN through a WAN bridged by at least two PathBuilder S200 series switches to another LAN.

Ethernet LAN

What Is It?

Ethernet is a common implementation of LAN topology wherein stations are connected using a bus topology. Stations access the Ethernet using Carrier Sense with Multiple Access and Collision Detection (CSMA/CD).

PathBuilder S200 Series Switch Support for Ethernet

PathBuilder S200 series switch Ethernet functionality complies with the IEEE 802.3 specifications and provides Transparent Bridging to transport many different protocols over the Wide Area Network (WAN) to remote destinations. Supported protocols include:

- Novell Netware
- DECnet
- Banyan Vines

Example of Basic Ethernet Frame Format

Figure 3 shows the basic frame formats for Ethernet frames supported by PathBuilder S200 series switches.

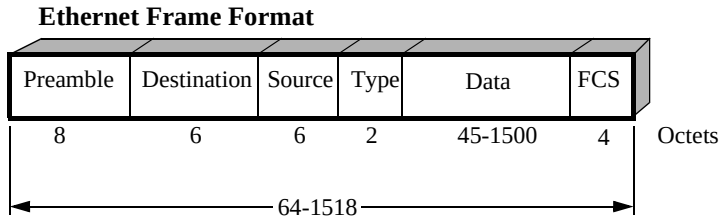


Figure 3. Frame Format for Ethernet Frames

802.3 MAC Frame Format

Figure 4 shows the supported 802.3 Ethernet MAC Frame format.

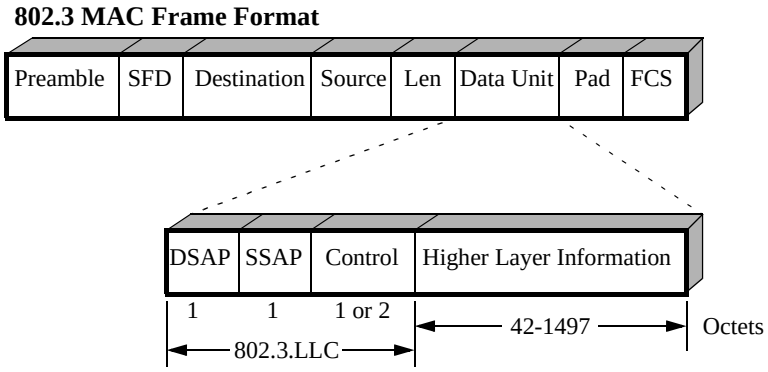


Figure 4. 802.3 Ethernet MAC Frame Format Example

Example of Ethernet Bridge Operation

Figure 5 shows an example of two Ethernet LANs connected across a WAN using two PathBuilder S200 series switches as bridges. The example shows a Frame Relay WAN application, but you can also bridge across an X.25 WAN.

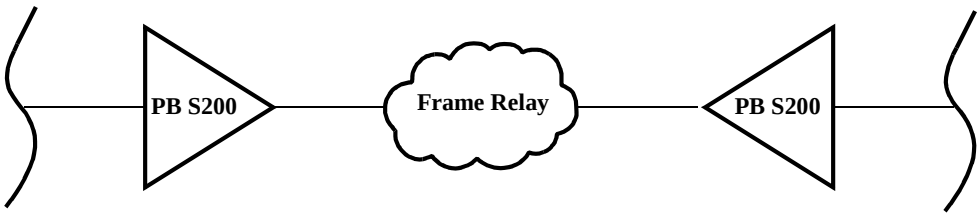


Figure 5. Ethernet Bridge Example

For More Details...

For more details on bridging Ethernet LAN traffic, see Transparent Bridging for Ethernet LANs on page 48.

Mixed LAN Bridging

What is It?

PathBuilder S24x, 26x, and 27x switches support a mixture of Token Ring and Ethernet interfaces configured in the same node. This means the PathBuilder S24x, 26x, and 27x switch is able to perform remote Transparent bridging for Ethernet LANs from the same PathBuilder S24x, 26x, and 27x switch as shown in Figure 6. If you happen to configure two Ethernet LAN interfaces in the same node, instead of a mix of one Ethernet and one Token Ring, you can perform local Transparent bridging between the two Ethernet LANs.

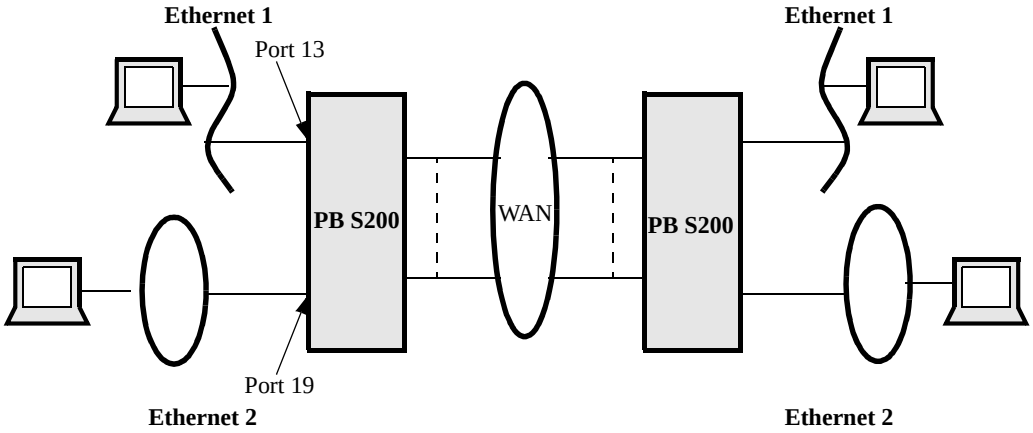


Figure 6. Example of Mixed LAN Bridging in PathBuilder S24x, 26x, and 27x Switch

Note

Mixed LAN operation does not support translational bridging, meaning you cannot pass LAN traffic from an Ethernet LAN to a Token Ring LAN without using some sort of conversion software.

For More Details

Refer to the “Mixed LAN Operation” section on page 114 for more details.

MAC Addressing

What Is It?

Bridges, whether they using Transparent Bridging, operate at the Data Link Layer, which is concerned with MAC addressing. The MAC Address is a 6-byte MAC (Media Access Control) address that identifies stations on a LAN. The IEEE administers distribution of the MAC address to ensure no duplicates occur in MAC addressing. This is accomplished by assigning a unique MAC address to each manufacturer. Each manufacturer then assigns sequential values to the lower three bytes for each interface manufactured.

For More Details

For more details on MAC Address filtering, see the section “MAC Address Filtering” section on page 58”in this manual.

LLC2 Local Termination

LLC2 Local Termination

PathBuilder S200 series switch support includes LLC2 Local Termination for your Bridging operations when passing SNA/SDLC data traffic. LLC2 Local Termination lets specific Token Ring ports generate and respond to LLC2 polls with local acknowledgments, thereby preserving bandwidth and preventing session timeouts.

Local Termination, also referred to as “spoofing,” provides an efficient means for carrying out an LLC2 session between two SNA end stations attached to separate Token Ring LANs connected by a Wide Area Network (WAN).

Additionally, Local Termination provides detailed statistics on LLC2 sessions.

LT Example

Figure 7 shows a network where running LLC2 Local Termination at the edge point PathBuilder S200 series switches enables spoofing from one side of the network to the other across multiple Token Rings.

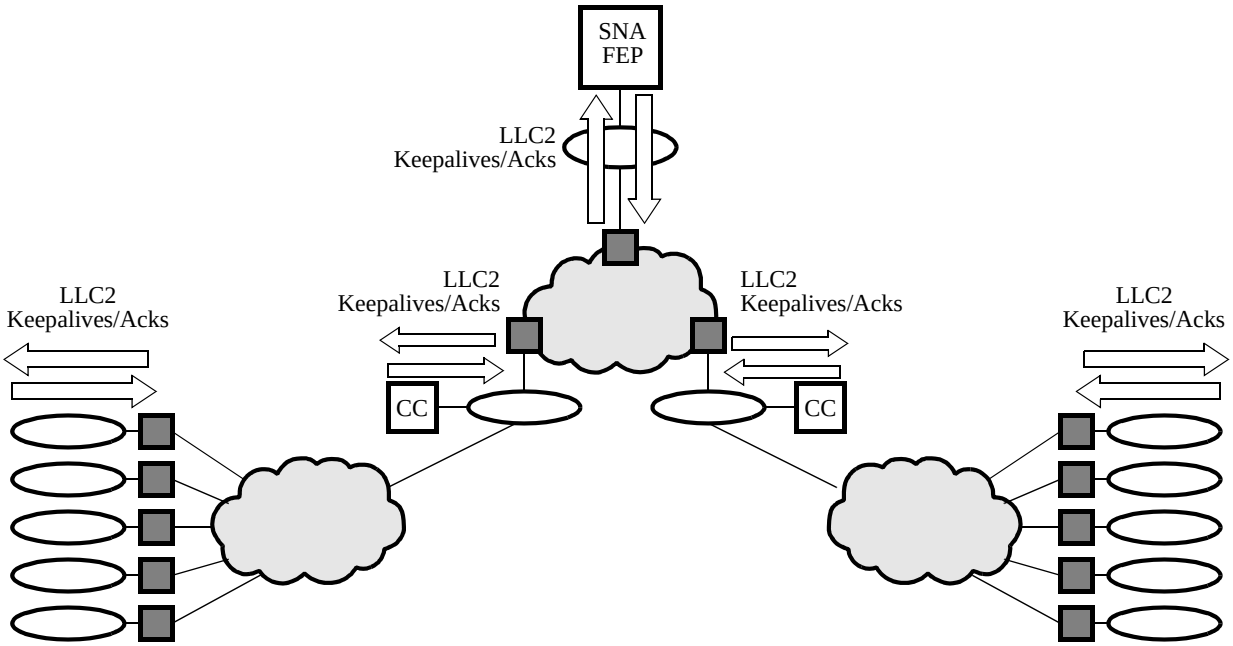


Figure 7. Local Termination Example

For More Details...

See“LLC2 Local Termination” section on page 100 in this guide.

Autolearn for Local Termination

What Is It?

Local Termination Autolearn reduces the amount of configuration you need to do by letting you spoof remote sessions without configuring a MAC address and a Service Access Point (SAP) for each station running a session to the host Front End Processor (FEP).

Since Local Termination supports up to 256 sessions for the PathBuilder S24x, 26x, and 27x switch, Local Termination Autolearn can save you considerable time during the configuration process.

Local Termination Autolearn is a default feature with PathBuilder S200 series switches operating software meaning it requires no special configuration, other than configuring the remote host MAC address in the PathBuilder S200 series switch Local Termination (LT) Station tables.

It does not interfere with previously configured Local Termination spoofing sessions.

Example

Figure 8 shows how a PathBuilder S200 series switch automatically learns the address of PCs connected to the local bridge so you can pass data traffic to the host without configuring entries in the Local Termination Station table for each PC session.

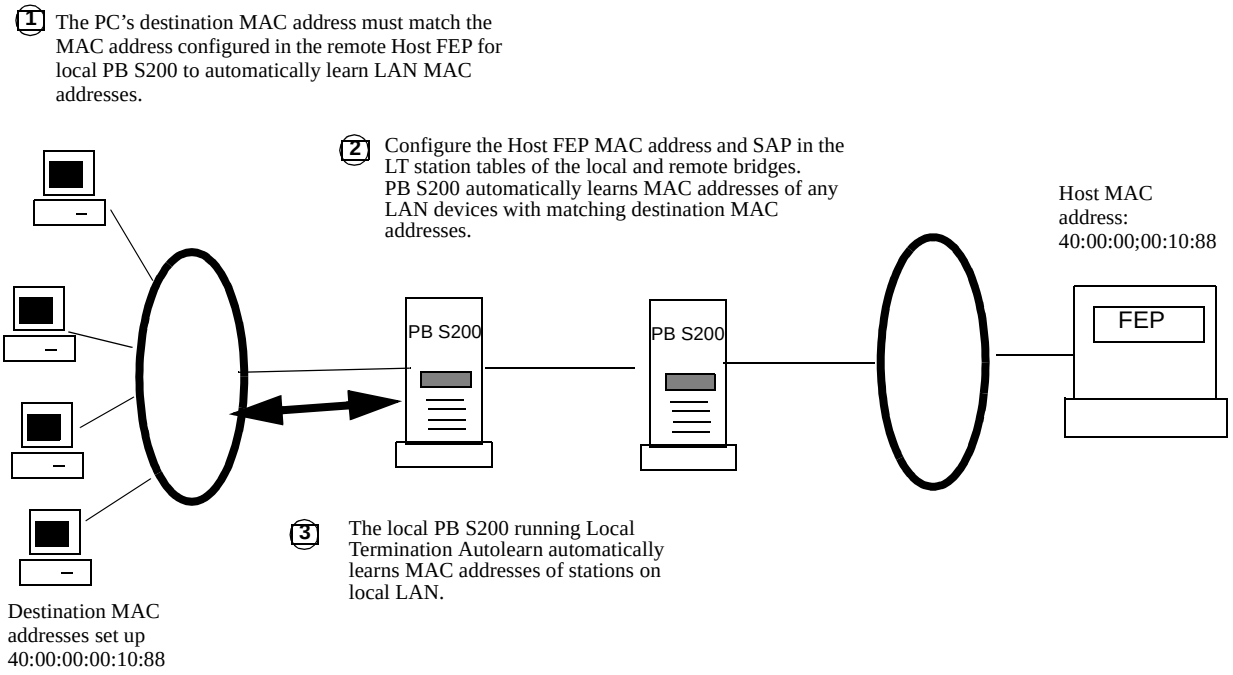


Figure 8. Example of Local Termination Autolearn

Filtering

What Is It?

Filtering lets you restrict data traffic from certain segments of your network. There are different methods used to filter data traffic on a bridged network. PathBuilder S200 series switch support for filtering includes:

- MAC Address Filtering
- NetBIOS Name Filtering
- Protocol Filtering

Mac Address Filtering

MAC Addressing is important in a bridging operation because one of the most common tasks in a bridging environment is to provide filtering of data frames. Filtering provides a way of stopping certain devices from communicating with other devices in a network. One way to filter traffic through a bridge is by identifying the devices you want to block by their MAC Addresses.

For more details on MAC Address filtering, see the section “MAC Address Filtering” section on page 58” in this manual.

NetBIOS Name Filtering

The NetBIOS Name Filtering feature of PathBuilder S200 series switches lets you restrict or filter all NetBIOS broadcasts, except those to or from a list of servers.

NetBIOS Name Filtering compares NetBIOS broadcasts to a “pattern” that may have a wild card “*” character at the end. For example, if all servers have a naming convention with the first part of the name the same, for example, “SVR...”, then you can complete only one entry in the NetBIOS Filter Table to permit broadcasts to and from the “SVR*” name pattern.

With NetBIOS Name Filters, you can block the local service name (for example, “SNA_GW”) on the WAN link so that NetBIOS broadcasts to and from that name are not forwarded across to the internetwork.This feature lets the branches use the same name for their local SNA service and you can configure all the workstations to access the same local SNA name.

Refer to “NetBIOS Name Filtering” section on page 76 in this guide.

Protocol Filtering

Protocol filtering prevents nodes operating with a certain protocol from operating outside their intended scope.

Refer to the“Protocol Filtering” section on page 70 for more details.

Spanning Tree Protocol

What Is It?

Spanning Tree Protocol reduces multiple bridge paths between LANs to a single path. Instead of a mesh network with several paths to a destination, the Spanning Tree Protocol remaps the network so that only one path is active for traffic between any source station and any destination station. The other paths block any frames between the LANs.

A spanning tree network eliminates parallel paths and traffic loops.

The PathBuilder S200 series switch implementation of the Spanning Tree Protocol Entity (SPTE) conforms to IEEE 802.ID specifications. Refer to the IEEE 802.ID specification for more detailed information on Spanning Tree Protocol operation.

Automatic & Manual Spanning Tree Support

PathBuilder S200 series switch support both automatic and manual spanning tree operations.

If you do not want to configure spanning tree operation yourself, you can use the automatic spanning tree creation option. Remember that a all bridges in your network must be configured to automatic spanning tree operation to allow for the spanning tree protocol to determine the spanning tree.

For More Details...

See the“Spanning Tree Protocol Entity (STPE)” section on page 86.

Dual Ethernet LANs

What Is It?

The PathBuilder S24x, 26x, and 27x switch supports up to two Ethernet LANs in t he same node. This means you can connect up to two Ethernet LANs to a single PathBuilder S24x, 26x, and 27x switch to perform bridging and routing of LAN traffic across the WAN to multiple Ethernet LANs. Before Dual Ethernet LAN, the PathBuilder S24x, 26x, and 27x switch supported only one Ethernet LAN port for remote bridging and routing of LAN traffic.

For More Details...

See the “Dual LAN Ethernet” section on page 117.

Basic Remote Bridging Examples

Introduction

This section shows some common examples of bridging applications using PathBuilder S200 series switches.

Remote Bridging Across a WAN

Figure 9 shows a common Source Route Bridging operation for PathBuilder S200 series switches where two Token Ring LANs are attached across a WAN. For example, two LANs could be bridged using two PathBuilder S200 series switches interconnected by an X.25 or Frame Relay link. Bridged traffic flows between the bridges over a Switched Virtual Circuit (SVC) that connects them together across the WAN (or Permanent Virtual Circuit (PVC) for Frame Relay).

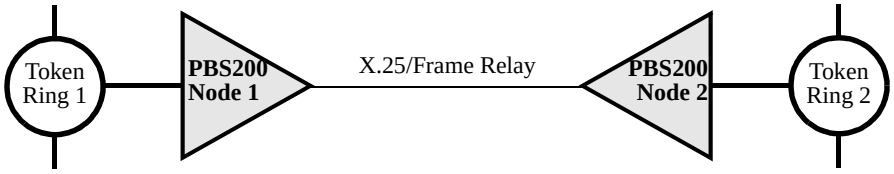


Figure 9. PB S200s Connecting LANs via an X.25/Frame Relay Link

Extended Bridging for Multiple LANs

If more than two remote LANs are involved in your bridging application, the bridge arrangement can be extended so that individual LAN pairs are connected by different bridges, as shown in Figure 10.

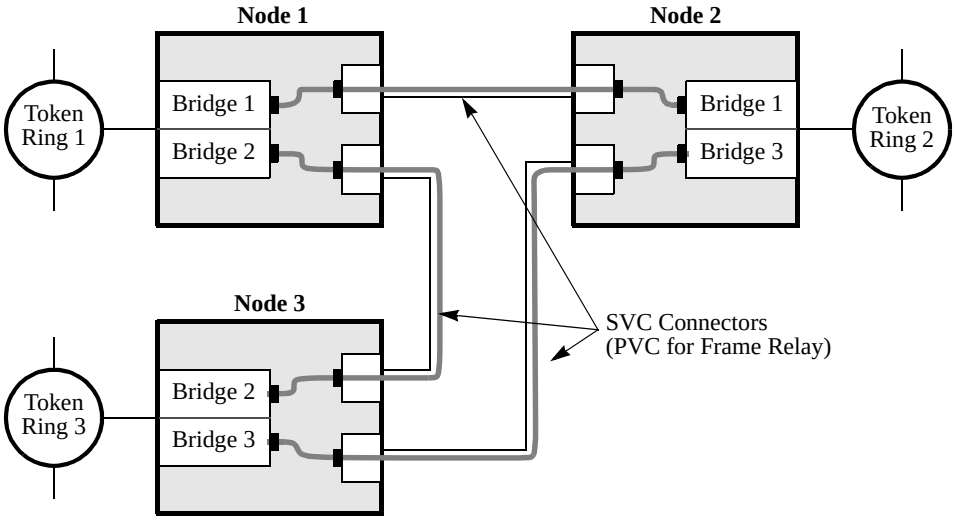


Figure 10. Two-Port Bridges Connecting Multiple Token Ring LANs

In this example, each pair of LANs is connected by a single bridge formed by bridge pairs.

- Bridge 1 interconnects Token Ring 1 and Token Ring 2
- Bridge 2 interconnects Token Ring 1 and Token Ring 3
- Bridge 3 interconnects Token Ring 2 and Token Ring 3

A Less Complex Extended Bridge

Figure 11 shows a possible arrangement of SVCs (PVCs for Frame Relay) that produces the same bridge arrangement as shown in Figure 10.

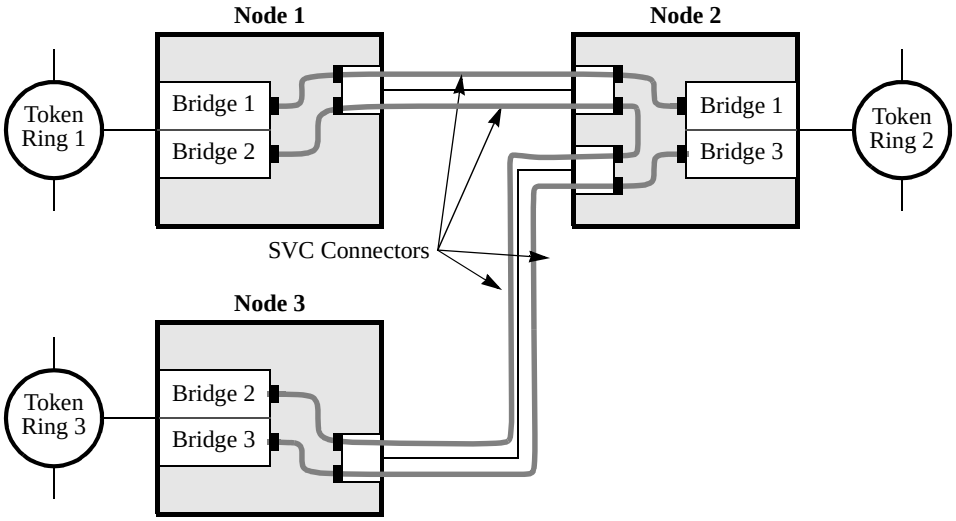


Figure 11. Example of Bridges in an SVC Arrangement

In this arrangement, all LAN segments are one hop away from each other since they are directly attached by a single pair of bridges. In Figure 11, Token Ring 1 is one bridge away from Token Ring 2 and Token Ring 3 and the same applies for the other rings.

From a bridged network point of view, Token Ring 1 is one bridge away from Token Ring 3, but Node 1 is not directly connected to Node 3. Traffic between Token Ring 1 and Token Ring 3 does not have to pass through Token Ring 2. This is an important advantage in configuring bridge networks with the PathBuilder S200 series switch because you can form a minimal bridge network to accomplish the desired interconnectivity.

Bridge Hardware Components in PathBuilder S200 Series Switches

Introduction

This section describes bridge hardware configuration and connections for the PathBuilder S200 series switch.

Bridge Configuration and Connections

Figure 12 shows the physical connections of the modules that provide bridging functionality for PathBuilder S200 series switch. This figure shows a LAN port module and supporting WAN Adapter module within a PathBuilder S200 series switch. The LAN port module is broken out into a driver and a forwarder to show the concept of bridge links.

At each end node, the bridge has connections referred to as bridge links. Bridge links that connect to the LAN are referred to as LAN bridge links. Bridge links that connect to remote bridges across the WAN are referred to as WAN bridge links.

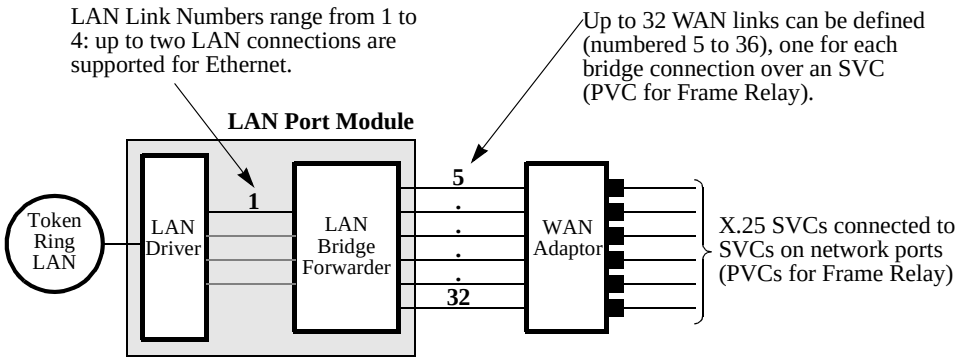


Figure 12. LAN Port Module and WAN Adapter Module (Logical View)

The LAN port consists of low level drivers and the bridge forwarder. This can be viewed as the functioning bridge. The WAN Adapter is closely associated with the bridge. The WAN Adapter provides the network services that the bridge requires in order to function over the WAN network. The principal service is establishing and maintaining SVC (PVC for Frame Relay) connections to remote LAN bridge forwarders so that virtual circuits can be formed between the forwarders.

The bridge sees the LAN and the WAN (by means of the WAN Adapter) as networks it is attached to by links. There are a total of 36 links: four LAN links and 32 WAN links.

LAN Interface Support

The PathBuilder S200 series switch supports only one LAN per node, so only one link is needed for the LAN port connection: link number 1. The PathBuilder S24x, 26x, and 27x switch supports up to two Ethernet LANs per node. See “Dual LAN Ethernet” section on page 117 for more details on this functionality.

On the PathBuilder S200 series switch links numbered 2 to 4 are not used and are reserved for future configurations. WAN links are numbered 5 to 36 and provide up to 32 WAN connection links which correspond to potential bridges.

Setting Up WAN Operation for Bridging

Introduction

With the 3Com Bridging Protocol option, you can use PathBuilder S200 series switches to connect remote LANs across a Wide Area Network (WAN), as shown in Figure 13.

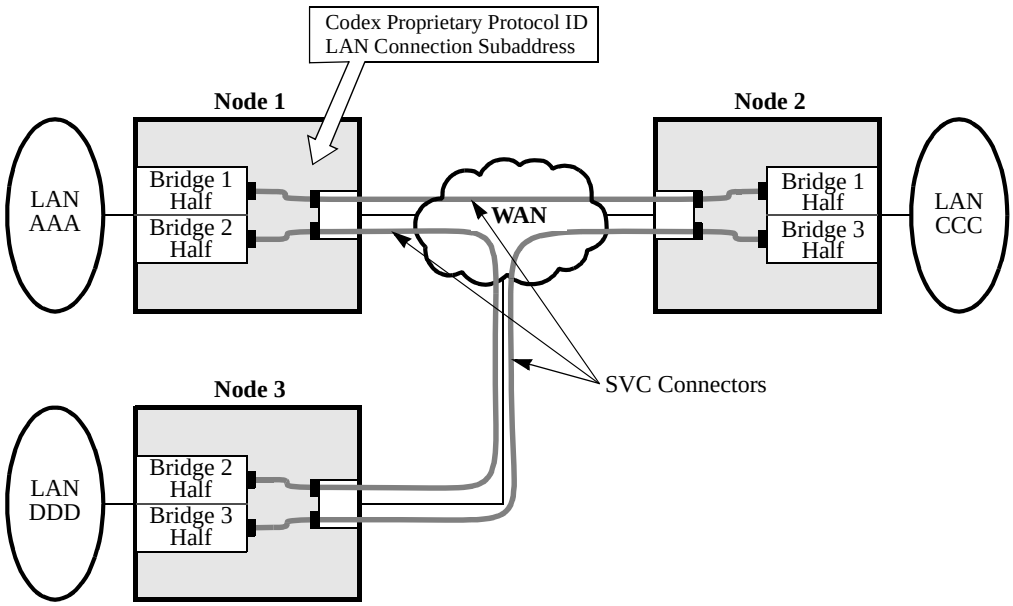


Figure 13. Interface Connections Between WAN and LAN

Critical Parameters for WAN Operation

Before you can use a PathBuilder S200 series switch as a bridge to connect LANs over a WAN, you must configure the following two parameters in the Node record for the bridge node. In most cases, use default values:

- Codex Proprietary Protocol ID
- LAN Connection Subaddress

You also need to configure the LAN Connection Table. Entries in this table are for the WAN Adapter and specify connections going across a wide area network, such as X.25, Frame Relay, or other proprietary protocols.

Codex Proprietary Protocol ID

The Protocol Identifier (ID) is placed on the Call User Data field of the Call Request packet. This packet is generated by the Autocall used to establish a circuit for a bridge link. If the bridge link is not configured to initiate an autocall, then this configured value is matched with that found in an Incoming Call packet to determine if the call should be established.

To define the Codex Proprietary Protocol ID, select a value within the designated range. Normally you would not configure a value different from the default value. The only reason to use a different value is if the default value conflicts with one already in use.

It is recommended that the Protocol ID value in all network nodes be the same.

LAN Connection Subaddress

The LAN Connection Subaddresses identifies all LAN Connections. Incoming calls with a network address consisting of the Node Address specified in the Node record and the LAN Connection Subaddress, specified in the LAN Connection Table, are verified and allowed to connect to the WAN Adapter in order to reach the LAN bridges.

The LAN Connection Subaddress is appended to the calling address of the Call Request packet if generated and sent by the WAN Adapter. Use the default value unless it conflicts with an address already in use.

Refer to the “LAN Connection Table” section on page 31 for more details.

Configuring the PathBuilder S200 Series Switch for Bridging Operation

Introduction

This section shows you how to configure a PathBuilder S200 series switch for bridging operation.

What You Need to Configure

When you are performing a Transparent Bridging operation, configure the following records in the bridge node:

- Node Record
- LAN Port Record
- Bridge Record
- Bridge Link Record
- LAN Connection Table
- Optional Filter Tables
- LAN Server Subsystem (LSS) Record (optional)
- Autocall Mnemonic Table (Some of the WAN Adapter connections are configured to Autocall.)
- Routing Table (At the destination node, a LAN Connection [LCON] entry is needed for the WAN Adapter.)

For general details on configuring the Node record and the LAN Port record, refer to the *PathBuilder S200 Series Basics Protocols*. For details on LAN Server Subsystem configuration, see the “LAN Server Subsystem” section on page 120.

The following sections describe how to configure the records and tables critical for performing bridging on a PathBuilder S200 series switch.

Bridge Parameters

Bridge Port Record Parameters

After you configure the Node record and the LAN Port record for the bridge node, configure the Bridge parameters. Figure 14 shows the parameters that make up the Bridge Parameters record.

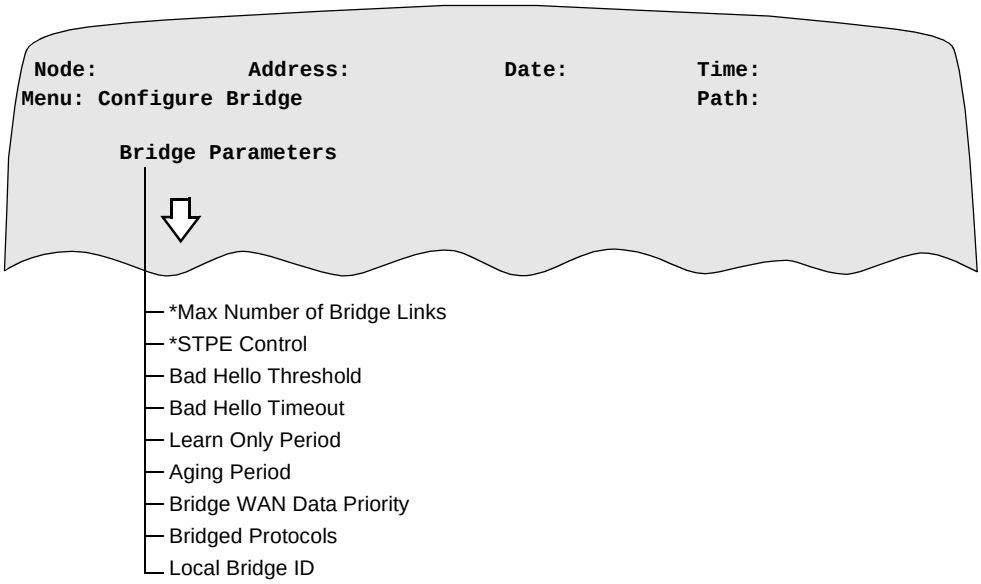


Figure 14. Configure Bridge Parameters

Parameters

These parameters make up the Bridge Parameter Record.

*Maximum Number of Bridge Links

Range:	36 to 250
Default:	36
Description:	Specifies the maximum number of bridge links allowed.
Boot Type:	A change to this parameter requires a Node boot to take effect.

*STPE Control

Range:	AUTO, MAN
Default:	MAN
Description:	The Spanning Tree Protocol Entity (STPE) module in the PathBuilder S200 series switch provides automatic calculation of the spanning tree. Spanning tree allows for the proper support of single route broadcast frames that occur in LANs. This parameter controls how a bridge determines the Spanning Tree: either automatically using the STPE, or manually using additional parameters in the bridge link record. • AUTO: The bridge participates in Spanning Tree Protocol (STP) and automatically determines the single path between LANs using the "Path Costs" assigned to the different links. Bridge protocol data units (BPDUs) are special frames used to continually communicate this information between bridges. • MAN: The Spanning Tree is configured by the network administrator. This is done using the STPE Link State parameter found in the next section, "Bridge Link Parameters." Configure all bridges in your network to MANual if you are not an expert user of Spanning Tree protocol operation. This prevents problems in operation, especially when lower speed WAN links are involved in forming bridges.

■ Note

If STPE Control parameter is set to MAN, the following parameter appears.

Bad Hello Threshold

Range:	10 to 30
Default:	15
Description:	Use this parameter to generate alarms when some bridges are configured AUTO and others are configured MAN in order to detect nonmatching configurations. A Bad Hello counter is incremented when a HELLO Protocol Data Unit (PDU) is received while the STPE Control parameter is configured to MAN. An event (alarm) is generated when the counter exceeds the value of this parameter. The event is generated only once during the Bad Hello Time.

■ Note

If STPE Control parameter is set to MAN, the following parameter appears.

Bad Hello Timeout

Range:	10 to 30
Default:	15

Bad Hello Timeout *(continued)*

Description:	Represents the timeout value in minutes. The Bad Hello counter is reset when the timeout expires and can be used to control how frequently the Hello counter reaches its alarm threshold.

Learn Only Period (used for Ethernet only)

Range:	2 to 604800
Default:	10
Description:	The time in seconds that a bridge is prevented from forwarding frames after the forwarding is cleared due to a node boot.

Aging Period (used for Ethernet only)

Range:	2 to 1000000
Default:	10
Description:	Specify the time in seconds that a learned entry in the Forwarding Table is allowed to remain in the table without being updated (relearned). If the entry is not updated within this time period, it is discarded from the table.

Bridge WAN Data Priority (used for Ethernet only)

Range:	EXP, HIGH, MED, LOW
Default:	HIGH
Description:	Specify the transmission priority of the bridged data over the WAN.

Note

If STPE Control parameter value is AUTO, this parameter appears.

Bridged Protocols

Range:	None, IP, IPX
Default:	None
Description:	Specify the routable protocols that can be bridged across BROUT or BRID links. “None” specifies no routable protocols (IP, IPX) will be bridged. “IP” specifies that IP packets can be bridged. “IPX” specifies that IPX packets can be bridged. **Note** Any combination of the available selections may be specified by summing, such as IP + IPX.

Bridge Link Parameters

Introduction

The bridge uses Bridge Links as connections to the LAN and WAN networks. The LAN Bridge Link connects the bridge directly to the local LAN, and its parameters control the characteristics of this connection.

The WAN Bridge Link parameters let you establish and maintain SVC connections to a remote LAN bridge. The bridge views the LAN bridge links and the WAN bridge links as links to the networks attached to it.

Bridge Link Parameters

Figure 15 shows the Bridge Link parameters.

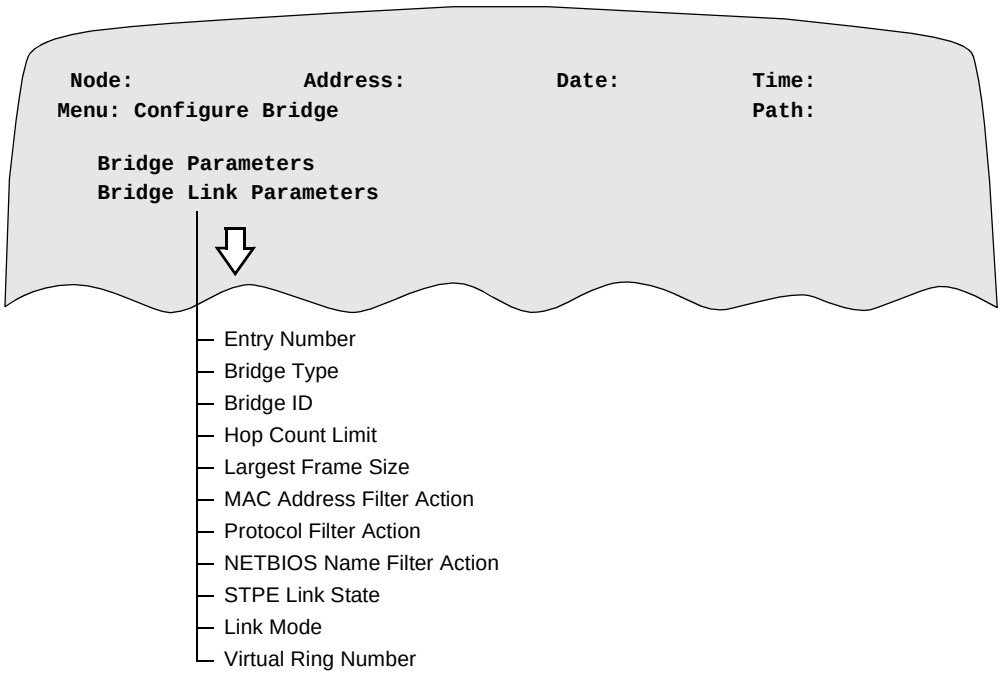


Figure 15. Configure Bridge Link Menu

Parameters

These parameters make up the Bridge Link Record.

Entry Number

Range:	1, 5 to 36
Default:	1
Description:	Specify the Bridge Link number that references this record. Two Ethernet LANs can be configured on the PathBuilder S24x, 26x, and 27x switch using 1 and 2. Links 1-4 are reserved for LAN port connections. There are 32 possible WAN Bridge Links, numbered 5 to 36. Bridges are formed by PVC/SVC connections to WAN bridge links in remote PathBuilder S200 series switch. Each bridge link used in a WAN connection is connected to a remote bridge link and such an arrangement forms a bridge between the two LANs. At the destination node, the routing table must have an entry that lists the destination port as LCON (LAN Connection). This allows the call to be directed to a connection on the WAN Adapter.

Note

The following parameter appears if you enter 5 top 36 at the Entry Number parameter.

Bridge_Type

Range:	SR, TB, BOTH_SR_AND_TB
Default:	TB
Description:	This is the bridge type for links connecting to WANs. It defines the kind of bridging that will be employed on the link. It applies only to WAN links, number 5 to 36, the maximum number of links allowed. Choose: • TB - to perform Transparent Bridging • BOTH_SR_AND_TB - when you perform mixed LAN bridging operation. This lets the node perform TB and SRB operations simultaneously.

Bridge ID

Range:	0 to 15
Default:	1
Description:	A bridge number uniquely identifies a bridge when more than one bridge is used to span the same two segments. This should match the Bridge ID of the remote Bridge half.

Hop Count Limit

Range:	0 to 7
Default:	7
Description:	Specifies the maximum number of bridges through which a broadcast frame may pass on the way to its destination.

Largest Frame Size

Range:	516, 1500, 2052, 4472
Default:	2052
Description:	Specifies the maximum size of the INFO field that this Bridge Link can send and receive. The minimum value of this parameter or of adjacent Bridge Link or values of Largest Frame Size of bridge wide parameter is used to determine whether a modification of the Routing Control field of RIF is necessary.

MAC Address Filter Action

Range:	NONE, PASS, BLOCK
Default:	NONE
Description:	Specify how the MAC Address Filter Table is used. • NONE: No MAC address filtering using the MAC Address Filter Table is performed for this link. • PASS: Look in the MAC Address Filter Table for an entry with a matching MAC frame address and take the filtering action specified by this filter table. If no matching entry is found, this value indicates that this frame should be passed. • BLOCK: Look in the MAC Address Filter Table for an entry with a matching MAC frame address and take the filtering action specified by this filter table. If no matching entry is found, this value indicates that this frame should be blocked.

Protocol Filter Action

Range:	NONE, PASS, BLOCK
Default:	NONE
Description:	Functions similarly to the MAC Address Filtering Action parameter. The filtering is applied to each link. Frames passing on a link can be either incoming or outgoing. • NONE: No Protocol filtering using the Protocol Filter Table is to be performed for this link. • PASS: Look in the Protocol Filter Table for an entry with a matching frame address and take the filtering action specified by this filter table. If no matching entry is found, this value indicates that this frame should be passed. • BLOCK: Look in the Protocol Filter Table for an entry with a matching frame address and take the filtering action specified by this filter table. If no matching entry is found, this value indicates that this frame should be blocked.

NETBIOS Name Filter Action

Range:	PASS, BLOCK, NONE
Default:	NONE
Description:	Specify how NetBIOS Name Filter is used on this node: • PASS: Pass all frames with NETBIOS name not listed in NETBIOS Name Filter Table. • BLOCK: Block all frames with NETBIOS name not listed in NETBIOS Name Filter Table. • NONE: No NETBIOS name filtering to be performed for this link.

STPE Link State

Range:	FORWARD, BLOCK
Default:	FORWARD
Description:	Specify whether to forward or block data frames when the STPE Control parameter is configured to MAN.

Link Mode

Range:	NORMAL,RFC1294, TRANS
Default:	NORMAL
Description:	Specify one of the following: • NORMAL - Bridge link connects to another Bridge using the Link Control Protocol to determine remote Ring Number. This option is not supported for PVC connections. Use another option for PVC connections. • RFC1294- Bridge link uses RFC1294 (or RFC1490) bridging to connect to another Bridge or Frame Relay Access Device. A Bridge Link Virtual Ring Number is required • TRANS - Translational Bridging support for PathBuilder S24x, 26x, and 27x switch only.
Boot Type:	A change to this parameter requires a node boot to take effect.

Note

The following parameter appears if you set Link Mode to RFC1294

Virtual Ring Number

Range:	0001-0FFF hexadecimal
Default:	0000
Description:	This is a virtual ring number that is used by the Bridge Link for connecting to another Bridge or Frame Relay Access Device via RFC1294 or RFC1490 Bridging. It must match the virtual ring number of the connecting Bridge or Frame Relay Access Device.

LAN Connection Table

Introduction

The LAN Connection Table provides information about the connections that cross over the WAN.

LAN Connection Table Parameters

Figure 16 shows the LAN Connection Table parameters.

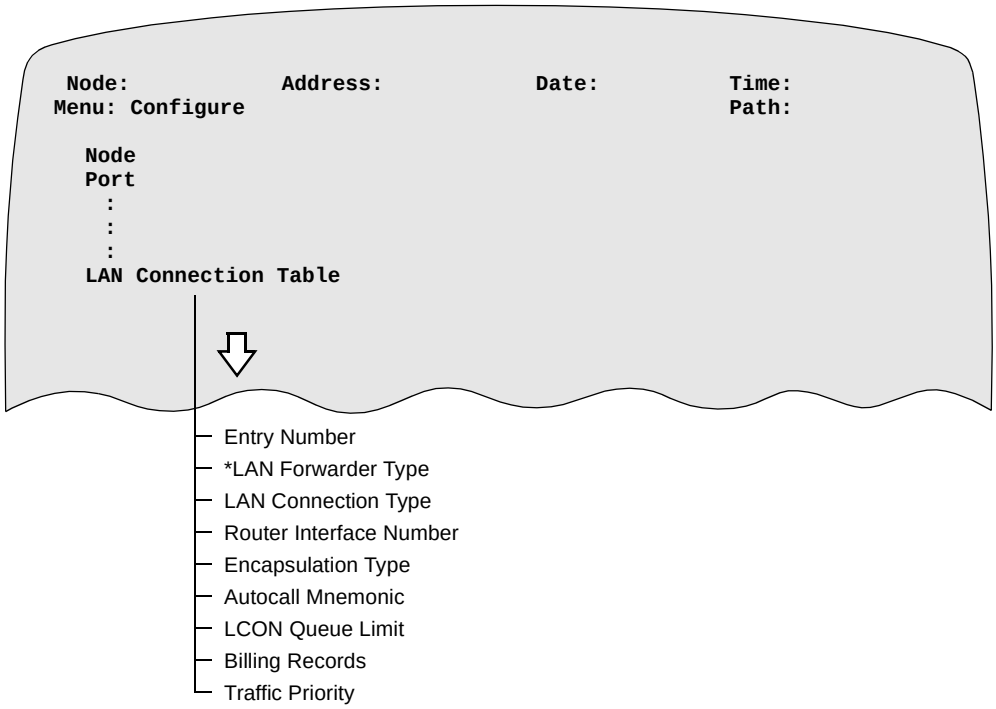


Figure 16. LAN Connection Table Menu

Parameters

These parameters make up the LAN Connection Table Record.

Entry Number

Range:	1 to 32
Default:	1
Description:	Specify the entry number used to reference this table record.

*LAN Forwarder Type

Range:	ROUT, BRID, BROUT
Default:	ROUT
Description:	Specify if the LAN Connection is to pass bridged, routed, and/or brouted traffic: • BRID: Bridged LAN traffic is transported across this connection. • ROUT: Routed LAN traffic is transported across this connection. • BROUT: Both bridged and routed LAN traffic are transported across this connection.
Boot Type:	Changes to this parameter require a Node Boot to take effect.

LAN Connection Type

Range:	PT_to_PT, GROUP
Default:	PT_to_PT (Point-to-Point)
Description:	Specify whether this LAN Connection defines a point-to-point connection across the WAN, or is part of a group of LAN Connections. If configured as GROUP, multiple LAN Connections can use the same Router Interface number. If configured as PT_to_PT, the Router Interface configured must be unique to this LAN Connection. **Note** This parameter appears if the LAN Forwarder Type is configured as ROUT or BROUT.
Boot Type:	When changing from GROUP to PT_PT, a Node boot is required. Otherwise, a Table and Node Record boot is required.

Router Interface Number

Range:	5 to n, where n = 36 to 254
Default:	5
Description:	Specifies a Router Interface using this LAN Connection record. This connection makes it possible to pass LAN data through the WAN network to a remote router. The allowable range of values reflect the maximum number of IP or IPX interfaces set in the IP or IPX Parameters Menu. **Note** This parameter appears if the LAN Forwarder Type is configured as ROUT or BROUT.
Boot Type:	Changes to this parameter require a Node Boot to take effect.

Encapsulation Type

Range:	RFC 877, RFC 1294
Default:	CODEX
Description:	Specify the type of encapsulation used over this LAN connection. Encapsulation types supported include: • CODEX: Codex Proprietary Encapsulation • RFC 877/1356: RFC 877/1356 X.25 protocol encapsulation for IP • RFC 1294/1490: RFC 1294/1490 multiprotocol encapsulation over Frame Relay
Boot Type:	Changes to this parameter require a Table and Node Record boot to take effect.

Autocall Mnemonic

Range:	0 to 8 alphanumeric characters
Default:	0 (blank)
Description:	Specify the mnemonic name used when the LAN connection is configured to autocalling. A corresponding entry must be made in the Mnemonic Table. A blank entry means autocalling will not be initiated by this LAN connection entry. The LAN connector at the remote device must initiate the call. If configured, the Autocall Mnemonic references a remote address which will be called by the LAN connection. Specifically, it must equal the node address of the node to which the remote LAN is attached (the LAN to which we want to bridge). The LAN connection subaddress configured in the node record is appended to this address to form the complete called address of an X.25 call.

LCON Queue Limit

Range:	0 to 65536
Default:	16000
Description:	The LCON Queue Limit parameter specifies the maximum number of bytes that are queued for this LAN before transmission on the WAN link. Set this parameter for two seconds of data on the WAN link.

Billing Records

Range:	OFF, ON
Default:	OFF
Description:	Enables or disables the creation (storing and printing) of billing records for the LAN connection: • ON: Billing records are generated. • OFF: Billing records are not generated.

Traffic Priority

Range:	LOW, MED, HIGH, EXP
Default:	HIGH
Description:	Specify the Traffic Priority level of this LAN Connection. • LOW: One Low Priority packet is sent for every Traffic Priority Step number of Medium priority packets. • MED: One Medium priority packet is sent for every Traffic Priority Step number of High priority packets. • HIGH: High is the first level of priority packets sent, if no expedite priority packets are sent. • EXP: Expedite priority packets have the highest priority and use all of the link bandwidth that they need. Any remaining bandwidth is shared by the high, medium, and low priority packets.

Limiting Bridge Frame Sizes

Overview

Although there are valid reasons for using larger frame sizes on bridges, there are limiting factors that must be considered when selecting a maximum frame size.

There are several reasons for limiting the maximum size of the frame, especially where bridging is done remotely across a WAN:

- The larger the frame, the longer it takes to transmit the frame on a WAN link.
- Increasing the frame size also causes a reduction in frame overhead.

Conversely, the smaller the frame, the less time it takes to transmit the frame. Since a smaller frame cannot be forwarded by an intermediary node until it is fully received, a large frame cannot be forwarded for the time it takes to transmit and receive it over a given link. On a LAN, this time is less of an issue where the link speed is approximately 10 Mbps. On a WAN link, it becomes an issue because the transmission times for large frames become significant.

Example of Frame Sizes

Figure 17 shows the effect on transit delay across a network for two cases: in one, an end system sends a large packet as a single frame and in the other, the same large packet is sent as three smaller packets.

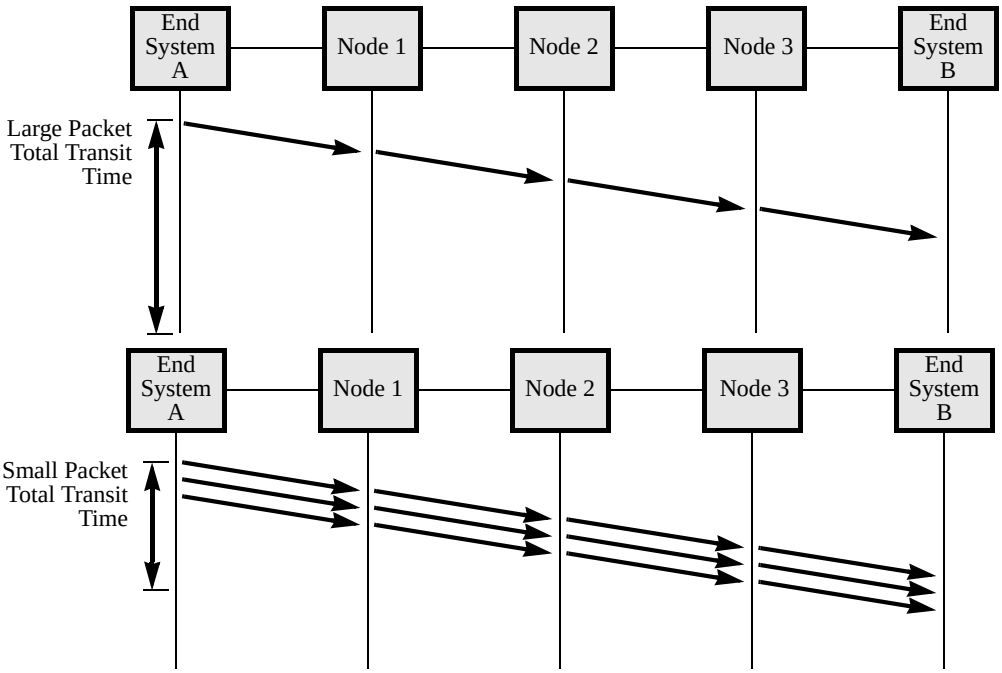


Figure 17. How Packet Size Affects Transit Delay

Small packets are forwarded more quickly by intermediate nodes resulting in the end system receiving several short frames in less time than a long frame. How much improvement is achieved depends on the transmission times and line speeds involved. The trade-off in this case is that even though the transit delay is reduced, the packet-per-second load is increased on all three nodes (and two end systems) involved. In this case, the factor is at least three if continuous streams of packets are involved.

Increasing the frame size also causes the reduction in frame overhead. If a 1000 byte data packet required a 50 byte header (frame + IP + TCP), then if 2000 bytes were placed in the frame with the same frame, the difference in overhead is 50/1000 = 5% versus 2.5%. As the size of the data increases, the overhead becomes even less. However, at these levels, the gain is marginal. Other factors may reduce this method of gain considerably. For example, intermediate systems have a limit on how large a frame they can handle.

As the size of the frame becomes larger, there is a corresponding increase in the time the frame spends in transmission media. The error rate of transmission media is finite and becomes a problem when the time for transmitting a frame becomes long enough that the probability of an error occurring during the transmission time is likely. An error on a large frame with its subsequent retransmission means the media are used with unproductive transmissions and reduced efficiency.

Standard Frame Sizes

In general, these industry standards can be used as a guideline for selecting the maximum frame size.

Max Frame Size	*Line Speed Range (kbps)*
512	9.6 to 38.4
1500	38.4 to 56
2052	56 to 1544
4472	1544

Bridge Transit Time

The transit time for bridged traffic within a PathBuilder S200 series switch is fixed to an upper bound of approximately one second. If the time is exceeded, the frame is discarded. This avoids extra traffic being sent (especially due to LLC2 recovery procedures).

Duplicate frames will frustrate normal recovery procedures and cause extra traffic to be generated. When a frame is discarded in this manner, the port statistic in the Detailed Port Stat screen displays “Frames Discarded: Congestion.”

Configuring Translational Bridging

Introduction

This section explains how to configure your PathBuilder S24x, 26x, and 27x switch to implement the Translational Bridging feature.

What is Translational Bridging

Translational Bridging allows a PathBuilder S24x, 26x, and 27x switch to bridge traffic between Ethernet and Token Ring networks. Upon receiving traffic from one network the PathBuilder S24x, 26x, and 27x switch's Source Route translates the data into a translational bridge format that can be used by the other network.

For Translational Bridging to function, several conditions must exist:

- The Token Ring network must conform to IEEE standard 802.5 and the Ethernet network mst conform to 802.3.
- The PathBuilder S24x, 26x, and 27x switch must contain a 4 Meg FLASH and be using one of these software options: Option 71 to 75.

Note

In a single node, Translational Bridging performance is limited to 350 packets per second.

Parameter

To enable Translational Bridging, you need to set the parameter Link Mode = TRANS (in the Bridge Link Parameters Record). Also, be sure the parameter Virtual Ring Number is set to a unique value.

Configuration Guidelines

These factors should be considered when configuring your PathBuilder S24x, 26x, and 27x switch for Translational Bridging:

- Only one link in a PathBuilder S24x, 26x, and 27x switch can have the parameter Link Mode = TRANS.
- Only Bridge Link with Bridge Type = SR can have Link Mode = TRANS.
- LLC Termination is not supported between Token Ring and Ethernet when using Translational Bridging.
- You can increase the value of the parameter Aging Period (in the Bridge Parameters Record) to limit the relearning of the entries in the Translational Bridging MAC Address.

For more information about configuring a PathBuilder S24x, 26x, and 27x switch for Translational Bridging, refer to the configuration example in the next section.

Configuration Examples

Figure 18 shows an example of a PathBuilder S24x, 26x, and 27x switch configured for Translational Bridging between an Ethernet and Token Ring Network within the same node. The records and parameters that need to be configured for Translational Bridging are shown.

Note

In this example, the parameters in Bridge Link 1 and Bridge Link 2 records remain at their default values. However, to implement the default settings, you need to call up the records (from the CTP) and then save them.

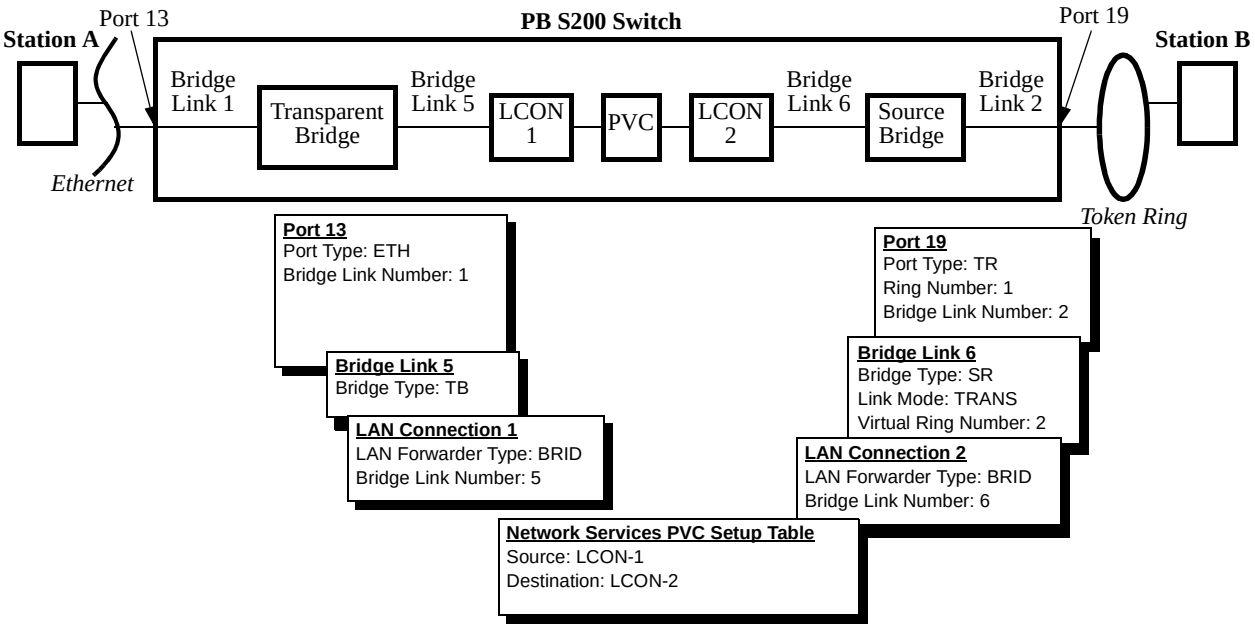


Figure 18. Translational Bridging Example

Figure 19 shows a situation where a PathBuilder S24x, 26x, and 27x switch is configured for translational bridging with SVCs/PVCs originating from two remotes. Multiple remote Ethernet and Token Ring LANs may attach to the local Token Ring via the PathBuilder S24x, 26x, and 27x switch with Translational Bridging.

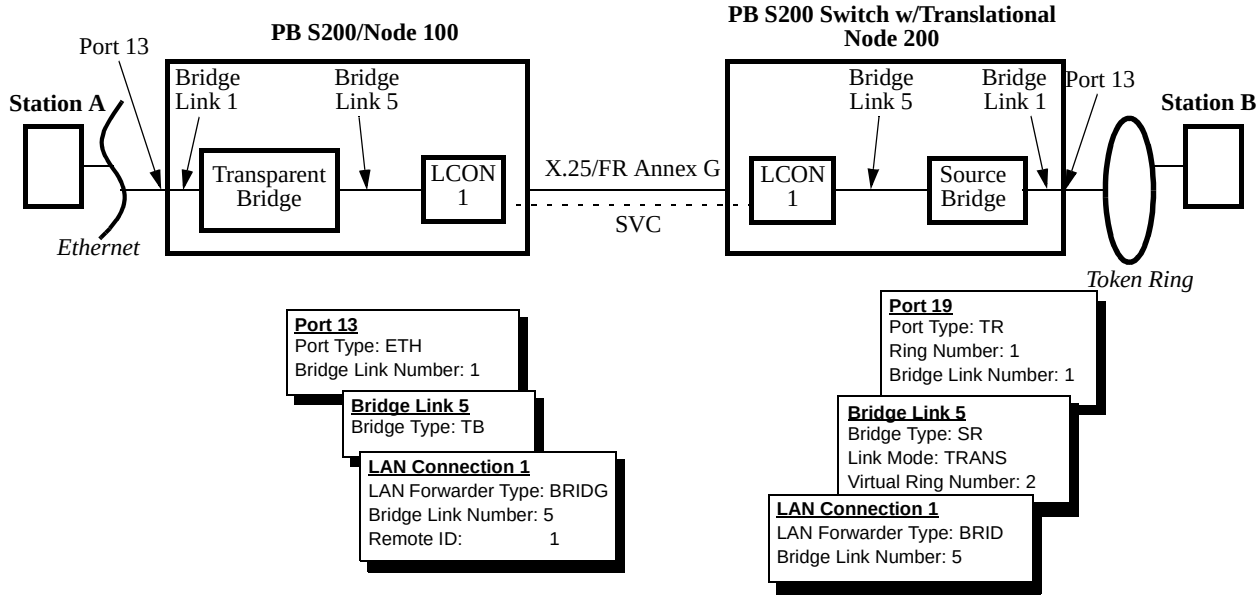


Figure 19. Translational Bridging Point-to-Point Example

Bridge Frame Handling

Introduction

This section summarizes how PathBuilder S200 series switches handle frames during Source Route Bridge operation.

How Frame Handling Works

Once a PathBuilder S200 series switch station connected to a Token Ring and is operating normally, non-MAC frames are copied from the ring as they pass through the bridge station only if they satisfy these requirements:

- The Routing Information Present bit must be set in the source MAC Address of the frame.
- If the frame is non-broadcast, the local ring number, bridge number, and remote ring number must match the bridge's stored values for these numbers, and the routing field must have less than 7 to 14 LAN/bridge couplets (depending on the configured maximum allowed).
- If the frame is single route broadcast and forwarding of single route broadcast is enabled, then the Routing Information field must not contain the remote ring number since the frame has already been on the forward ring. If single route broadcast is disabled, the frame is not copied.
- If the frame is All Route Broadcast, then the Routing Information field must not contain the remote ring number.

These rules apply to frames with either locally or universally administered addresses and for frames with either individual or group addresses.

Broadcast Frame Handling

When the All Route Broadcast frame is received from the LAN and initiated by another device on the LAN, it is sent to all remote bridges on all SVCs.

The single route broadcast frame is sent only to the remote bridge that is part of the spanning tree. The specific route frame is sent to the remote bridge via the single SVC that connects the bridges.

When received from the WAN, broadcast frames are sent to the Token Ring. They are sent to the other SVCs for general or spanning tree distribution, as appropriate, after the LAN port removes the frame from the local ring.

Routed Frame Handling

When a specifically routed frame is received from the WAN, it is sent to the Token Ring if the next bridge listed in the Routing Information field does not correspond to a bridge formed by a local SVC. Otherwise, it is forwarded to the proper SVC for additional bridging without being sent to the LAN. This keeps transit traffic off rings where it can be avoided.

Configuring Source Route Bridging Operation

Introduction

You configure a node for Source Route Bridging during normal bridge configuration. Refer to "Configuring the PathBuilder S200 Series Switch for Bridging Operation" section on page 21 for more details.

This section provides some guidelines you should consider when configuring a node for Source Route Bridge operation.

Configuring the Node for SRB Operation

The Node must be enabled for Bridge operation and some general parameters established in the "Software Key" and "Node Record" sections of the configuration menu.

- Make sure the CSK is entered for Source Route Bridging (SRB).
- The subaddress within the node for the bridge module should be specified. This allows the bridge connections to other nodes to be targeted to the right subaddress upon entering the node.
- A Codex Proprietary Protocol ID must be specified in the Node Record to ensure that calls for other traffic types, if mistakenly connected to the bridge subaddress, are rejected. Only similar remote bridges must identify themselves with this ID.

For details on configuring the Node record, refer to the *PathBuilder S200 Series Basic Protocols*.

Individual Bridge Links

Once you complete node and port configuration, individual bridge links to other nodes must be established, up to a maximum of 32 per node. Figure 20 shows LAN/WAN Bridge Links used in a PathBuilder S200 series switch LAN network.

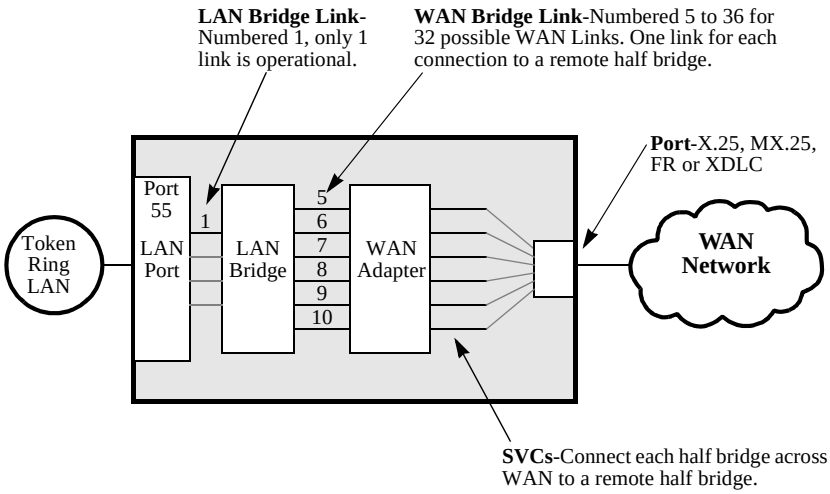


Figure 20. LAN/WAN Bridge Links Used in PathBuilder S200 Series Switch LAN Network

To assist you in configuring the node, the LAN bridge-oriented parameters are considered separate from the WAN-oriented parameters:

- **LAN Side**: The LAN port connection consists of one link. To configure the bridge module requires that you configure the LAN Port; the LAN Bridge; and the LAN Bridge Link, which passes the LAN traffic from the LAN Port to the LAN Bridge (always numbered “1”).
- **WAN Side**: The WAN Adapter (default subaddress 94) is used to make the transition from the LAN to the WAN. The WAN links are numbered 5 to 36 and provide up to 32 WAN connection links which correspond to potential bridges. These links pass the LAN traffic from the LAN Bridge to the WAN Adapter. Refer to the sections on Bridge software modules and links for more information.
- **WAN Adapter:** The WAN Adapter adapts LAN traffic to WAN protocols. It also provides other WAN services for the bridge, such as establishing network calls via a set of configurable records.

Connecting a Station to a Server in Source Route Bridging

Introduction

The following is an example of the process involved in establishing a connection between a station on one Token Ring LAN with a server on a remote Token Ring LAN for a Source Route Bridging operation.

Procedure

These steps describes the process of how a a station to server connection is set up:

1) The PC station (source) on LAN AAA requests a session to a server (destination) located on remote LAN CCC (Figure 21).

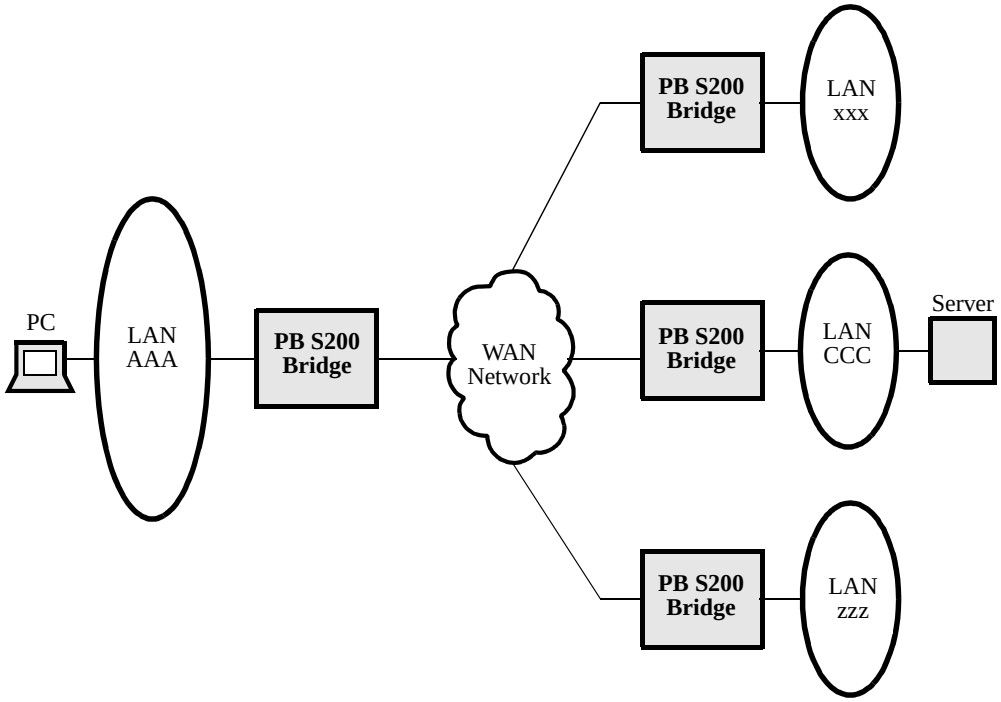


Figure 21. Example of a Station to Server Configuration

2) The PC assumes the server is on the local LAN, and the PC sends an LLC frame (typically an LLC1 TEST frame) around its local LAN AAA looking for a response from the server. The TEST frame has a destination MAC Address equal to the server's MAC Address. Since the server is not on the local ring, no station responds to the server's destination MAC Address (Figure 22). This TEST frame does not have the Routing Information Indicator bit (RII) set (the high order bit in the Source MAC Address) and as a result, it does not build a Routing Information Field (RIF) to trace the path to the destination.

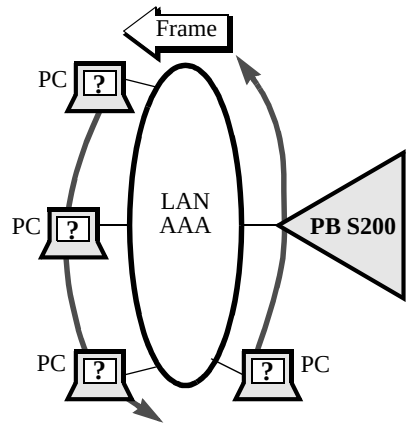


Figure 22. Server's Destination MAC Address Not on LAN AAA

3) After receiving no response on the local LAN, the PC uses Source Route Bridging (SRB) to find the path to the remote server. The PC can resend the TEST frame indicating that the frame is to be bridged over all routes. The PC resends an All Route Explorer (ARE) TEST frame via its SRB software (Figure 23).

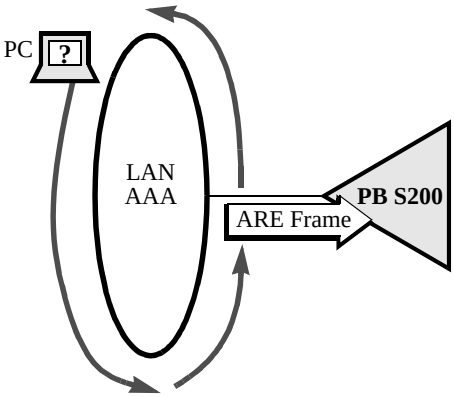


Figure 23. All Route Explorer (ARE) Frame Searches the Network for the Server

4) The TEST frame includes the following:

- Destination Address is server's MAC Address.
- Routing Information Indicator bit (RII) is set to one. This bit is the most significant bit in the source address, indicating this frame has a Routing Information Field (RIF).
- Three bits in the Routing Information Field (RIF) indicate this is an ARE. This instructs all bridges that encounter this frame to forward the frame to their destination LANs. This form of broadcast ensures that at least one copy of the frame arrives at the destination.
- Routing Information Field (RIF) shows the path (LAN number/Bridge number, LAN number/Bridge number, etc.) that each ARE frame took on its search between the source and the destination.

5) The PathBuilder S200 series switch transfers a copy of the ARE frame from the LAN Port across LAN Bridge Link number 1 to the Bridge (Figure 24). Since the frame is an All Routes Explorer, the Bridge broadcasts the frame across each of the existing WAN Bridge Links (32 max) to the WAN Adapter module.

6) The WAN Adapter transmits each ARE frame to a separate, already established SVC which connects it across the WAN to a remote node (Figure 25). Note that in the node attached to LAN AAA, three bridge links (5, 6, and 7) to the WAN side are necessary because they go to the three remote LANs to establish complete bridges to those LANs. The three right-hand nodes really need only one WAN Bridge Link each, but two additional ones are shown; they could be attached to other bridges in other nodes not shown.

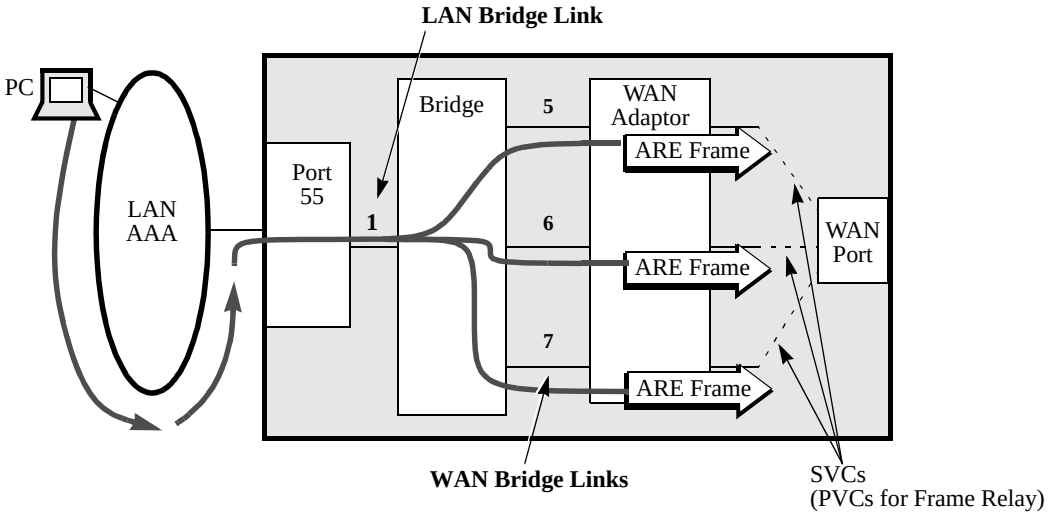


Figure 24. PathBuilder S200 Series Switch Transfers a Copy of ARE Frame to the Bridge Module

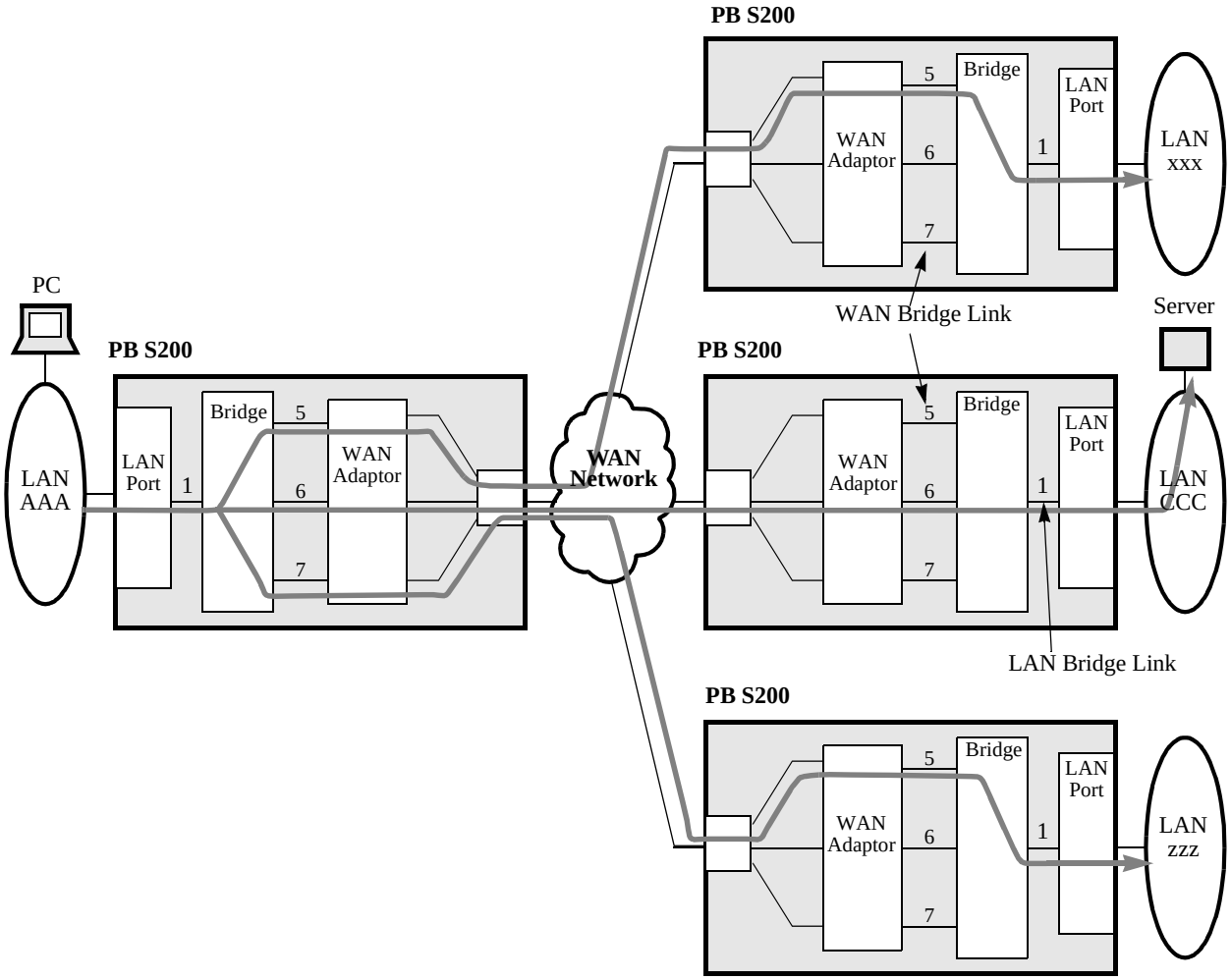


Figure 25. WAN Adapter Transmits Each ARE Frame Across the WAN

7) One of the ARE frames finds the destination server, and the server recognizes the MAC address in the TEST frame.

8) The server issues a Specific Route TEST frame (also called a non-broadcast frame) in response using the route indicated in the ARE TEST frame. Note that the server does not have to broadcast (use ARE) to get the TEST response back to the PC; it uses a Specifically Routed TEST frame (Figure 26).

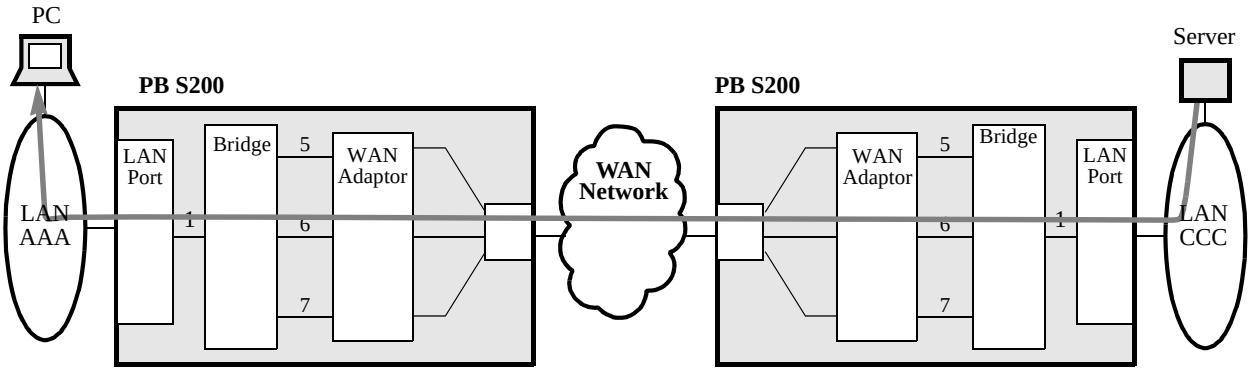


Figure 26. Server Responds with Specifically Routed TEST Frame

9) The response TEST frame also has a Routing Information Field (RIF) with the same path trace as the original ARE TEST frame except the Direction bit is set to 1. This reverses the direction in which the RIF sequence is read and indicates the path back to the source. The RIF also sets three bits in the Routing Type field that indicate the frame is to be specifically routed and not broadcast.

10) When the response TEST frame reaches the source PC, the PC now knows what route to use to send its frames to the server.

Attaching a Station to a Ring

This table describes how a station attaches to a ring.

Step	*Action*		*Result/Description*
1	The station requests values for the ring's operational parameters from the RPS.		
2	An attaching station also sends the RPS its adapter software level as well as its Upstream Neighbor Address.		
	If...	***Then...***	
	An RPS is present on the ring,	It responds to the station's request by sending it the current values for the ring's operational parameters.	The RPS then notifies the LAN managers that a new station has attached to the ring.
	An RPS is not present on the ring,	The ring station uses the values assigned by the program using the ring station or the default values for its operational parameters.	An RPS has a functional address of C00000000002.

Transparent Bridging for Ethernet LANs

Introduction

A transparent bridge, also known as a spanning tree bridge, decides where to relay Ethernet LAN frames by using the spanning tree protocol to develop and maintain a loop-free topology.

Using spanning tree, you can add a bridge anywhere in the Ethernet LAN without creating loops. The network devices are not involved in this decision process, which is *transparent* to them.

Learning

A transparent bridge monitors Ethernet LAN traffic, “learns” the source address of each frame it receives, and maintains a database (also known as the Forwarder) of source addresses and associated bridge connections. A transparent bridge uses a timeout process to purge its database of what it considers inactive addresses.

For the PathBuilder S200 series switch to “learn” where MAC stations are located in relation to themselves, they use a hardware accelerator, a transparent bridging forwarder, and a transparent bridging forwarding table.

A transparent bridge learns based upon the MAC source address. This address is placed into the transparent bridging forwarder table, along with the link that the PathBuilder S200 series switch received the frame on, if the address is not to be filtered.

When a transparent bridge receives a frame, it checks its database for the frame address and performs one of the following actions:

- If the frame’s MAC destination address is not found in the TB forwarding table, then the bridge sends the frame on all bridge connections (except for the connection on which it arrived).
- If the bridge has learned the destination address, meaning the frame’s MAC destination address is found in the TB forwarding table, then the frame is sent out on the learned link, unless there is a filter set on the link.
- The Hardware Accelerator discards local traffic before it reaches the node.

The Forwarder initiates the Learning process of the transparent bridge logic for frames received from the LAN and WAN ports.

Transparent Bridge Forwarder

After receiving an Ethernet frame, the Forwarder applies bridging logic, routes the frame to the appropriate Handler, and sends the frame to the outgoing link, which is a path to the frame’s MAC destination address.

The Forwarder:

- Initiates WAN frame learning
- Initiates LAN frame learning
- Filters the frame using the filtering facility

Information sent to the Hardware Accelerator includes:

- Source address
- Destination address

Transparent Bridge Forwarder Example

Figure 27 shows how the Forwarder and the Hardware Accelerator process a frame.

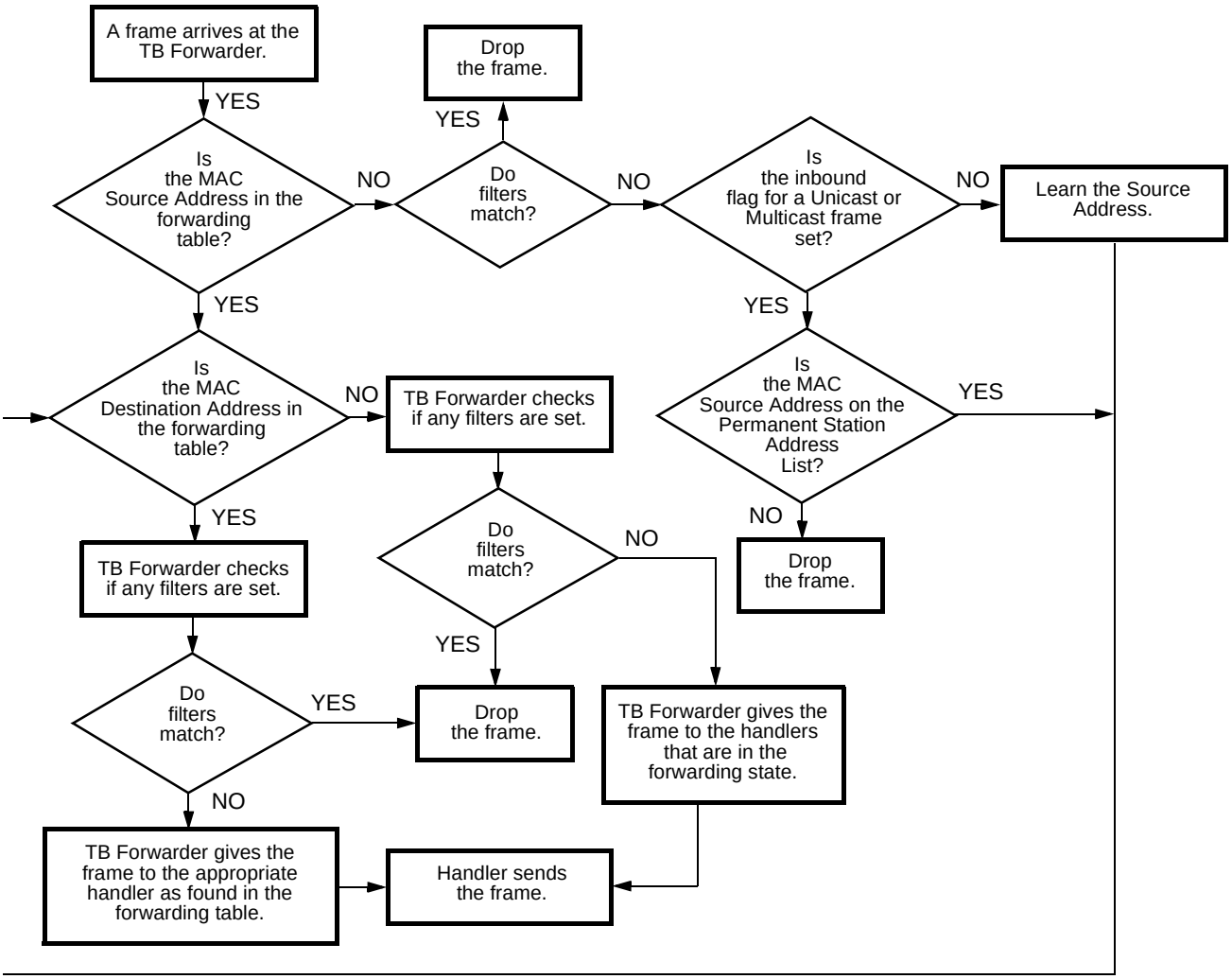


Figure 27. How the Forwarder and Hardware Accelerator Process a Frame

Forwarder Statistics

In addition, the Forwarder collects the following types of statistics:

- Filtering
- LAN link
- WAN link
- Link error

Forwarder/ Hardware Accelerator and LAN/WAN Handlers

Figure 28 shows the relationship of the Forwarder and Hardware Accelerator to the LAN and WAN Handlers.

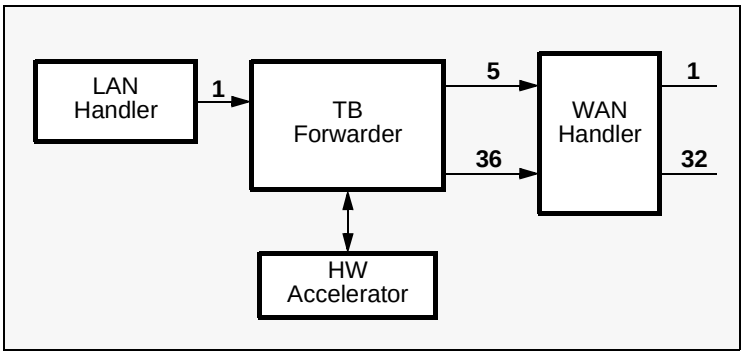


Figure 28. Relationship of Forwarder and Hardware Accelerator to LAN and WAN Handlers

Hardware Accelerator Functions

The Hardware Accelerator performs these functions:

- Discards local traffic before it reaches the node
- Participates in the learning process for LAN traffic
- Participates in the aging process for LAN traffic

The Hardware Accelerator applies the aging process to the learned addresses on a LAN port. It needs to:

- Set the aging timer bit for each address learned on the LAN link.
- Reset the aging timer bit for the entry whenever a frame with the same source address passes through the bridge
- Decrement the aging timer bit when it receives periodic timeout notification from the Forwarder
- Remove all the aged-out entries from the Hardware Accelerator database

The statistics which show the number of local traffic frames discarded by the Hardware Accelerator are displayed on the LAN port Statistic CTP menu.

Forwarder Functions

The Forwarder bridging logic includes decisions such as:

- Which Link(s) the frame should be sent to.

  If the destination address of the frame exists in the Forwarding Table, and there is a link number associated with it, then the Forwarder checks whether filters should be applied to the frame and cause the frame to be dropped. If all these conditions are satisfied and no filters apply, the Frame is sent over to the link via the Handler.

- Whether the frame should be broadcast to all ports, even though the frame is not a multicast or broadcast frame.

If the destination address of the frame did not exist in the Forwarding Table (such as when this is the first time the bridge learns the source address of the frame), the Forwarder attempts to send the frame out over all links which are in Forwarding state (except the link where the frame arrived). Before the Forwarder sends the frame out, it also checks whether filters are to be applied to this frame. The frame may get filtered at certain links.

- Whether the frame is a multicast or broadcast frame, and if it is, to which links the frame should be sent out.

The Forwarder attempts to send the multicast or broadcast frame over to all links which are in forwarding state (except the link where the frame arrived). Before sending the frame out to each link, the Forwarder checks with the filtering facility to see if filters are to be applied to the frame at that link. If not, the Forwarder sends the frame over to the link. A multicast/Broadcast frame is a frame with the Least Significant Bit of its destination address being set to 1.

- Whether the received non-multicast and non-broadcast frame should be dropped without sending it out.

The Forwarder drops the frame due to filtering, when the link is unconfigured or the link is not in forwarding state.

Two types of forwarding database entries that are kept in running memory are:

- Learned (dynamic)
- Permanent (static)

The learned entries of the forwarding database are obtained from the source address of frames that are received by the bridge entity. This relies on the end stations sending frames so that the bridge learns the station location from the source address contained in the frame.

The permanent entries are obtained from a CMEM record that is configurable by the system administrator. They are loaded into the database whenever the node or the table is booted. The permanent entries are maintained by the system administrator.

Forwarder Initialization

During Forwarder Module initialization, the Forwarder creates the sockets to connect to other modules in the node, such as sockets used to communicate with the network handlers. It also defines MACRO services in the Forwarder Module Descriptor to export the socket addresses to the outside world.

Forwarder and STPE

The Forwarder cleans up all entries in the Forwarding Table when there are spanning tree topology changes taking place. These actions are considered services the Forwarder provides to the Spanning Tree Protocol Entity (STPE). The Forwarder provides these services through MACRO routines so that they are accessible to the entire system.

Note

The Forwarder is not required to pass STPE traffic to the handlers. The STPE is considered to be an independent entity and similar to all the forwarders in the system. It has its own interface with the network handlers and it uses this interface passing PDUs to the network via the handlers. For example, it forwards Spanning tree PDUs directly to the handler and does not go through the Forwarder.

Learn Only Period

The Learn Only Period is a timer you can set from the CTP. This timer is started whenever the node boots. Until this timer expires, the bridges learn only LAN station addresses and place them into the forwarding database. The bridges do not forward any frames during this interval. When the timer expires, the bridges forward frames in the usual way. The default setting for this parameter is 10 seconds.

This timer is not to be confused with the Forward Delay timer of the spanning tree protocol entity (STPE). The STPE timer is used to control how long a bridge link withholds a link from going into the forward state once it is determined that the link should be part of the spanning tree. This timer is set to avoid bridge topology loops from forming. The Learn Only Period timer prevents the bridge from sending broadcasts (as part of the learning process) when the bridge first comes up, and has a sparse forwarding database.

Aging

Aging is an important process associated with the learned database entries. When a new entry is learned and placed in the forwarding database, a timer is set that indicates the station with the MAC address is still active. If the timer expires for an entry, the entry is removed from the database. The aging time for learned entries in the forwarding table is configurable by the system administrator. This parameter is located in the Bridge Parameters menu. The default setting for this parameter is 3600 seconds (1 hour).

The Forwarder starts the Aging Timer for the learned addresses in the Forwarding Table.

The purpose for aging database entries is to allow changes in the network configuration to be automatically accounted for in the forwarding table. If a station is moved from one LAN to another, the station becomes reachable when the entry ages out and is replaced with a new entry that indicates new forwarding information.

Aging does not apply to the permanent entries in the forwarding table. These entries are maintained by the system administrator and kept in CMEM. They are never aged out of the forwarding database and they are never corrected. If a frame arrives on an unexpected link with a source address in the permanent part of the forwarding table, the table is not changed.

Forwarder Database and Spanning Tree

How They Work Together

There is a close relationship between the forwarding database and the spanning tree. The spanning tree can be manually configured. This is a reasonable thing to do in the case where a stable environment exists since it saves CPU processing by eliminating aging timers and the broadcasting that is employed when the forwarding table does not have a suitable entry. In this case, when the node is booted, bridges will form a spanning tree (always the same one provided all equipment remains operational), and a permanent forwarding database can be loaded from CMEM that is required for the configuration. This also allows a quick method for the bridge to become operational.

The learning process continues even if the forwarding table is formed initially from permanent CMEM entries. That is, the forwarding database adds learned entries as they occur; if there are stations active that are not in the initial database, they will be added as they are learned. Such an expanded database can be written to the CMEM by a CTP update command. This has the effect of converting the entire forwarding table in running memory to permanent entries and creating a new permanent table in CMEM equal to the running configuration.

If the spanning tree is configured for automatic configuration, then the operation of the forwarding database is as noted previously. The permanent database offers a means of quickly obtaining a forwarding database without the bridge having to broadcast frames for which it does not know the destination link. However, since the bridge topology can change in an unpredictable way (corresponding to unpredictable network failures), it is best that the entries in the database are all aged. Aging all entries allows the forwarding database to remain current even with topology changes. Therefore, it is recommended that if such changes are expected, the system administrator should not use permanent forwarding entries. However, there is no reason that they cannot be used, and the full set of editing and saving commands still apply when the spanning tree is in automatic operation.

Deleting Forwarding Table Entries

Forwarding table entries can be deleted from CMEM by CTP command. If the system administrator changes the topology (changes bridges or stations), the CMEM record (edit, delete, add) can be updated and the table booted to get a cleaned up version of the database in working memory. This boot does not disrupt bridge operation other than a momentary disruption to forwarding traffic.

The entire forwarding table in CMEM can also be deleted by a single CTP command. This lets you make substantial changes to the topology, then boot the bridge network (with no permanent forwarding table entries) to let the bridge learn station locations. After a suitable learning time, you can update the entries to permanent CMEM entries using the update command. From that point on, the permanent forwarding table will contain valid entries for the configuration.

Using Filters

Support

The Forwarder provides its own filtering facility which is used to reduce unnecessary traffic and to provide security. The filtering facility supports the following types of filters:

- Incoming Source Address Filter
- Incoming Destination Address Filter
- Outgoing Source Address Filter
- Outgoing Destination Address Filter

Incoming Source Address Filter

The Incoming Source Address Filter filters packets are based on their source address and incoming links. Frames with a source address found in the Incoming Source Address Filter List are discarded without applying bridge logic. This filter may be applied to all links or selected links.

Incoming Destination Address Filter

The Incoming Destination Address Filter filters packets based on their destination address and the incoming ports. Frames with a destination address found in the Incoming Destination Address Filter List are discarded without applying bridge logic. This filter may be applied to all links or selected links.

Outgoing Source Address Filter

The Outgoing Source Address Filter filters packets based on their source address and the outgoing links. Frames with a source address found in the Outgoing Source Address Filter List are discarded. This filter may be applied to all links or selected links.

Outgoing Destination Address Filter

The Outgoing Destination Address Filter filters packets based on their destination address and the outgoing links. Frames with a destination address found in the Outgoing Destination Address Filter List are discarded. This filter may be applied to all links or selected links.

Unicast Link Protect Flag

When a frame comes from a link with the Unicast Link Protect Flag set, and if its source address is not found in the Permanent Station Address list, the frame is dropped.

When a frame is being sent out over a link with the Unicast Link Protect Flag set, and if its destination address is not found in the Permanent Station Address List, the frame is dropped.

Once the Unicast Link Protect Flag is set for a link, source address learning for Unicast frames is stopped for that link and all the addresses that were learned before are moved into the Permanent Station Address List.

Setting or Clearing of Unicast Link Protect Flag is performed via the LAN Control menu located in the Main menu.

Multicast Link Protect Flag

When a multicast/broadcast frame comes from a link with the Multicast Protect Flag set, and if its source address is not found in the Permanent Station Address list, the frame is dropped.

When a multicast/broadcast frame is sent out over a link with the Multicast Protect Flag set, and if its destination address is not found in the Permanent Station Address List, the frame is dropped.

Once the Multicast Protect Flag is set for a link, source address learning for multicast/broadcast frames is stopped for that link totally and all the addresses that were learned before are moved into the Permanent Station Address List.

Setting or Clearing of Multicast Link Protect Flag is performed using the LAN Control menu located in the Main menu.

Transparent Bridge Configuration Parameters

TB Forwarding Table

Figure 29 shows the Transparent Bridge Forwarding Table parameters.

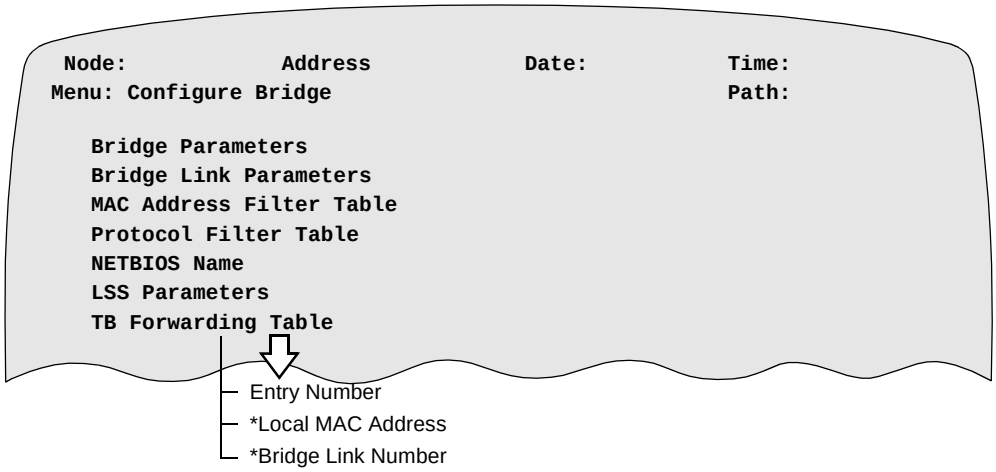


Figure 29. Transparent Bridge (TB) Forwarding Table Menu

Parameters

These parameters make up the Transparent Bridge Forwarding menu.

Entry Number

Range:	1 to 8000
Default:	1
Description	Entry used to reference this table record.

*Local MAC Address

Range:	00-00-00-00-00-01 to FF-FF-FF-FF-FF-FF
Default:	00-00-00-00-00-01
Description	MAC Address that is to be used for forwarding.

Bridge Link Number

Range:	1, 5 to 36,
Default:	1
Description	The bridge link to forward a frame with the associated MAC Address.
Boot Type:	Perform a node boot to implement changes to this parameter.

Bridge Filtering

What is It?

Bridge filtering prevents extraneous traffic from traversing the WAN and stops the unintentional proliferation of traffic onto other remote LAN segments.

In Ethernet Transparent Bridging, the broadcast feature lets stations determine routes to other end stations. Broadcasting to the entire network can unnecessarily degrade performance because of broadcasts traversing LAN segments that are not in any part of the network where the target station resides.

Therefore, you can use bridge filtering methods such as MAC Address Filtering, Protocol Filtering, and NetBIOS Name Filtering to control broadcast traffic and reduce overhead.

How Filtering is Used

Filtering is used to:

- Reduce unnecessary traffic affecting the performance of LAN segments. Filtering broadcasts can help to reduce this overhead.
- Control the unnecessary proliferation of application level broadcasting used on Novell and NetBIOS applications.
- Restrict access to certain LAN segments for security reasons.
- Prevent unnecessary traffic from proliferating onto the WAN where bandwidth is limited. This can help to reduce congestion and minimize delay for traffic that must cross the WAN.
- Prevent stations using a certain protocol from operating outside their intended scope. Protocol formats that are filtered include DSAP and SNAP.

You can filter the MAC address contained in a frame or a protocol. The system applies MAC address filtering first and then follows with protocol filtering if appropriate.

MAC Address filtering can be performed on either the source address or destination address.

MAC Address Filtering

What Is It?

This feature lets you filter bridge traffic based on MAC address.

The Bridge Link Table and the MAC Address Filter Table are used to configure MAC Address filtering.

The Bridge Link Table specifies:

- Whether or not any filtering action is to be performed.
- The filtering action to perform when the MAC frame address is not found in the MAC Address Filter Table.

The Bridge Link Table contains these parameters, including the MAC Address Filtering Action parameter, which lets you specify the filtering actions to be applied at the bridge link. These parameters are located under the Configure Bridge Link menu selection:

- Entry Number
- Bridge ID
- Hop Count Limit
- Largest Frame Size
- MAC Address Filter Action
- Protocol Filter Action
- STPE Link State
- STPE Priority
- STPE Path Cost

MAC Address Filter Table Parameters

The MAC Address Filter Table specifies:

- The MAC Address of the frame to be filtered.
- The filtering action to perform on the frame.

This table is used in conjunction with the Bridge Link Table to specify filtering action and includes the link action parameters which allow you to apply filtering action to every link.

This table describes the MAC Address Filter Table parameters.

Parameter	*Action*
MAC Address	Frames that have MAC Addresses matching this MAC Address are filtered as specified by the parameters in this table.
Incoming Source Address Link Action	Perform filtering action on an inbound frame having the indicated MAC Source address.
Outgoing Source Address Link Action	Perform filtering action on an outbound frame having the indicated MAC Source address.
Incoming Destination Address Link Action	Perform filtering action on an inbound frame for the indicated MAC Destination address.

Parameter	Action (continued)
Outgoing Destination Address Link Action	Perform filtering action on an outbound frame for the indicated MAC Destination address.
List of Links	Specifies the links associated with the preceding link action parameters in this table. When Passlist (PL) is specified, the associated listed links pass the frame and the unlisted links block it. Conversely, when Blocklist (BL) is specified, the associated listed links block the frame and the unlisted links pass it.

MAC Address Filtering Action Parameter Selections

This table lists the filtering actions available for the MAC Address Filtering Action parameter.

Parameter Value	Action
Pass (P)	Look in the MAC Address Filter Table for an entry with a matching MAC frame address and perform the filtering action specified by this entry. If no matching MAC frame address is found, pass the frame.
Block (B)	Look in the MAC Address Filter Table for an entry with a matching MAC frame address and perform the filtering action specified by this entry. If no matching MAC frame address is found, block the frame.
None (N)	No filtering to be performed; pass the frame.

What Happens During Filtering

When filtering is performed, the system checks the Bridge Link Table of the bridge link involved with the frame to see if the MAC Address Filtering Action parameter is configured to disable all filtering on that bridge link. Figure 30 shows the process involved in MAC Address filtering.

If the parameter is configured to disable filtering (NONE selected), then the frame is allowed to pass and no filtering is applied.

If the parameter is configured with another value, either PASS or BLOCK, this signifies that the MAC Address Filter Table is to be checked to determine whether filtering action is to be performed. In this situation, the frame is checked to see if a match occurs between the MAC address in the frame and an address contained in an entry in the MAC Address Filter Table.

MAC Filtering Process

Figure 30 shows the MAC Filtering process.

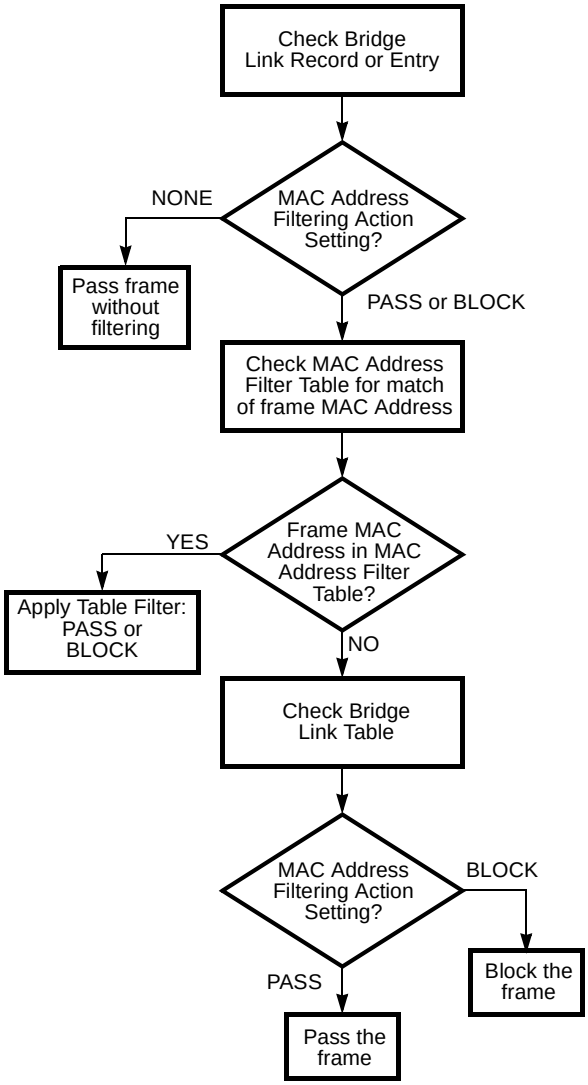


Figure 30. MAC Address Filtering Action

Mac Filtering Process

As shown in Figure 30, if a match is detected, the system applies the filtering action configured for that entry. The filtering action is to either PASS the frame or BLOCK the frame for all links or for a configured list of links. This filtering action overrides the action specified in the MAC Address Filter Action parameter.

If there is no match between the frame MAC Address and any entry in the MAC Address Filter Table, then filtering action on that frame is not controlled by the MAC Address Filter Table.

When the filtering action is not controlled by the MAC Address Filter Table, the action taken by the bridge is determined by the MAC Address Filter Action parameter in the Bridge Link Table; the action is to either PASS the frame or BLOCK it.

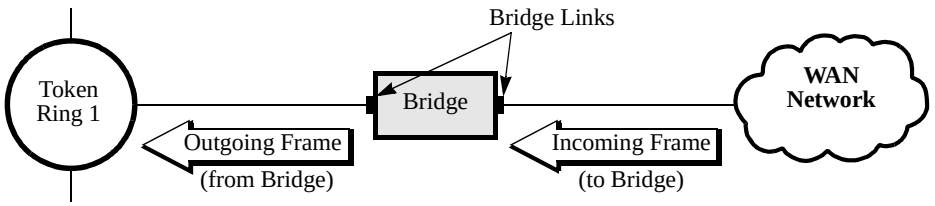
The MAC Address Filter Action parameter determines if the filter table is enabled on a bridge link. This same parameter is used to define the action taken (PASS or BLOCK) when no match is made in the MAC Address Filter Table.

For a detailed description of the MAC Address Filter parameters, refer to "Configuring the MAC Address Filter Table" section on page 66."

Incoming and Outgoing Frames

The filtering action is applied to each link. The frames passing on a link can be either incoming or outgoing (see Figure 31). Incoming means that the frame is entering the bridge from elsewhere either from the LAN or WAN. Outgoing means the frame is leaving the bridge. Therefore, a given frame can be incoming on one link and outgoing on another link (provided it does not get blocked due to filtering). Filtering can be applied at each of those links.

For any link, the PASS or BLOCK attribute can be set for either the source address or the destination address. This method allows you to individually configure every combination of in/out and source/destination to either a pass or a block action for any link.



Frames passing on a link can be either incoming or outgoing.
The same frame can be incoming on one link and outgoing on another link.

Figure 31. Example of a Frame Passing on a Bridge Link

The source address (incoming or outgoing) refers to the frame having the indicated MAC source address. The destination address (incoming or outgoing) refers to the frame having the indicated MAC destination address.

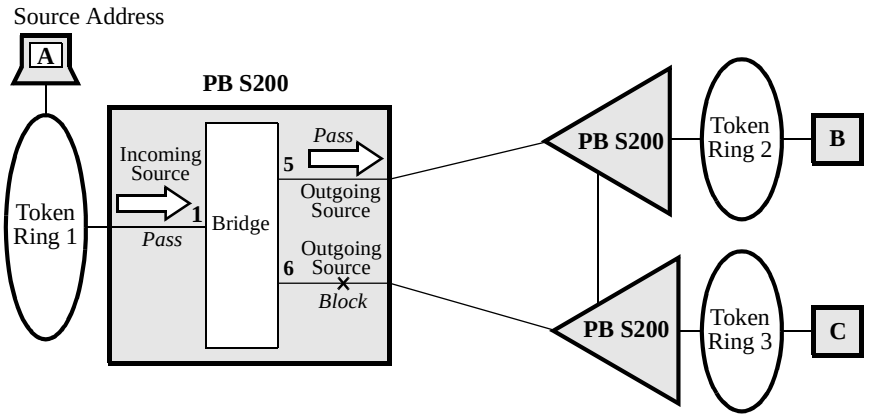
MAC Address Filtering Examples

Introduction

This section shows two filtering examples. Figure 32 shows how the source address can be used to filter frames. Figure 35 shows how the MAC Address Filter Table can be used to filter frames by combining multiple source and destination addresses.

First Example

In Figure 32, the source address (MAC Address represented by A) is used to filter frames passing in or out of the bridge via links 1, 5, and 6 (Figure 32). Frames originating from the station with MAC Address A are to be sent to server B but not server C. Figure 32 shows that for bridge link 1, Incoming Source Address frames with MAC Address A are passed, and Outgoing Source Address frames with MAC Address A are passed on link 5, but blocked on link 6.



Incoming Source Address: Pass Link 1
Outgoing Source Address: Pass Link 5; Do Not Pass Link 6 (Block)

Figure 32. Example of Bridge Links Configured to Filter Selected MAC Address Frames

How To Configure the Example in Figure 32

To configure something similar to Figure 32, complete the Bridge Link record for the bridge and the MAC Address Filter Table as shown in these tables.

Configuring the Bridge Link Record

Parameter	*Values*		
Entry Number	1	5	6
MAC Address Filter Action	Pass	Pass	Pass

Configuring the MAC Address Filter Table

Parameter	*Values*
Entry Number	1
MAC Address	A
Incoming Source Address Action	Passlist
List of Links	1
Outgoing Source Address Action	Passlist
List of Links	5

In a Bridge Link Record, Pass (or Block) tells the system to check the MAC Address Filter Table to find out what filtering to perform. If the Bridge Link Record specified None, then the frame would pass without any filtering.

If the frame MAC Address is in the MAC Address Filter Table, filtering is performed on the frame as specified in this table. The MAC Address Filter Table used in this example specifies the filtering to be performed on MAC Address A as the incoming source address to the bridge. Frames with Incoming Source Address A are passed at link 1 (see Figure 32). Frames with Outgoing Source Address A are passed at link 5 (to server B), but not passed on link 6 (to server C).

Identifying Address Links for MAC Addressing

Why it is Important

Identifying the address links is an important step in configuring MAC Address filtering.

A Source Address link allows a device on the LAN to send frames. A Destination Address link allows a device on the LAN to receive frames.

The Incoming Source Address link provides a path for a frame to go from the Token Ring to the bridge. The Outgoing Source Address link provides a path for a frame to go from the bridge to the WAN.

The Incoming Destination Address link provides a path for a frame to go from the WAN to the bridge. The Outgoing Destination Address link provides a path for a frame to go from the bridge to the LAN.

Example of Address Links

Figure 33 shows that link 5 serves as both the Outgoing Source Address link and the Incoming Destination Address link. In this example, Outgoing Source Address link 5 allows the File Server with MAC Address 10:00:5A:00:00:40 (the source) to send frames to the WAN via link 5. Incoming Destination Address link 5 allows the File Server with MAC Address 10:00:5A:00:00:40 (the destination) to receive frames from the WAN via link 5.

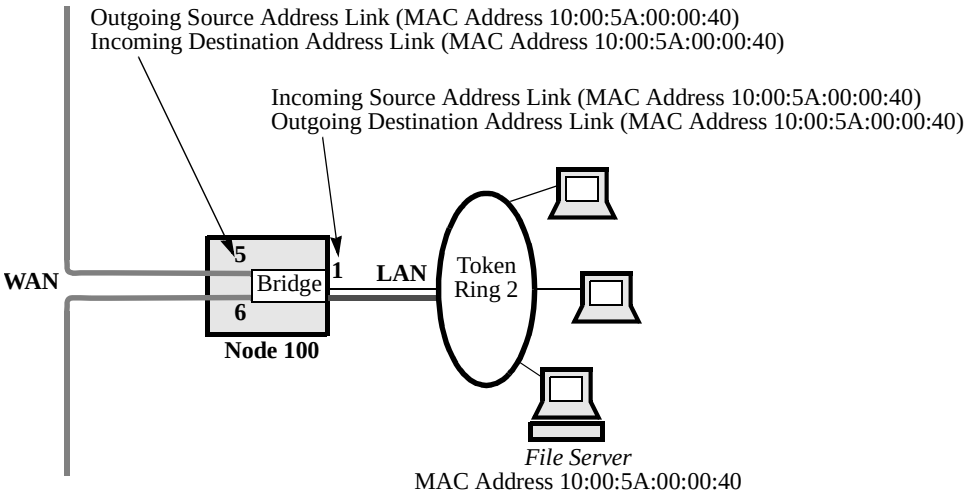


Figure 33. Example of Address Links

MAC Wildcard Filtering

What Is It?

MAC wildcard filtering is an enhancement to the Motorola Network Access Products MAC Filter table. MAC wildcard filtering lets you configure the MAC filter tables and use wildcards "*" to designate numeric pieces of the MAC address.

The MAC Address filter lets you configure a table of MAC Address filters (each filter contains a MAC address which is a string of 12 characters from the range 0-9, A-F). The table is searched for each incoming and outgoing frame on the LAN/WAN link to find a match in the table for the MAC address in the frame.

This enhancement lets you use the wildcard character "*" in any of the 12 character positions while configuring a filter. The wildcard character matches any of the valid characters allowed in a MAC address (0-9, A-F) when it is used to filter a given MAC Address.

MAC wildcard filtering lets you configure a smaller MAC Address Filter table if you configure MAC Address filters where one or more of the 12 character positions can be allowed to take any value in the permissible range.

For example, with the existing functionality, if the Bridge had to be configured to block all the frames with MAC addresses in the range 080004001F00 to 080004001FFF, you would have to configure 256 filters. Now you can simply specify 080004001F**.

PathBuilder S200 Series Switch Support

PathBuilder S200 series switches support the MAC wildcard feature on the Ethernet.

How MAC Wildcard Filtering works

Figure 34 shows a typical MAC wildcard filtering application:

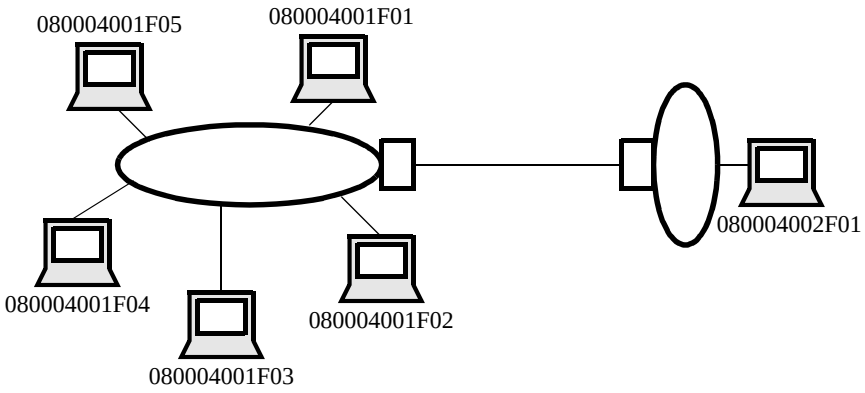


Figure 34. Example of How MAC Wildcard Filtering Works

With the old filtering system, if you do not want any of the devices shown on the LAN on the left to access the WAN, you would need to configure all five entries. With the MAC wildcard filtering, only one entry is required. For example, you can specify 080004001F** to prevent all devices from accessing the WAN.

Configuring the MAC Address Filter Table

Introduction

The MAC Address Filter Table controls which frames are allowed to pass on to different links and lets you control proprietary information that you may not want to go to another LAN. It is also useful in controlling the unnecessary proliferation of broadcast frames in the LAN network.

MAC Address Filter Table Parameters

Figure 35 shows the MAC Address Filter Table parameters.

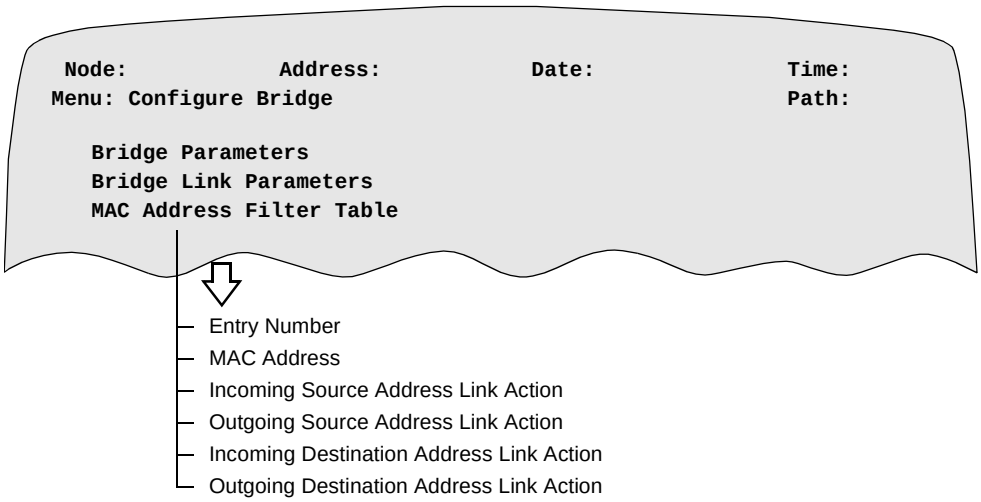


Figure 35. MAC Address Filter Table Menu

Categories

MAC Addresses can fall into four categories:

- Incoming Source
- Outgoing Source
- Incoming Destination
- Outgoing Destination

Every node (bridge) has one MAC Address Filter Table. Every bridge link can be configured to determine whether or not frames passing on that bridge link are to be filtered according to the entries in the MAC Address Filter Table.

The filter table is examined to see if there is a match. If a match is found (table and frame), additional table parameters determine when to pass or block the frame. If there is no match, the decision is dependent upon the Bridge Link record to determine whether to pass or block.

Action is then taken on what is specified in this record (pass or block), rather than the filter table, when there is no match to an entry in this filter table.

Note

A Table boot is required to make MAC Address Filter parameters part of an active configuration. Booting is nondisruptive to data or call connections.

Parameters

These parameters make up the MAC Address Filter Table.

Entry Number

Range:	1 to 300
Default:	1
Description:	Entry number used to reference this table record for filtering action. **Note** If you do not wish to determine filter action for this link through the MAC Address Filter Table, select NONE in the Bridge Link record.

MAC Address

Range:	00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF (Canonical)
Default:	00-00-00-00-00-00
Description:	Frames with MAC Addresses that match this MAC Address are filtered as specified in the following parameters. For an example of MAC Address Filtering, refer to “MAC Address Filtering Examples” in this guide.

Incoming Source Address Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	Incoming source means that the frame is entering the bridge entity from the LAN that includes the MAC address (the source). Therefore, a given source frame will be incoming from the LAN to the Bridge and outgoing from the Bridge to the WAN (provided it does not get blocked due to filtering). Refer to Figure 31. • PASS: Pass incoming frames with this MAC Address value on all links that are referencing this table. If this value is chosen, skip the List of Links. • BLOCK: Block incoming frames with this MAC Address value on all links that are referencing this table. If this value is chosen, skip the List of Links. • PASSLIST: If this value is used, a pass list is specified by the following parameter, List of Links. Links in this list pass the frame. Links not in this list block the frame. • BLOCKLIST: If this value is used, a block list is specified by the parameter, List of Links. Links in this list block the frame. Links not in this list pass the frame.

Outgoing Source Address Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	Outgoing source means that the frame is leaving the bridge for the WAN. Therefore, a given source address frame will be outgoing from bridge to WAN and incoming from LAN to bridge (provided it does not get blocked due to filtering). • PASS: Pass outgoing frames with this MAC Address value on all links that are referencing this table. If this value is chosen, skip the List of Links. • BLOCK: Block outgoing frames with this MAC Address value on all links that are referencing this table. If this value is chosen, skip the List of Links. • PASSLIST: If this value is used, a pass list is specified by the following parameter, List of Links. Links in this list pass the frame. Links not in this list block the frame. • BLOCKLIST: If this value is used, a block list is specified by the parameter, List of Links. Links in this list block the frame. Links not in this list pass the frame.

Incoming Destination Address Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	A Destination Address link allows a device on a Token Ring to receive frames. An Incoming Destination Address link provides a path for a frame to go from the WAN to the bridge. • PASS: Pass incoming frames with this MAC Address value on all links that are referencing this table. If this value is chosen, skip the List of Links. • BLOCK: Block incoming frames with this MAC Address value on all links that are referencing this table. If this value is chosen, skip the List of Links. • PASSLIST: If this value is used, a pass filtering list is specified by the following parameter, List of Links. Links in this list pass the frame. Links not in this list block the frame. • BLOCKLIST: If this value is used, a block filtering list is specified by the following parameter, List of Links. Links in this list block the frame. Links not in this list pass the frame.

Outgoing Destination Address Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	The Outgoing Destination Address link provides a path for a frame to go from the bridge to the LAN. It allows a device on a Token Ring to receive frames. • PASS: Pass outgoing frames with this MAC Address value on all links that are referencing this table. If this value is chosen, this filter is fully configured and the next prompt would wrap to MAC Address to allow further configuration of this record. If this value is chosen skip the List of Links parameter. • BLOCK: Block outgoing frames with this MAC Address value on all links that are referencing this table. If this value is chosen, this filter is fully configured and the next prompt would wrap to MAC Address to allow further configuration of this record. If this value is chosen, skip List of Links parameter. • PASSLIST: If this value is used, a pass filtering list is specified by the parameter List of Links. Links in this list pass the frame. Links not in this list block the frame. • BLOCKLIST: If this value is used, a block filtering list is specified by the parameter, List of Links. Links in this list block the frame. Links not in this list pass the frame.

List of Links

Range:	1,5, to 36
Default:	(no entry)
Description:	Each entry is a bridge link number in the range 1, 5, to 36. The individual numbers correspond to the links that filter according to the preceding parameter. If the preceding parameter is: • PASSLIST: The listed links pass the frame and unlisted links block the frame. • BLOCKLIST: The listed links block the frame and unlisted links pass the frame. This parameter appears only when the parameter Outgoing Destination Address Link Action = PASSLIST or BLOCKLIST.

Protocol Filtering

What is It?

Protocol filtering is used to prevent nodes operating with a certain protocol from operating outside their intended scope. For protocol filtering, the same fundamentals apply as with MAC Address Filtering except the Bridge Link record specifies Protocol Filtering Action.

This table shows how to configure the Bridge Link record for protocol filtering.

Parameter	*Values*		
Entry Number	1	5	6
Protocol Filtering Action	Pass	Pass	Pass

When protocol filtering is performed, the system checks the Bridge Link Table of the bridge link involved with the frame to see if the Protocol Filtering Action parameter is configured to disable all filtering on that bridge link.

Figure 30, which describes the MAC Address filtering process, is also applicable to protocol filtering. For example, if the parameter is configured to disable filtering (NONE selected), then the frame is allowed to pass and no filtering is applied.

The Protocol Filter Table is used with the Bridge Link Table to specify filtering action. It includes the link action parameters used to apply filtering action to every link.

Configuring the Protocol Filter Table

Introduction

The Protocol Filter Table prevents stations operating with a certain protocol from operating outside their intended scope. This filtering action is applied to that part of the frame that defines the protocol carried by the frame.

Note

A Table boot must be performed to implement changes to the Protocol Filter Table parameters.

Protocol Filter Table Parameters

Figure 36 shows the Protocol Filter Table parameters.

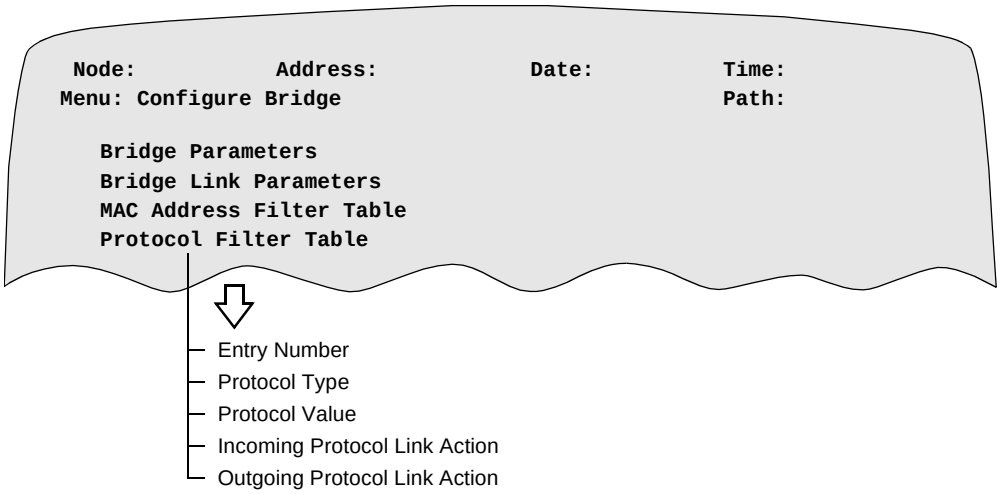


Figure 36. Configure Protocol Filter Table Menu

Parameters

These parameters make up the Protocol Filter Table Record.

Entry Number

Range:	1 to 100
Default:	1
Description:	Entry number used to reference this table record.

Protocol Type

<table>
<tr><td>Range:</td><td>DSAP, SNAP</td></tr>
<tr><td>Default:</td><td>DSAP</td></tr>
<tr><td>Description:</td><td>Indicates what type of protocol is involved in the frame.
DSAP (Destination Service Access Point): The protocol value to be filtered is the Destination SAP field of the 802.2 LLC formatted frame. This type includes:
<table>
<tr><th>Protocol</th><th>SAP (hex value)</th></tr>
<tr><td>Banyan</td><td>BC (used only for 802.5)</td></tr>
<tr><td>Novell IPX</td><td>E0 (used only for 802.5)</td></tr>
<tr><td>NetBIOS</td><td>F0</td></tr>
<tr><td>ISO Connectionless Internet</td><td>FE</td></tr>
</table>
SNAP (Sub Network Access Protocol): The Protocol Value to be filtered is specified by the SNAP header which identifies the 3-byte Organizationally Unique Identifier (OUI) and 2-byte Protocol Type used for the frame. This type includes:
<table>
<tr><th>Protocol</th><th>OUI/IP (hex value)</th></tr>
<tr><td>AppleTalk Phase II</td><td>08-00-07-80-9B</td></tr>
<tr><td>Apple ARP Phase II</td><td>00-00-00-80-F3</td></tr>
<tr><td>Proteon Proprietary AppleTalk Phase I for FDDI</td><td>00-00-93-80-02</td></tr>
<tr><td>Proteon Proprietary AppleTalk ART Phase I for FDDI</td><td>00-00-93-80-02</td></tr>
</table>
■ Note
The protocols listed here represent only some of those that are currently available for DSAP and SNAP.</td></tr>
</table>

Protocol Value

Range:	00 to FF (If Protocol Type = DSAP) 0000000000 to FFFFFFFF (If Protocol Type = SNAP)
Default:	00 (If Protocol Type = DSAP) 0000000800 (If Protocol Type = SNAP)
Description:	Indicates the hexadecimal value of the protocol that is filtered or forwarded.

Incoming Protocol Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	Specifies the action to be taken on the incoming protocol. These actions include: PASS, BLOCK, PASSLIST, or BLOCKLIST. • PASS: If this value is used, incoming frames with the specified protocol value are passed on all links. All other protocols are blocked on incoming links. If this value is chosen, skip the List of Links parameter. • BLOCK: If this value is used, incoming frames with the specified protocol value are blocked on all links. All other protocols are passed on incoming links. If this value is chosen, skip the List of Links parameter. • PASSLIST: If this value is used, a pass list is specified by the List of Links parameter. Links in this list pass the frame. Links not in this list block the frame. An empty list means all links will block. • BLOCKLIST: If this value is used, a block list is specified by the List of Links parameter. Links in this list block the frame. Links not in this list pass the frame. An empty list means all links will pass.

Outgoing Protocol Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	Specifies the action to be taken on the outgoing protocol. These actions include: PASS, BLOCK, PASSLIST, or BLOCKLIST. • PASS: If this value is used, outgoing frames with the specified protocol value are passed on all links. All other protocols are blocked on outgoing links. If this value is chosen, skip the following parameter, List of Links. • BLOCK: If this value is used, outgoing frames with the specified protocol value are blocked on all links. All other protocols are passed on outgoing links. If this value is chosen, skip the following parameter, List of Links. • PASSLIST: Pass list. If this value is used, a pass filtering list is specified by the following parameter, List of links. Links in this list pass the frame. Links not in this list block the frame. • BLOCKLIST: Block list. If this value is used, a block filtering list is specified by the following parameter, List of Links. Links in this list block the frame. Links not in this list pass the frame. An empty list means all links will pass.

DSAP Values

The DSAP is a 1-byte ID found in the LLC field (see Figure 37). You set this value in the Protocol Value parameter of the Protocol Filter Table. Examples of DSAPs include:

- IBM (04, 08,...)
- Banyan Vines (BC)
- Novell IPX (E0)
- IBM NetBIOS (F0)

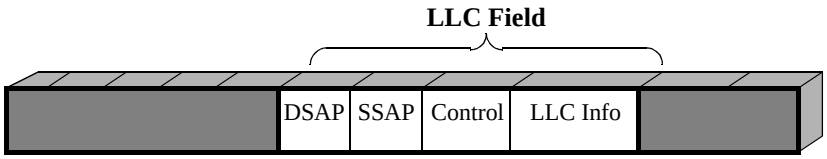


Figure 37. Protocol ID DSAP Located in LLC Field

SNAP Protocol ID

The SNAP is five bytes and is also found in the LLC field. The first three bytes are OUI and the last two bytes are the Protocol ID (Figure 38).

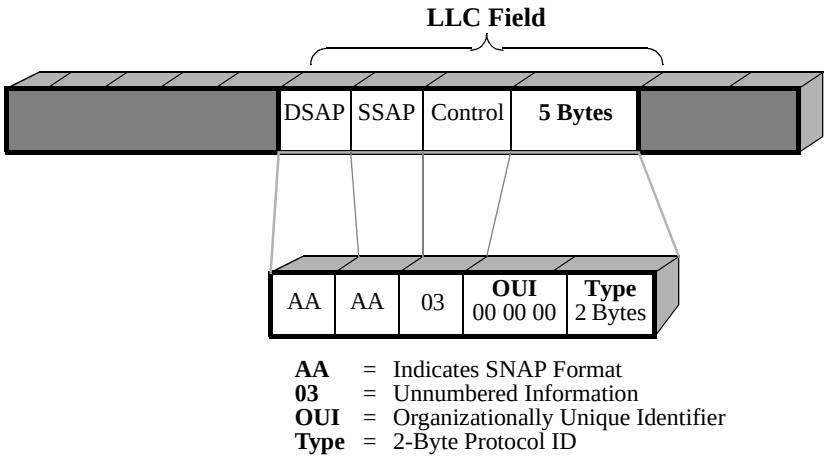


Figure 38. SNAP Protocol ID

The SNAP format is used to identify Ethernet and pre-IEEE 802 protocol IDs that do not fit the 1-byte ID.

Example of Protocol Filter Table

This table provides an overview of the Protocol Filter Table parameters.

Parameter	Action(s)
Entry Number	Used to reference this table record.
Protocol Type	Indicates what type of protocol is involved in the frame. Selections include: NONE, DSAP, and SNAP.
Protocol Value	Indicates the value of the protocol that is filtered or forwarded. Range: 00-0xFF (DSAP); 0000000000-FF... FF (SNAP).
Incoming Protocol Link Action	Specifies the action to take on the incoming protocol. Actions include: Pass, Block, Passlist, and Blocklist.
Outgoing Protocol Link Action	Specifies the action to take on the outgoing protocol. Actions include: Pass, Block, Passlist, and Blocklist.
List of Links	Specifies the links associated with the preceding link action parameters in this table. When Passlist (PL) is specified, the associated listed links pass the frame and the unlisted links block it. Conversely, when Blocklist (BL) is specified, the associated listed links block the frame and the unlisted links pass it.

NetBIOS Name Filtering

Introduction

The NetBIOS Name Filtering feature compares NetBIOS broadcasts to a “pattern” that may have a wild card “*” character at the end. For example, if all servers have a naming convention with the first part of the name the same, for example, “SVR...”, then you can complete only one entry in the NetBIOS Filter Table to permit broadcasts to and from the “SVR*” name pattern.

Example of NetBIOS Name Filtering

Figure 39 shows an example of how to configure NetBIOS Name Filtering in a Token Ring Source Rout Bridging application, however the same is true for Ethernet Transparent Bridging.

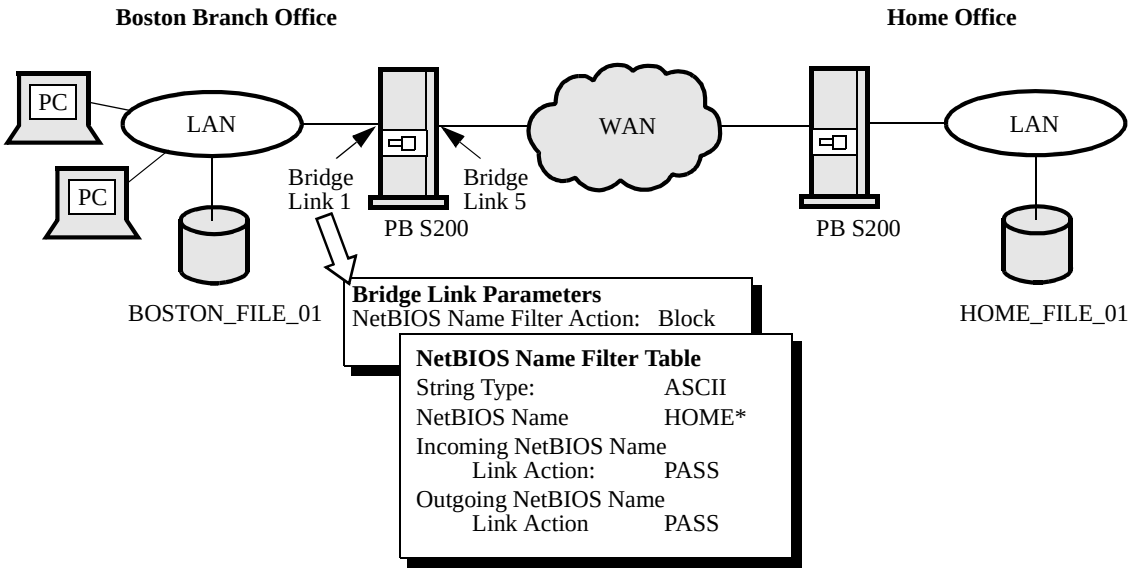


Figure 39. NetBIOS Name Filtering Configuration Example

What Is NetBIOS?

Network Basic Input Output System (NetBIOS) is a session-level protocol standardized by IBM that serves as one of the main Application Programming Interfaces (APIs) for local area network software. Software such as SNA 3270 emulation packages and Lotus Notes operate on top of the NetBIOS layer. Microsoft LAN Manager uses NetBIOS extensively for identifying clients and servers.

NetBIOS is based on 16-character named “services” that connect to each other. Servers advertise their implementation of a named service, and clients try to find servers by transmitting broadcast frames that contain the name of the service they want.

Forcing a Local Domain With NetBIOS Name Filters

The NetBIOS Name Filtering feature can also force a local domain, or context, of a NetBIOS name. All branch offices, for example, may connect to an SNA gateway function in OS/2 by accessing a gateway local to the branch. Under normal bridging conditions, you configure the SNA gateway NetBIOS server with a different name for each branch office and every workstation to attach to the name for its branch office.

With NetBIOS Name Filters, you can block the local service name (for example, “SNA_GW”) on the WAN link so that NetBIOS broadcasts to and from that name are not forwarded across to the internetwork.This feature lets the branches use the same name for their local SNA service and you can configure all the workstations to access the same local SNA name.

Wildcard Name Patterns

Name filter patterns may contain “wildcard” characters such as “?” that matches any character or “*” at the end of the pattern that matches all remaining characters. As a result, a single filter record can pass or block a large set of NetBIOS names. Unlike current MAC Filter and Protocol filters for a bridge, a packet may match more than one filter record.

For this reason, NetBIOS Name Caching operates using an ordered list of name matching records. A packet is compared against each name matching string in order, and the action for the first match is taken. If a packet does not match any NetBIOS Name Filter record, the Default NetBIOS Filter Action is taken.

Another Use of Name Filters

Another way of using NetBIOS Name Filters is to pass all NetBIOS broadcasts except those that are identified in the NetBIOS Name Filter table. This can be used, for example, to restrict access to a particular server to the local segment.

Checking NetBIOS Broadcasts

The NetBIOS Name Filtering feature does not check every NetBIOS packet. It only checks the NetBIOS broadcast packets that are used to initiate a session. Activating NetBIOS Name Filtering does not affect NetBIOS sessions already in progress.

Configuring NetBIOS Name Filtering

Introduction

This section describes how to use the Control Terminal Port (CTP) to configure NetBIOS Name Filtering.

How to Configure NetBIOS Name Filtering

Follow these steps:

Step	*Action*
1	Configure the NetBIOS Name Filter Action parameter in the Bridge Link Parameters.
2	Configure the parameters in the NetBIOS Name Filter Table record.

Bridge Link Parameters Record

Figure 40 highlights the parameter, NetBIOS Name Filter Action, in the Bridge Link Parameters record.

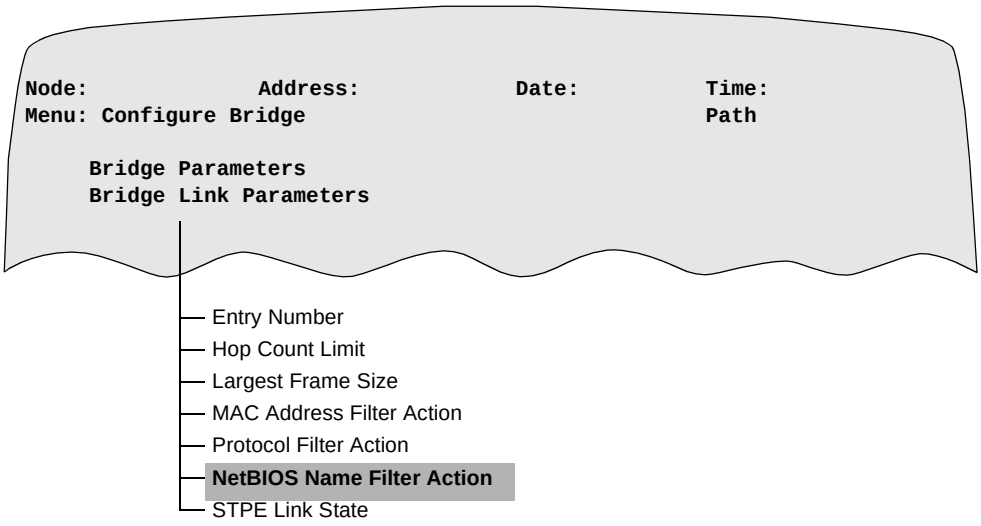


Figure 40. Bridge Link Parameters Record

Configuring NetBIOS Name Filtering

To access the NetBIOS Name Filter Action parameter, follow the steps below:

Step	*Action*	*Result*
1	Select **Configure -> Configure Bridge -> Bridge Link Parameters** from the CTP Main menu.	Entry Number 1 appears. **Note** The table has one entry for each logical bridge link in the bridge node. Bridge Link Entry 1 is reserved for the primary LAN interface. The WAN bridge links start at entry 5.
2	Enter the number of the link that you are defining and complete the NetBIOS Name Filter Action parameter using the description in the Parameters section that follows.	

Parameter

The NetBIOS Name Filter Action parameter is in the Bridge Link Parameters record.

NetBIOS Name Filter Action

Range:	PASS, BLOCK, NONE
Default:	NONE
Description:	When using NetBIOS Name Filters, set the NetBIOS Name Filter Action to BLOCK on Bridge Link 1 (the LAN link). Then define the NetBIOS Name Filter Table records with patterns for each of the server names that you want to access. • PASS — Passes all frames with a NetBIOS name that is not listed in the NetBIOS Name Filter Table. • BLOCK — Blocks all frames with a NetBIOS name that is not listed in the NetBIOS Name Filter Table. • NONE — Indicates no NetBIOS name filtering for the link.

Configure NetBIOS Name Filter Table

Figure 41 highlights the NetBIOS Name Filter Table selection in the Configure Bridge menu.

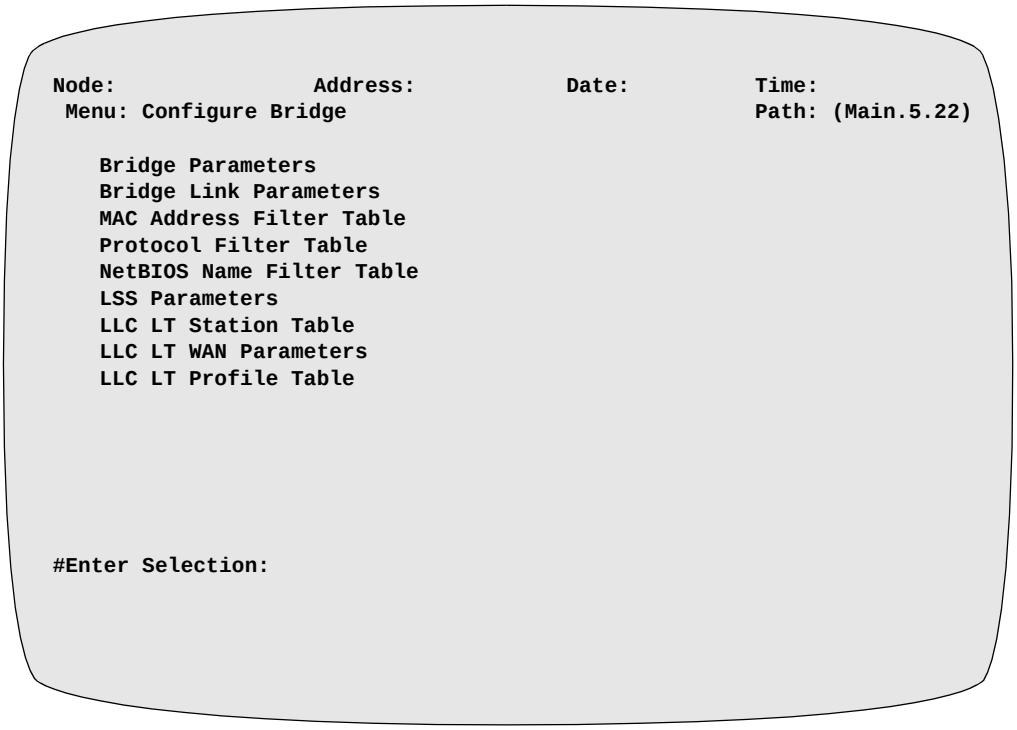


Figure 41. Configure Bridge Menu

Configuring NetBIOS Name Filter Table

To configure the NetBIOS Name Filter Table, follow these steps:

Step	*Action*	*Result*
1	Select **Configure -> Configure Bridge ->NetBIOS Name Filter Table**. from the CTP Main menu.	The first entry of the NetBIOS Name Filter Table appears. **■ Note** You can enter up to 255 entries in the table. Each entry can be a wildcard pattern that matches a class of servers used in an organization.
2	Complete the record by configuring the parameters using the description shown in the “Parameters” section on page 81”.	

Typical Filtering

For the typical case, where you filter client broadcast traffic by default and pass server traffic as discussed in the ““Typical Filtering” section on page 81.”

- Define only the NetBIOS Name field.
- Define one record for each wildcard pattern that encompasses all NetBIOS service names.

Parameters

These parameters make up the NetBIOS Name Filter Table record:

String Type

Range:	ASCII, Hex
Default:	ASCII
Description:	This parameter determines how you enter the 16-character NetBIOS name for this record. ASCII means that you enter ASCII characters for the name. The name is left-justified, blank filled to the 15th byte, and the 16th byte is ignored. Hex means that you enter hexadecimal values for up to all 16 bytes. The string is left-justified and the remaining bytes are ignored.

NetBIOS Name

Range:	0 to 16 ASCII characters (if parameter String Type=ASCII). Blank set to null. 2 to 32 hexadecimal digits (if parameter String Type=hex)
Default:	<blank>
Description:	This name string is matched against NetBIOS packets. ASCII-type strings are case-sensitive. They may contain the wildcard character “?” that matches any character, or “*” as the last character that matches all remaining characters. Hex type strings may contain the sequence “**” for a byte position to indicate a wildcard match of any byte value.

Incoming NetBIOS Name Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	The following describes the options that you can define for the link: • PASS — Passes all incoming frames with a specified NetBIOS name on all links. • BLOCK — Blocks all incoming frames with a specified NetBIOS name on all links. Passes incoming frames with other NetBIOS names on all links. • PASSLIST — If you choose this value, you need to specify a pass list in the List of Links parameter. Links that are listed pass the frame. Links that are not listed block the frame. An empty list means that all links block frames. • BLOCKLIST — If you choose this value, you need to specify a block list in the List of Links parameter. Links that are listed block the frame. Links that are not listed pass the frame. An empty list means that all links pass frames. **Note** If you chose PASS or BLOCK, skip the List of Links parameter.

Incoming NetBIOS Name List of Links

Range:	1, 5 to 36
Default:	The individual numbers correspond to the links that you filter according to the preceding parameter.
Description:	The following describes the options that you can define for the link: • PASSLIST — Passes all incoming frames on the links that are listed. Blocks all the incoming frames on the links that are not listed. An empty list means that all links block the frames. • BLOCKLIST — Blocks all incoming frames on the links that are listed. Passes all the incoming frames on the links that are not listed. An empty list means that all links pass the frames. You can enter a range of link numbers, for example, 1, 6, 8-12 indicates 1, 6, 8, 9, 10, 11, and 12.

Outgoing NetBIOS Name Link Action

Range:	PASS, BLOCK, PASSLIST, BLOCKLIST
Default:	PASS
Description:	These are the options that you can define for the link • PASS — Passes outgoing frames with the specified NetBIOS name on all links. All outgoing frames with other NetBIOS names are blocked on all links. • BLOCK — Blocks outgoing frames with the specified NetBIOS name on all links. All outgoing frames with other NetBIOS names are passed on all links. • PASSLIST — Passes all outgoing frames on the links that you listed in the List of Links parameter. Blocks all the outgoing frames on the links that are not listed. An empty list means that all links block the frames. • BLOCKLIST — Blocks all outgoing frames on the links that you listed in the List of Links parameter. Passes all the outgoing frames on the links that are not listed. An empty list means that all links pass the frames. **■ Note** If you chose PASS or BLOCK, skip the List of Links parameter.

Outgoing NetBIOS Name: List of LInks

Range:	1, 5 to 36
Default:	The individual numbers correspond to the links that you filter according to the preceding parameter.
Description:	The following describes the options that you can define for the link: • PASSLIST — Passes all outgoing frames on the links that are listed. Blocks all the outgoing frames on the links that are not listed. An empty list means that all links block the frames. • BLOCKLIST — Blocks all outgoing frames on the listed links. Passes all the outgoing frames on the links that are not listed. An empty list means that all links pass the frames.

NetBIOS Name Filtering Statistics

Introduction

For each bridge link, you can display the number of packets discarded due to matching a NetBIOS name filter on a bridge filter statistics screen. There are separate counts for the number discarded on incoming and outgoing directions for each bridge link.

Check Detailed Bridge Link Stats

Figure 42 shows the detailed statistics screen that includes counts of the number of NetBIOS broadcasts filtered on the link.

```
Node:                Address:        Date:               Time:
Detailed Bridge Link Statistics:  Bridge Link 01         Page: 2 of 2

Filter Discards:             In      Out       RIF Error Discards:
   Source MAC Address:       0       0         Segment Mismatch:   0
   Dest MAC Address:         0       0         Duplicate Segment:  0
   Protocol Filtered:        0       0
   NETBIOS Filtered:         46      0         Hop Count Exceeded: 0
Total Filter Discards:       46      0




 Press any key to continue ( ESC to exit ) ...
```

Figure 42. Detailed Bridge Link Statistics

For More Details...

Refer to the “Detailed Bridge Link Statistics” section on page 127.

NetBIOS Packet Formats

Introduction

NetBIOS Name Filtering operates only on the Microsoft or IBM-compatible NetBIOS implementations, which represents the majority of NetBIOS implementations. It does not recognize at this time Novell's implementation of NetBIOS over IPX, nor does it recognize the packet format of NetBIOS over TCP (RFC 1000).

NetBIOS Name Filtering operates on Ethernet LANs.

IBM NetBIOS Formats

IBM NetBIOS formats are documented in the IBM publication *LAN Technical Report for IEEE 802.2 and NetBIOS Interfaces*, SC-303587.

When to Use NetBIOS Name Filtering

Configure NetBIOS Name Filtering when:

All of the following are true:

- The bridged packet is a MAC-level multicast or broadcast, that is, the first transmitted bit of the destination is set.
- The bridged packet contains an 802.2 LLC field (that is, on Ethernet implementation, the packet does not use an EtherType code to distinguish the packet format).
- The LLC DSAP/SSAP/CTL fields are:

  0xF0 0xF0 x03

The first byte following the above LLC layer is considered offset 0 of the NetBIOS PDU (protocol data unit).

- The two bytes at NetBIOS offset 2-3 are 0xFF and 0xFE (NetBIOS frame delimiter).

Either one of the following is true:

- The NetBIOS command byte at offset 4 is:

  00 (Add_Group_Name) or 01 (Add_Name Query)

The packet field to be compared to the NetBIOS Name Filter list is the SOURCE name field, occupying the 16 bytes starting an offset 0x1C in the NetBIOS PDU.

- The NetBIOS command byte at offset 4 is:

  08 (Datagram) or 0x0A (Name Query)

The packet field to be compared to the NetBIOS Name Filter list is the DESTINATION name field, occupying the 16 bytes starting at offset 0x0C of the NetBIOS PDU.

When Filters Are Applied

NetBIOS name filters are applied to the broadcast packets that are transmitted in order to initiate NetBIOS sessions and to broadcast datagrams. Application of NetBIOS filters does not halt the operation of any NetBIOS sessions already in progress.

Spanning Tree Protocol Entity (STPE)

Introduction

The Spanning Tree Protocol Entity (STPE) is part of the PathBuilder S200 series switch Source Route Bridge functionality. The parameters that control Spanning Tree Protocol operation are in the Bridge Record and Bridge Link Record. In the Bridge Record, the STPE Control parameter setting determines whether Automatic or Manual Spanning Tree is used.

For detailed information about the parameters in the Bridge Record and in the Bridge Link Record, refer to the "Bridge Parameters" and "Bridge Link Parameters" sections earlier in this guide.

Automatic Spanning Tree

Automatic Spanning Tree is dynamic and involves more parameters that enable and control the Spanning Tree Protocol messages that communicate between the bridges. By processing these messages, the bridges automatically determine a spanning tree for the network. These messages are continually updated so the spanning tree automatically adjusts to the current topology. These messages consume a small amount of the bandwidth. The automatic version is redundant since PathBuilder S200 series switch has the capability of re-autocalling the destination, thereby rerouting over another link.

Manual Spanning Tree

Manual Spanning Tree is static and cannot adjust to bridge network topology changes. However, the process is more straightforward and does not consume network bandwidth (no Hello frames are used). The Spanning Tree is manually configured on a bridge link basis using the Bridge Link "STPE Link State" parameter (FORWARD/BLOCK).

What You Need to Configure

When you configure a node for bridging operation, the spanning tree parameters that appear on the Bridge Parameters Record and Bridge Link Record depend on whether you configure manual or automatic spanning tree.

Configuration Menu	*STPE Control= AUTO*	*STPE Control = MANUAL*
Bridge Record	STPE Control = Auto Bridge Priority Max Age Hello Time Forward Delay	STPE Control = Manual Bad Hello Threshold Bad Hello Count
Bridge Link Record	STPE Priority STPE Path Cost	STPE Link State

Note

All bridges in a network must operate in the same mode, either all automatic or all manual.

Custom Software Key

One Custom Software Key (CSK) enables both the Source Route Bridging and the Spanning Tree Protocol Entity.

Bridge Links

There are three types of bridge links within a given spanning tree network:

- The Root Bridge Link. The link representing the best path to the root bridge. A root link is always on the spanning tree.
- The Designated Bridge Links. All the other bridge links on the spanning tree.
- The Standby Bridge Links. All other bridge links which are not on the spanning tree.

All the bridge links of the root bridge are in the spanning tree and are designated bridge links.

Forwarding and Blocking States

After the spanning tree is determined, all root links and all designated links are placed in a forwarding state and standby links are placed in a blocking state. These states refer to the action that a link performs on data frames. For Source Route Bridging, forwarding and blocking refer to Spanning Tree Explorer data frames (Specifically Routed Frames and All Route Explorer frames are not subjected to blocking/forwarding by this link state).

When a link is in blocking state, it still monitors and passes to its own bridge the Hello message from the adjacent designated bridge link. Bridge links are not put into a forwarding state immediately upon determining their link classification. Forwarding Delay is used to allow the determination of the spanning tree network to stabilize. This prevents the network from sending information frames into temporary routing loops.

Topology Change Notification

The Topology Change Notification Bridged Packet Data Unit (BPDU) is used by a bridge that notices a topology change to send a notification in the direction of the Root Bridge. This occurs only during Automatic spanning tree operation.

When the Root Bridge finally gets this notification, it sets the topology change notification bit in the BPDU that it periodically generates. This informs all bridges that there has been a change in topology and that they should expect that station locations might have changed.

In a manual spanning tree, all the single paths are manually assigned. No Hello frames are exchanged between bridges; rather, each bridge port in the network is configured to either forward or block all Spanning Tree Explorer frames. If a link or bridge goes down, then that path stays broken until the problem is fixed.

No topology change notification occurs in manual spanning tree operation. You have to adjust the spanning tree to changes in your network either by reconfiguring the spanning tree or wait until the lost path is restored.

A manual spanning tree forms fixed single route paths between LANs, and cannot dynamically reestablish an alternate path for the broken one. However, the PathBuilder S200 series switch LAN option can use its SVC rerouting capability to overcome this problem. The PathBuilder S200 series switch senses the break, drops the original SVC between the bridged nodes, and re-autocalls creating another SVC connection using a different path across the WAN.

Since a manual spanning tree does not send Hello messages between bridges, it minimizes network bandwidth overhead. An automatic spanning tree requires sending and receiving BPDUs, which consumes processing cycles from the CPU of a node and therefore increases CPU use. A manual spanning tree avoids this usage.

Tips on Spanning Tree

Determining a spanning tree in order to set up a manual tree may seem more labor intensive than letting the bridge network determine the tree by algorithm. However, even with automatic spanning tree determination, you must study the possible arrangements of resulting trees and assign the bridge priorities accordingly to avoid unreasonable performance due to long data paths.

In fact, this responsibility points out a major disadvantage of using a bridge network in a mesh topology instead of a router. The spanning tree protocol does not allow the bridges to determine optimal paths and to route frames along them. Trying to handle this task manually by configuring bridges and bridge links quickly becomes unwieldy as soon as additional loops are possible and one tries to maintain optimal traffic routing when faced with a variety of possible link or bridge failures.

STPE Parameter Setting Considerations

Introduction

This section discusses how the bridge and bridge link parameters can be used to influence the design of a bridge network and to show how they relate to overall PathBuilder S200 series switch configuration during spanning tree operation.

Note

You should thoroughly understand the spanning tree protocol and how its parameters influence performance before you consider changing SPTE-related these parameters in a PathBuilder S200 series switch network. Otherwise, because of the critical nature of the timers involved, the spanning tree topology may become unstable. It may become difficult to trace this behavior as the effect might occur only occasionally and only in certain types of traffic patterns.

Example of a Bridge Network With Spanning Tree

Figure 43 shows a bridge network composed of six PathBuilder S200 series switches and five LANs. The links that are in the blocking state have been selected to achieve the shortest path for the bulk of the expected data flow.

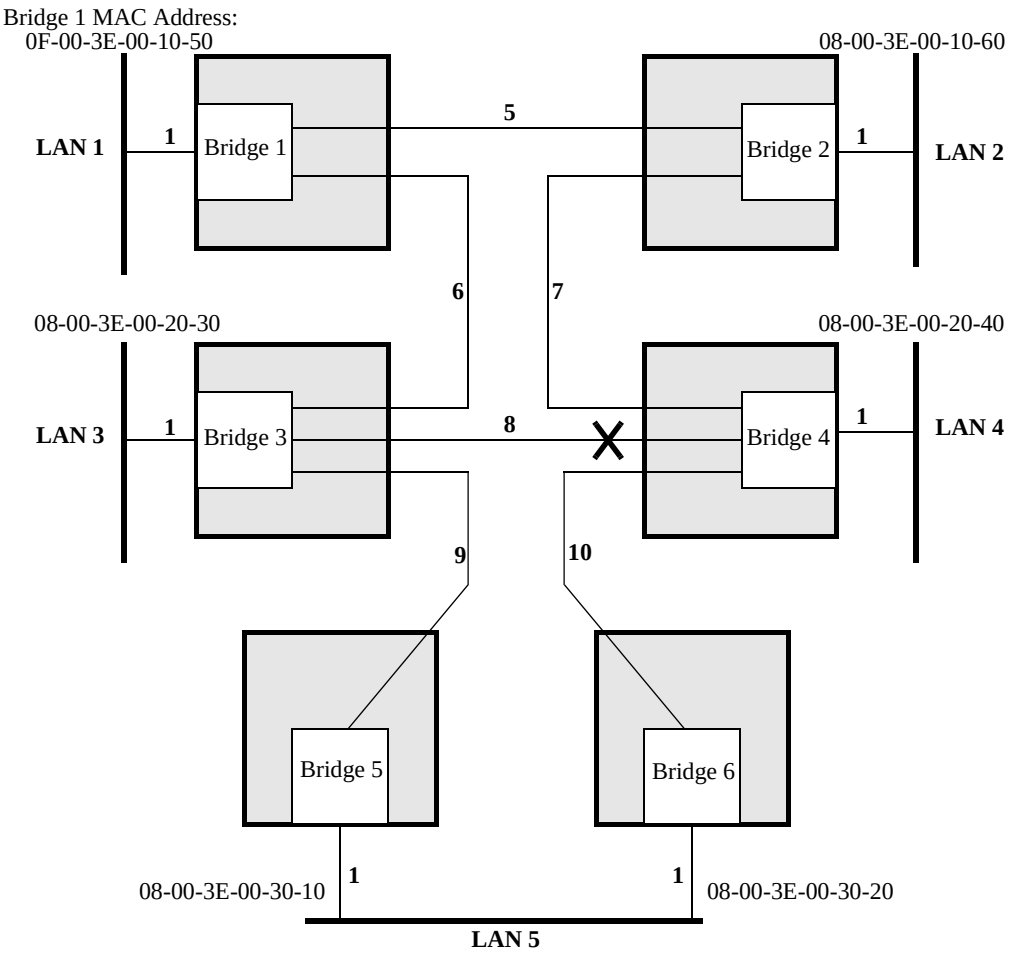


Figure 43. Example of a Bridge Network

Setting the Root Bridge of the Spanning Tree

The bridge with the lowest Bridge ID becomes the root bridge in a spanning tree network.

The Bridge ID is made up of two parts: the Bridge Priority and the MAC address of the LAN port. You modify these elements during bridge configuration from the Bridge Priority parameter in the Bridge Parameters record and the MAC Address parameter in the LAN Port record.

All bridges have the same default priority value (32768). So, without any changes to this value, the MAC address of the LAN port determines the root bridge in a network.

If you want to control which bridge becomes the root bridge, modify the Bridge Priority value appropriately.

For example:

Bridge ID: equals (Bridge Priority Value in hex) + (MAC Address)

The default bridge priority value is 32768 (8000 in hex). So, a bridge with a MAC address of 08-00-3E-02-53-8F and a default bridge priority value would have this bridge ID:

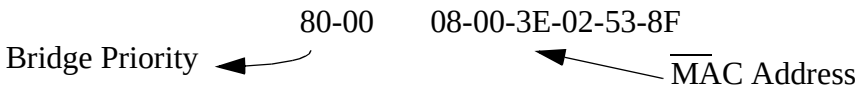


Figure 44. Example of Bridge ID and MAC Address

Determining Root Links and Designated Links

A Root Link is the Bridge Link on a particular bridge that is the preferred path to the Root Bridge.

A Designated Link is all other links that are part of the spanning tree.

In Automatic mode, the Root Link is determined by summing path costs from a bridge to the Root Bridge. Path costs are configured in the Bridge Link Record. If there are multiple paths to the Root Bridge, the bridge selects the route with the least cost to the root as the preferred link (Root Link).

All other links associated with the bridge become Designated Links.

For example, in the network in Figure 43, bridge 3 receives messages from bridges 1, 4, and 5 because these bridges are adjacent (directly connected by links). If the cost of traversing any of the WAN links is equal and bridges 1, 4, and 5 are reporting B1 as the root and that they know how to get to it, then bridge 3 will choose link 6 as the preferred link to the root because this path will have the least cost to the root.

Note

The fewest number of links involved yields the lowest cost—the fact that the link is directly attached to the root bridge is coincidental in this example.

The path cost to the root bridge has an influence on the spanning tree topology. The bridge link parameter called STPE Path Cost is the parameter that sets the incremental path cost to the root, should that bridge link be followed to the root bridge. In general, the speed of the bridge link is the most important factor that determines the path cost increment.

Determining Path Costs

Bridges use Path Cost to determine their Root Link. The range of Path Cost is 0 to 65535. The lower the path cost, the more likely this path will be used. Use This table to determine the path costs for each type of link in your network.

Type of Network	Speed	STPE Path Cost
802.3	10 Mbps	10
802.5	4 Mbps	25
802.5	16 Mbps	6
serial	1.54 Mbps	65
serial	384 kbps	260
serial	56 kbps	1768
serial	19.2 kbps	3536

For speeds not listed, interpolate to reasonable values. The valid range for path cost is 0 to 65535 so that when values are determined, they should not be such that the total path cost along any reasonable route adds up to more than 65535.

Some bridge manufacturers may list a different set of values for path cost increment. It is important that the same rule be applied to all bridges involved in the spanning tree calculation.

Returning to the mesh network in Figure 43, look at bridge B3: if the WAN lines are all 19.2 kbps and the links are directly connected with a single SVC hop, then their incremental cost for WAN links can be set to STPE Path Cost = 3536. Therefore, B3 will see messages from other bridge links resulting in the following cost to the root bridge:

- From bridge 1 link 6: root is bridge 1, cost to root = 3536
- From bridge 4 link 8: root is bridge 1, cost to root = 7072 (3536+3536)
- From bridge 5 link 9: root is bridge 1, cost to root = 14154 (3536+10+3536+3536+3536)

Based on these numbers, B3 determines B1 to be the root bridge, because B1's bridge ID is lower than all reported root bridges (including B3's own bridge ID). B3 also designates bridge link 6 as the root link since it has the least cost to the root.

Consider the Nature and Expected Number of SVCs

A further consideration for setting path cost is the nature and expected number of SVCs that the bridge link uses to achieve its connectivity and adjust the value of incremental path cost accordingly. For example, consider the topology shown in Figure 45.

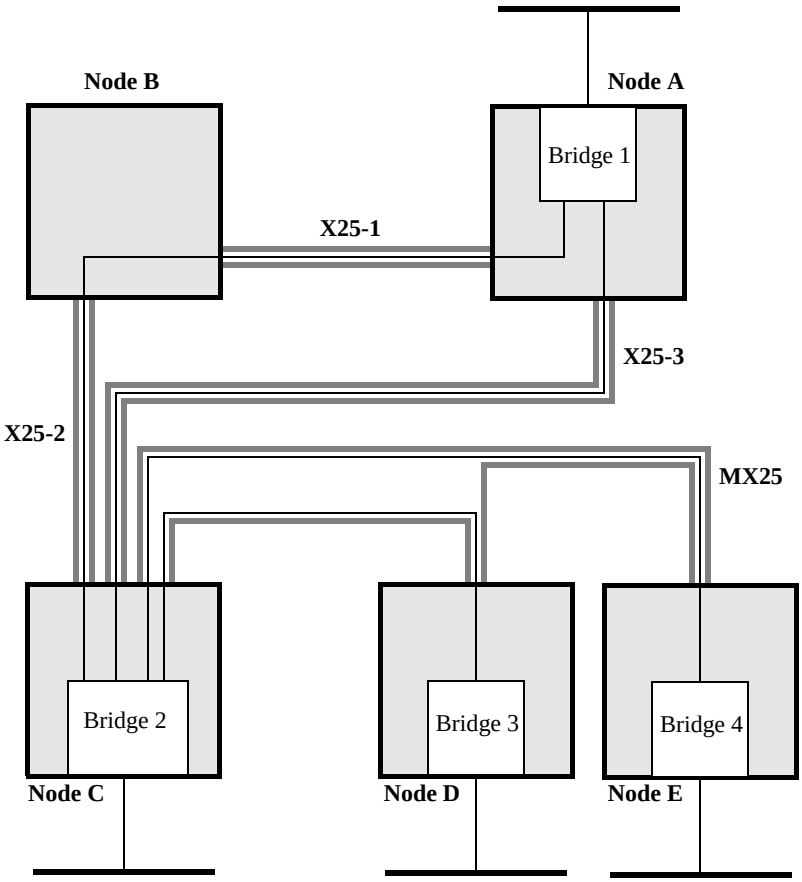


Figure 45. Bridge Links Within Network

Bridge 2 is linked to bridge 1 by two separate links. The link through Node B must traverse two separate SVC hops while the direct link has only a single hop. If the speed of the lines are all equal, then the cost for the bridge link through Node B should be higher than the cost for the direct link.

On the other hand, if the amount of traffic (due to sources other than bridging traffic) causes added delay for the direct route, or if the direct route has a lower speed, it might be better to use the direct route as a backup. Therefore one would set the cost for the direct route higher than for the Node B route. For the multipoint line connecting bridges 2, 3, and 4, the cost for each link should be increased in proportion to the amount of bandwidth-sharing involved. This also accounts for the fact that a slave node such as Node D or Node E must wait to be polled before it can pass data to its master, thus adding some extra delay.

Other Considerations for Selecting Links

There are two final considerations when selecting links on the basis of reported cost, when the costs and indicated root bridge on different links are the same. The first is the case where, for example, B4 receives a message on link 8 from B3 designating B1 as the root bridge with a cost of 10608 to the root. At the same time, B4 receives a message on link 8 from B2 designating B1 as the root bridge with a cost of 7072. In this case, B4 will select link 7 as the root link because the spanning tree algorithm dictates that if more than one message has the same root bridge indicated, at the same cost to the root, then the message with the higher priority-reporting adjacent should be given priority. In this case, B2 has been configured to have a higher priority (lower Bridge ID) than B3, so B4 selects link 7 as its root link.

The second consideration occurs when two links on the same bridge are receiving messages from the same adjacent bridge, and the messages report the same root bridge and the same cost to the root bridge. This could occur if there were two links between B3 and B4. The bridge will choose the link with the lower bridge link priority. The priority for the link is a 2-byte number formed by concatenating the value of the parameter STPE Priority with the link number.

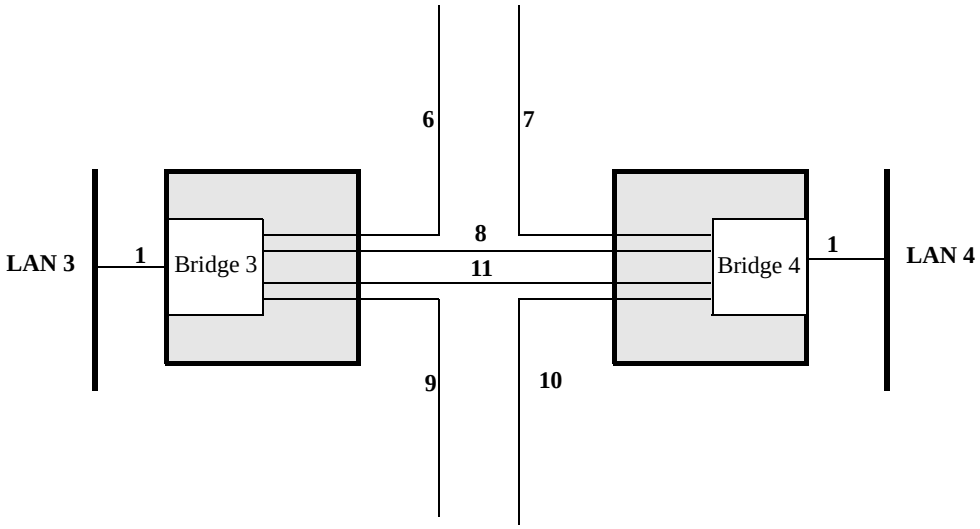


Figure 46. Two Bridge Links Between B3 and B4

For example, B3 sends messages to B4 that the root bridge is B1, and that the cost to the root is 10608 (3536+3536). To cause bridge 4 to favor link 11 over link 8, configure:

link 8: STPE Priority = 128 (80 hex)

link 11: STPE Priority = 64 (40 hex)

In this example, should a link between bridge 3 and bridge 4 be necessary for a spanning tree, bridge 4 will favor link 11 and remove link 8 from the tree.

The same priority mechanisms that determine the root link are also applied in determining which links become designated links (a root link is never a designated link). The designated link is the link that is responsible for issuing the bridge messages when more than one link is involved in a network. For example, in the network in Figure 43, Bridge 5 and bridge 6 are connected to LAN 5 and will both issue each other spanning tree messages until they determine which one of them is the designated bridge for LAN 5. Once determined, the designated bridge issues bridge messages and the other bridge only listens (unless it has received another message from another link that would make its link the designated bridge; such a message must have higher priority than the one it receives from its designated adjacent). Another case where there is contention and resolution to a designated bridge is link 8 between bridge 3 and bridge 4.

To determine which link becomes designated, the same set of priority parameters are used as in determining the root link. In this case, the designated link is the link issuing the message that:

- Identifies the root bridge with the lowest numerical bridge ID
- Has the lowest cost to the root (assuming there is a tie in reporting the root bridge)
- Identifies itself with a higher priority ID (assuming there is a tie in reporting the root bridge and the cost to the root bridge)
- Has the higher priority link (assuming all of the above are tied)

In this network, bridge 5 link 1 is the designated link for LAN 5 because between bridge 5 link 1 and bridge 6 link 1, bridge 5 link 1 generates a message with a lower cost to the root than bridge 6 link 1 (they both have the same root). Between bridge 3 and bridge 4 on link 8, bridge 3 link 8 becomes the designated link because it has a lower cost to the link.

Links that are not root links or are not designated links are not part of the spanning tree. Links that are not on the spanning tree do not forward data packets (or spanning tree explorer frames in source route bridging). However, they are constantly receiving bridge messages on these links from the designated bridges and comparing these messages to those they originate. This action allows the bridge to detect failures and adjust the spanning tree, should this become necessary.

Spanning Tree Timers

Introduction

If the spanning tree converges to a final topology (it usually does, but misconfiguration as discussed below can cause instability and lack of convergence), the topology is maintained by timed messages initiated by the root bridge and sent out its designated links. Subsequently, bridges receive the message on their root link and in turn pass the message along the spanning tree by transmitting it on their designated links.

Timer Parameters

The root bridge message has timer parameter values that all bridges should copy and use. These timers are:

- Message Age
- Max Age (Bridge Parameters Record)
- Hello Time (Bridge Parameters Record)
- Forward Delay (Bridge Parameters Record)

Notice that the last three are parameters configured for each bridge. Once the root bridge is determined, however, all the other bridges use the value in the root bridge initiated message rather than their own configured values. The Max Age and Hello Time are the two principal timers used by the spanning tree protocol for detecting a fault condition.

When selecting values to configure these two parameters, consider the fact that the bridge network is, when X.25 WAN circuits are used, overlaid onto an underlying network which has its own timers and recovery procedures. It is important that the two networks do not interfere with each other’s protocols, especially where timer considerations are involved.

Hello Timer

Hello messages are sent by the Root Bridge at specific time intervals. These intervals are determined by the Hello Timer parameter configured in the Bridge Parameters record.

If the bridges in the network receive these Hello messages, then this indicates to the bridges that the Root Bridge is functioning and the path from the bridge to the Root Bridge is functional as well.

If a bridge does not receive a Hello message from the Root Bridge within the time allowed by the Max Age Timer parameter, then that bridge begins the process of recalculating the spanning tree for the network.

Max Age

The Max Age is a configurable parameter on the Bridge Parameters Record. This parameter indicates to a bridge when to discard information about the Root Bridge and the link to the Root Bridge.

Other Considerations

One important consideration is based on the fact that any bridge downstream from the root bridge copies the message received on the root link (which is also passed along designated links), and the retained copy is constantly aged. If the age of the message reaches the value of Max Age, the bridge discards the stored message and chooses another link as the root link. Potentially this could result in a different bridge selected as the root bridge and in turn cause it to recalculate the root, root link, and designated links (recalculate the spanning tree). Since the root port generates the update message every Hello Time period (in seconds), it is obvious that the parameter Max Age should not have a value less than or in fact near the value of Hello Time. The spanning tree protocol (IEEE 802.1D) dictates that a bridge should enforce the following relationship:

Max Age >= 2 x (Hello Time - 1)

In the PathBuilder S200 series switch this rule is not strictly enforced by CTP configuration checks. You should check that the values are satisfactory for the operational environment. The Max Age range of values is 6 to 40 and the default is 20. The Hello Time range of values is 1 to 4 and the default is 2 seconds.
These values allow the enforcement of timer relationships for any reasonable choice of values. The factor of two between Max Age and Hello Time allows one of the hello messages to be lost due to, for example, congestion.

In general, increasing the value of Max Age lessens the chance of a false timeout due to a delay of the hello message. When bridge traffic must compete with other traffic on WAN links, setting this value can become an important consideration. On the other hand, beyond a certain point, a large value for Max Age may cause the detection of a true fault to be prolonged beyond what is desired. The Hello Time should be considered similarly:

- Too low a value causes frequent transmission of the message, resulting in network overhead.
- Too long an interval between transmissions forces a longer Max Age which results in lack of responsiveness to failure situations.

In spite of the overhead, a short Hello Time helps in cases where the message might be inadvertently lost in the network (not likely) or where a short convergence time for the spanning tree is desired.

Bridge Forward Delay Timer

Forward Delay

For transparent bridges the bridge Forward Delay is used to allow the spanning tree algorithm to converge to a stable topology before the bridging process is allowed to proceed. Spanning tree topology determination is an iterative process and requires time to converge. The bridge should not forward packets during this time because temporary loops might cause forwarded packets to be exponentially duplicated and disable the network. Once the topology has stabilized, the bridge should not forward packets immediately since, initially, it will not have learned station locations and will have to broadcast packets when it does not find the entry in its local station cache. Once the bridge has built up its cache by listening for a short period of time, it can forward packets directly, rather than using high overhead broadcasts.

The Forward Delay is used twice: once to allow the topology to stabilize and during this time to process only spanning tree protocol messages; and then again to allow the bridge to learn station locations, during which time data packets are received but not forwarded.

To understand how long it takes to converge a spanning tree, consider the following simplified network shown in Figure 47, together with the message events shown as a timed sequence below the network:

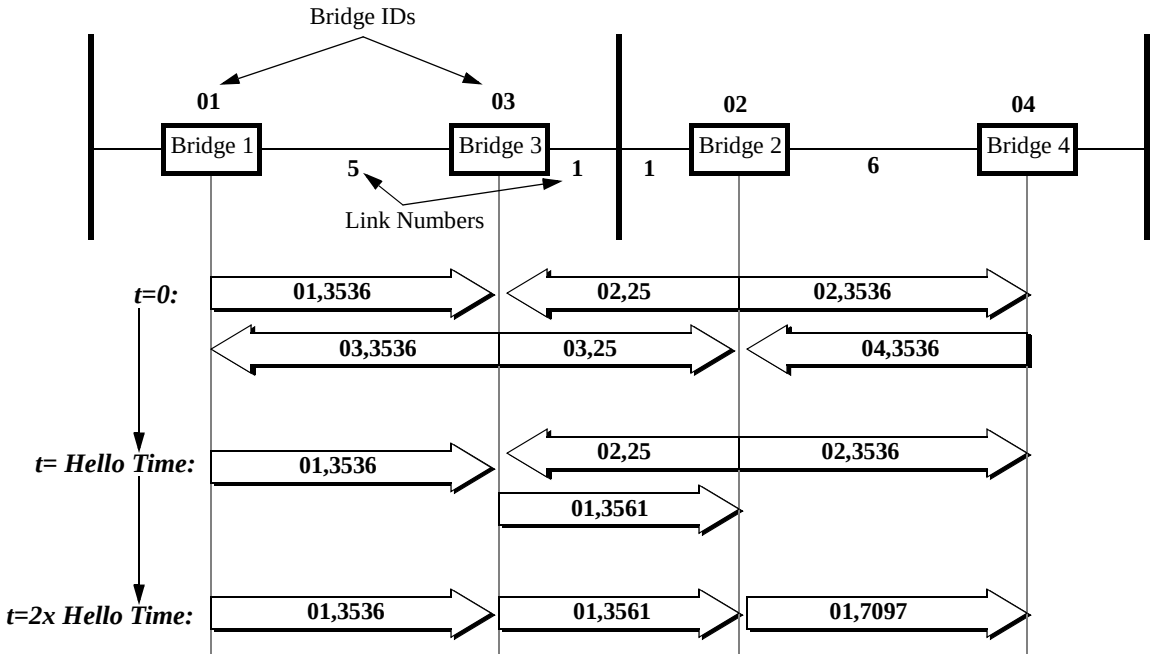


Figure 47. Message Events in Network

Suppose all bridges come up at the same time. Initially, at t=0, all bridges think they are the root and they issue the messages shown on the t=0 line. For simplicity, the bridge ID is a two digit number and the couplet such as 01,3561 should be interpreted as: root_ID, cost_to_root. The messages sent to the LAN attached to B1 and B4 are irrelevant to this discussion and are not shown.

At the end of this first iteration, after the bridges have compared messages sent and received on the various links, they conclude the following:

- B1 will continue to see itself as the root bridge. Its link 5 and link 1 (to the LAN, not shown) will be set as designated links.
- B2 will continue to see itself as the root bridge temporarily. Its link 1 and link 6 will be set as designated links.
- B3 will determine B1 as the root bridge. Its link 5 is its root link and its link 1 is a designated link.
- B4 will temporarily see B2 as the root bridge. Its link 6 is its root link and its link 1 (not shown) is a designated link.

At t = Hello Time, the root bridges issue the spanning tree hello message. After the bridges have compared the new messages, they form the following conclusion:

- B1 will continue to see itself as the root bridge. Its link 5 and link 1 will be set as designated links.
- B2 will determine B1 as the root bridge. Its link 1 will be the root link and link 6 will be set as a designated link.
- B3 will determine B1 as the root bridge. Its link 5 is its root link and its link 1 is a designated link.
- B4 will temporarily still see B2 as the root bridge. Its link 6 is its root link and its link 1 is a designated link.

At t = 2 x Hello Time, there is only one root bridge B1 to issue the spanning tree hello message. This message is passed along the tree and, at this iteration, B4 finally sees B1 as the root bridge, and the spanning tree has converged.

From this example, it is seen that the convergence time is dependent on how many link hops the farthest bridge is from the root bridge and how frequently the hello message is sent. Until the bridges converge, no bridge should learn station locations (nor forward data frames); therefore, the forward delay (the time the bridge should wait before learning), should be set to a value that might be at least as high as the hello time multiplied by the network diameter. With special consideration this time might be considerably reduced. For example, in the preceding network, if B2 and B3 are interchanged, the spanning tree will converge at t = Hello Time (half the time of the original network).

Note

The Forward Delay time is used a second time to allow the bridge to learn station locations before allowing the bridge to forward frames.

When the spanning tree is configured for manual operation, no spanning tree protocol needs to converge, but the station locations still must be learned.
For manual operation, a different timer is used only for setting the Learn Only Period. This timer is used by the bridge to set the time it will learn only after the bridge has booted.

Aging Timer

The Aging Timer is a configurable parameter found in the Bridge Parameters Record. It allows learned station addresses to be aged in the station address cache and deleted once their age has reached the value of the Aging Timer parameter. This allows automatic updates for certain dynamic conditions, such as when a station is physically moved from one part of the network to another. Provided the Aging Timer is low enough to age out the station that is being moved, the entry is deleted and, once the station becomes active at its new location, the bridge relearns its new location and forwards packets to it properly.

The Aging Timer is also used when there is a topological change to the network. Generally, if a bridge, based on the automatic spanning tree algorithm, notices that a link must be moved to or from a block state (moved to or from the spanning tree), then the bridge informs the root bridge by means of a special message sent out the root port. This message includes a flag that indicates a topological change has occurred. The root bridge, in turn, informs all the bridges in the network that a change has occurred by setting a flag in the hello message. Once a bridge is informed of a change in the topology by the hello flag, it switches the timer value used in aging to a value equal to the Forward Delay time. This allows the bridge to more quickly relearn new station locations, if a topology change occurs due to node or link failures. Note that the topological change messages are sent at the same rate as the Hello Time interval. This limits the speed and gives the lower time boundary so that bridges can adjust to the change.

LLC2 Local Termination

LLC2 Local Termination

LLC2 Local Termination lets specific Token Ring ports generate and respond to LLC2 polls with local acknowledgments, thereby preserving bandwidth and preventing session timeouts in a Bridging application.

Local Termination, also referred to as “spoofing,” provides an efficient means for carrying out an LLC2 session between two SNA end stations attached to separate Token Ring LANs connected by a Wide Area Network (WAN).

Additionally, Local Termination provides detailed statistics on LLC2 sessions.

LT Example

For example, Figure 48 shows a network where running LLC2 Local Termination at the edge point PathBuilder S24x, 26x, and 27x switches enables spoofing from one side of the network to the other across multiple Token Rings.

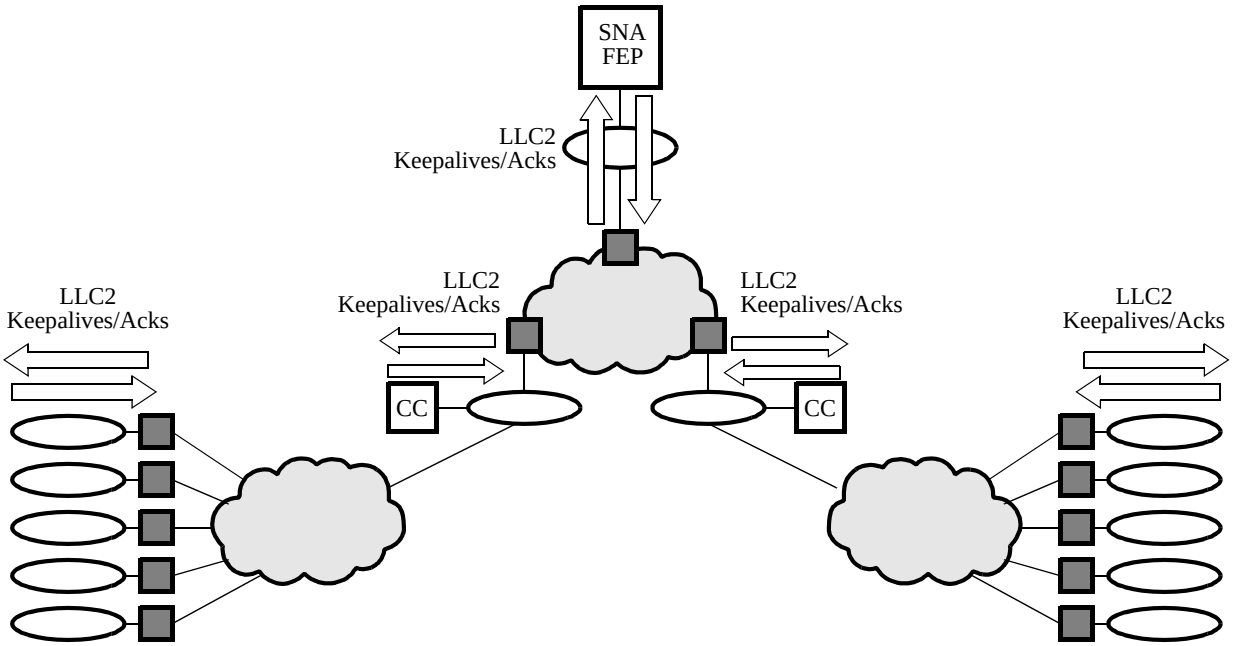


Figure 48. Local Termination Example

Before Local Termination

Without Local Termination, networks face significant problems with bandwidth usage and session timeouts due to polling overhead between the host and terminal, as well as network delays.

For example, Figure 49 shows a terminal session on a source route bridged Token Ring LAN connected to a host without Local Termination. During the terminal session, LLC2 polls, such as ACKs and keepalives, are exchanged between the host and the terminal session, causing:

- Inefficient use of the WAN bandwidth
- Increased session timeouts
- Ongoing tuning of network parameters to fix session timeouts

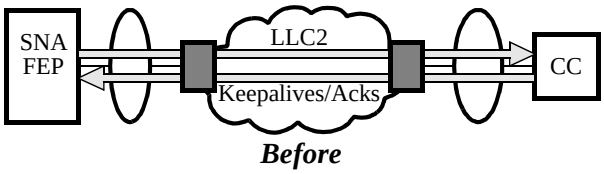


Figure 49. Before Local Termination Example

You can increase timer values to reduce the number of session timeouts experienced on a network, but configuring large numbers of stations makes such a solution impractical. Moreover, it does not solve the problem with “keepalives” slowing down network traffic.

After Local Termination

The best solution to such network traffic problems is to locally terminate the LLC2 session at the Token Ring interface, as shown in Figure 50.

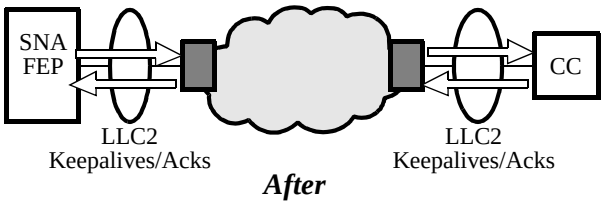


Figure 50. After Local Termination Example

Using LLC2 LT, you can spoof traffic on a Token Ring LAN, reducing the polling overhead by minimizing session timeouts. Ack and “keepalive” messages traverse the network between spoofers; they are controlled in frequency by the WAN parameters.

Supported Topologies

Local Termination is supported only on Token Ring topologies configured for Source Route Bridging. And there are two important guidelines to remember when you are planning your Local Termination strategy:

- When you turn on Local Termination in your network, the MAC address/SAP value you assign is always locally terminated.
- You must have a PathBuilder S200 series switch running Local Termination positioned at both ends of your network to provide spoofing from one edge point to another.

Improper LT Configuration

For example, Figure 51 shows a Token Ring network improperly configured for Local Termination.

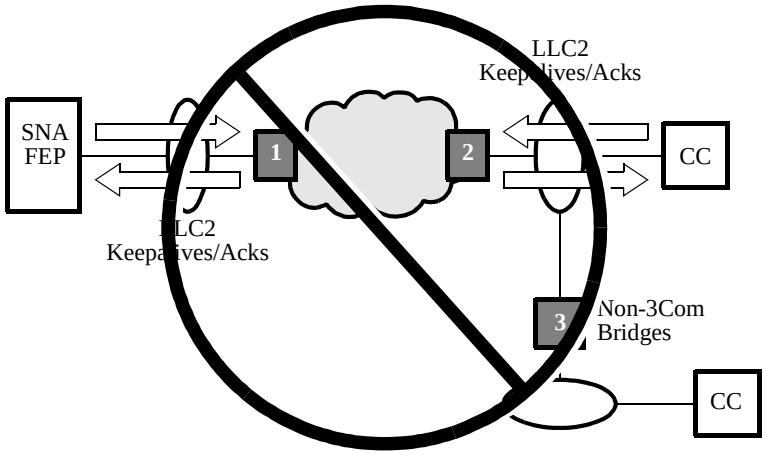


Figure 51. Example of Improper LT Configuration

The cluster controller (CC) using non-PathBuilder S200 series switch bridge 3 in Figure 51 is source route bridged to the FEP. The local PathBuilder S200 series switch, bridge 1, at the FEP use location tries to locally terminate the session since all frames bearing the MAC address of the FEP are to be spoofed. However, the non-PathBuilder S200 series switch bridged cluster controller will never come up unless Local Termination is disabled entirely. The cluster controller on PathBuilder S200 series switch bridge 2 will come up because it runs Local Termination. PathBuilder S200 series switch bridge 2 is unable to spoof traffic unless it originates from its own Token Ring. For spoofing to work, you must use PathBuilder S200 series switches with Local Termination enabled at the network's edge points.

Proper LT configuration

Figure 52 shows a Token Ring LAN properly configured for Local Termination.

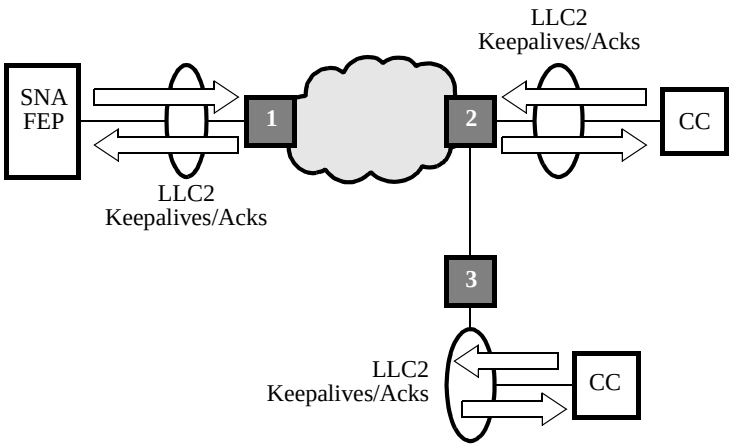


Figure 52. Example of Proper LT Configuration

Local Termination running on PathBuilder S200 series switch bridges 1, 2, and 3 at the edge points of the network provide a simple solution to congestion and bandwidth problems across the entire network.

LLC Protocol

LLC is a link layer protocol used in IBM environments and defined in the IEEE802.2 LAN model. Its function is to establish, maintain, and terminate the logical link between adjacent stations in a network.

LLC Frame Description

There are three types of LLC operations:

Type	*Name*	*Description*
Type 1	LLC1	Unacknowledged, connectionless services
Type 2	LLC2	Connection-oriented services
Type 3	LLC3	Acknowledged, connectionless services

LLC2 Frame Description

Logical Link Control 2 (LLC2) is a connection-oriented, acknowledged protocol. LLC2 requires a connection setup between two LAN devices. LLC2 is based on the HDLC protocol and is used to transport SNA traffic, as well as other protocols.

Spoofing

Local termination or “spoofing” of LLC protocol means that acknowledgments to information frames and certain supervisory frames are handled locally by the spoofer. The spoofer, the LT software in a PathBuilder S200 series switch, ensures the acknowledged information frames are reliably delivered to the destination peer spoofer and that any flow control issues are handled appropriately. Because of local acknowledgment, spoofing of LLC frames may enhance network performance and allows for reliable Token Ring to Token Ring connectivity.

This table describes the types of frames Local Termination spoofs:

Local Termination spoofs:
All Specifically Routed LLC frames, such as I frames and Supervisory frames
Local Termination does not spoof:
• Route Explorer frames, such as ARE or STE • Internally matched frames coming in from the LAN port • Frames generated by LSS/LLC in the bridge going out to the LAN port • WAN to WAN frames

Maximum Sessions Spoofed

The maximum number of sessions you can spoof at one time is 64. If you reach the maximum number of sessions, Local Termination does not establish additional spoofing sessions, nor does it source route bridge the additional sessions.

What Happens between Spoofers

Local Termination runs a subset of LLC2 protocol between spoofers to ensure that frame traffic reliably passes from one edge point node to another edge point node in your network. The subset protocol uses separate timers and retry counts that can be set greater than the LLC protocol timers.

Intermediate Frames between Spoofers

LLC2 LT supports intermediate Token Ring networks between spoofers. For example, Figure 53 shows Local Termination running in the edge point nodes of this network to provide “spoofing” across multiple Token Rings.

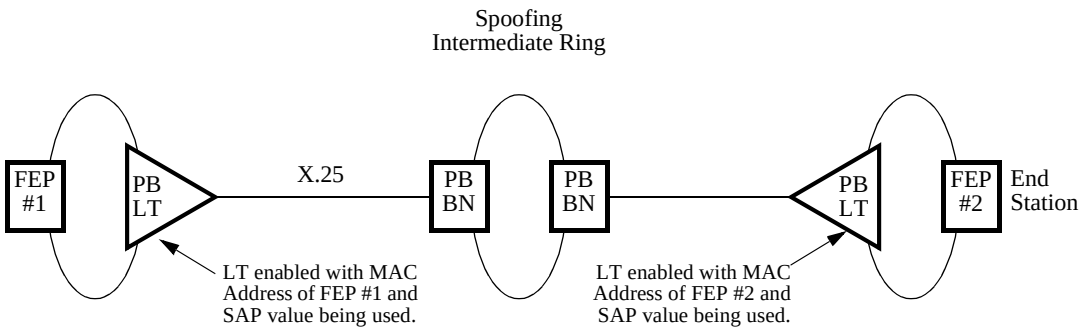


Figure 53. Example of LT Spoofing

Traffic Priority & Local Termination

You can significantly optimize your spoofing operations by prioritizing Local Termination traffic and regular bridge traffic. By assigning a separate lower priority to spoofer traffic, the regular bridge traffic is queued quicker. The extra delay of spoofer traffic does not affect the acknowledgments of frames on the LAN.

See ““Configuring Local Termination” section on page 106” for details on setting the LLC LT WAN Data Priority parameter record.

Configuring Local Termination

Configuring for Local Termination

Perform the following procedures to configure Local Termination on a Bridge node.

Step	Action
1	Configure the node.
2	Configure the ports.
3	Configure the route selection table.
4	Configure the LAN connection table.
5	Configure the Mnemonic Table and PVC Setup table.
6	Configure the bridge for Local Termination. Go to ““Configuring the Bridge” section on page 106”, for details on configuring the bridge table for Local Termination.

Before You Begin

Connect to the node using Control Terminal Port (CTP) access.

Obtain the following information:

- MAC Address of the device being spoofed.
- SAP value of the device being spoofed.

Configuring the Bridge

Follow these steps to configure bridge parameters to enable Local Termination on a node.

Step	Action	Result
1	Select **Configure -> Configure Bridge** from the Main menu. ■ **Note** Bridge must be configured for source routing. (*Bridge Type=SR).	The Configure Bridge Record menu appears.

Step	Action (continued)	Result
2	Configure all of these LT configuration options. Choose one to begin.	
	• LLC LT Station Table Then: Go to “Configuring the LT Station Table” for details.	LLC LT Station Table Configuration appears.
	• LLC LT WAN Parameters Then: Go to the section “Configuring the LT WAN Parameters."	LLC LT WAN Configuration appears.
	• LLC LT Profile Table Then: Go to the section “LLC LT Profile Table Configuration.”	LLC LT Profile Table Configuration appears.

Configuring the LT Station Table

These parameters make up the LT Station Table.

Entry Number

Range:	1 to 64 stations
Default:	1
Description:	Entry number used to reference this table.
Boot Type:	N/A

Local MAC Address

Range:	00:00:00:00:00:01 to 7F:FF:FF:FF:FF:FF
Default:	00:00:00:00:00:80
Description:	MAC address must match the source MAC address of the frame received from the LAN port or the destination MAC address of a frame received from the WAN for the session to be spoofed. If you are using Local Termination Autolearn, specify the remote MAC address.
Boot Type:	LLC LT Station

Local SAP

Range:	01 to FE (hexadecimal)
Default:	04
Description:	This SAP must match the source SAP of the frame received from the LAN port for the session to be spoofed. If you are using Local Termination Autolearn, specify the remote Host SAP for the local MAC.
Boot Type:	LLC LT Station

LLC Profile Name

Range:	0 to 8 (alphanumeric, space blanks field)
Default:	(Blank)
Description:	Local Term Station Table references this parameter for the T1, T2, TI, N2, N3, and TW values. If no profile name is specified, then default values are used.
Boot Type:	LLC LT Station

Configuring the LT WAN Parameters

These parameters make up the LT WAN Parameters Table.

T1Reply Timer

Range:	1 to 25 (seconds)
Default:	3
Description:	This Ack timer is used by a station to detect a failure of the remote station to acknowledge an outstanding I frame or supervisory frame with the pole bit set to 1.
Boot Type:	LLC LT WAN Parameters.

T2 Rx Ack Timer

Range:	1 to 255 (tenths of seconds)
Default:	1
Description:	The Receive Ack timer is used by a station to determine how long it will withhold acknowledgment of a frame from the remote station that requires acknowledgment. This is a method of reducing the amount of acknowledgments generated by a link station. When this timer expires, the link station should immediately send an acknowledgment for all received frames not yet acknowledged.

T2 Rx Ack Timer *(continued)*

Boot Type:	LLC LT WAN Parameters.

Ti Inactivity Timer

Range:	2 to 255 (seconds)
Default:	30
Description:	The Idle Timer is used by a station to detect an inoperative condition of the logical link. This timer is started when the link becomes idle (no data to pass and no outstanding acknowledgments) and if it expires, the station sends a supervisory frame with the pole bits set to 1.
Boot Type:	LLC LT WAN Parameters.

N2 Retry Count

Range:	1 to 20
Default:	8
Description:	This count defines the number of times an I frame or supervisory frame with pole bits set to 1 will be transmitted due to T1 acknowledgment timeout before the logical link will be declared down (inoperative).
Boot Type:	LLC LT WAN Parameters.

N3 ACK Delay Count

Range:	1 to 15
Default:	3
Description:	The Receive Count is used with T2 to reduce the number of acknowledgments a station generates. The receive count is used by a station to determine how many frames it receives from the remote station while withholding acknowledgment of these frames. This reduces the number of acknowledgments generated by a link station. When this count expires, the link station immediately sends an acknowledgment for all received frames not yet acknowledged.
Boot Type: :	LLC LT WAN Parameters.

Tx Window Size

Range:	1 to 15
Default:	7
Description:	Transmit window size is the maximum number of I frames a station may transmit without acknowledgment.
Boot Type:	Node Boot

LCC LT WAN Data Priority

Range:	HIGH, MEDIUM, LOW
Default:	HIGH
Description:	Specifies the transmission priority of the LLC LT data.
Boot Type:	LLC LT WAN Parameters.

LLC LT Profile Table Configuration

These parameters make up the LLC LT Profile Table.

Entry Number

Range:	1 to 8
Default:	1
Description:	Entry number used to reference this table record.
Boot Type:	N/A

LCC Profile Name

Range:	0 to 8 (alphanumeric, space blanks field)
Default:	(blank)
Description:	Local Term Station Table references this parameter for the T1, T2, TI, N2, N3, and TW values.
Boot Type:	Tables and Node Record.

T1 Reply Timer

Range:	1 to 25 (seconds)
Default:	1
Description:	This Ack timer is used by a station to detect a failure of the remote station to acknowledge an outstanding I frame or supervisory frame with the pole bit set to 1.
Boot Type:	Tables and Node Record.

T2 Rx ACK Timer

Range:	1 to 255 (tenths of seconds)
Default:	1
Description:	Specifies how long the station withholds acknowledgment of a frame from the remote station that requires acknowledgment. This reduces the number of acknowledgments generated by a link station. When the timer expires, the link station immediately sends an acknowledgment for all received frames not yet acknowledged.
Boot Type:	Tables and Node Record.

Ti Inactivity Timer

Range:	2 to 255 (seconds)
Default:	30
Description:	The Idle Timer is used by a station to detect an inoperative condition of the logical link. This timer starts when the link is idle (no data to pass and no outstanding acknowledgments). When the timer, expires, the station sends a supervisory frame with the poll bit set to 1.
Boot Type:	Tables and Node Record.

N2 Retry Count

Range:	1 to 20
Default:	8
Description:	Specifies the number of times an I frame or supervisory frame with poll bit set to 1 is transmitted due to T1 acknowledgment timeout before the logical link is declared down (inoperative).
Boot Type:	Tables and Node Record.

N3 ACK Delay Count

Range:	1 to 15
Default:	3
Description:	The Receive Count is used with T2 to reduce the number of acknowledgments a station generates. The receive count is used by a station to determine how many frames it receives from the remote station while withholding acknowledgment of these frames. This reduces the number of acknowledgments generated by a link station. When this counter expires, the link station immediately sends an acknowledgment for all received frames not yet acknowledged.
Boot Type:	Tables and Node Record.

Tx Window Size

Range:	1 to 15
Default:	7
Description:	Specifies the maximum number of I frames a station may transmit without acknowledgment.
Boot Type:	Tables and Node Record.

Deleting LT Configuration Records

Overview

You can delete the following LLC2 LT configuration records if you no longer use them:

- LT Station Table
- LT Profile Table

Before You Begin

Choose **List Bridge** from the CTP Main menu to obtain a list of the configured LT session records.

Procedure

This procedure describes how to delete LT session configuration records.

Step	*Action*	*Result*
1	Select **Delete Record**, from the CTP Main menu, and press Return.	The Delete Record menu appears.
2	Select **Delete Bridge** from the Delete Record menu.	The Delete Bridge menu appears.
3	Select • LLC LT Station Table Entry. Or: • LLC LT Profile Table Entry	Entry number: 1/ appears.
4	Press Return to delete entry number 1 or type in another entry number.	Proceed (Y/N): appears.
5	Type **Y** to delete the entry.	Record Deleted appears.

Mixed LAN Operation

Overview

PathBuilder S24x, 26x, and 27x switches support a mixture of Token Ring and Ethernet interfaces configured on the same node. This means the PathBuilder S24x, 26x, and 27x switch is able to perform remote Transparent bridging for Ethernet LANs and remote Source Route Bridging from the same PathBuilder S24x, 26x, and 27x switch, as shown in Figure 54.

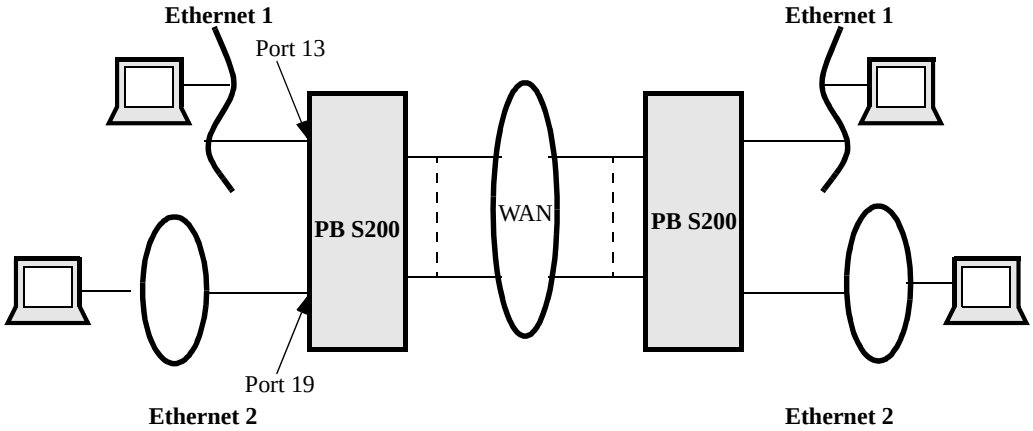


Figure 54. Example of Mixed LAN Bridging in PathBuilder S24x, 26x, and 27x Switch

Mixed LAN Environment Limitations

These limitations apply when you perform Mixed LAN bridging in a PathBuilder S24x, 26x, and 27x switch:

- The PathBuilder S24x, 26x, and 27x switch is limited to only one Spanning Tree Entity (SPTE) per node. If you perform automatic spanning tree in a Mixed LAN implementation, SPTE may prohibit traffic from passing between LANs by blocking some bridge links to avoid bridge looping.
- You must install Release 4.90 or above operating software on all PathBuilder S24x, 26x, and 27x switches in your network to perform Mixed LAN operation on any node in the network. If you have a mixture of nodes running earlier operating software releases, mixed LAN operation will cause node crashes. A PathBuilder S24x, 26x, and 27x switch used as a router and configured for Mixed LAN operation is not impacted by this limitation.

Steps to Configure Mixed LAN Bridging Operation

To perform mixed LAN bridging operation in a PathBuilder S24x, 26x, and 27x switch, configure a unique bridge link and router interface number for each LAN interface from the Port record. You must also configure the WAN bridge link to support Transparent Bridging and Source Route Bridging.

Follow these steps to configure Mixed LAN Bridging, as shown in Figure 54.

Step	Action	Result/Description
1	Make a local CTP connection to a PathBuilder S24x, 26x, and 27x switch.	The CTP is physically connected to the device you are configuring.
2	Select **Configure -> Port**. from the CTP Main menu.	The Port record appears.
3	Configure the Port record as you normally do for an Ethernet LAN connection.	Two new parameters, **Bridge Link Number** and **Router Interface**, appear in the record.
4	At the Bridge Link Number: parameter, type in a number **1-4** to identify the bridge link, and press Return. For example, you can configure the Ethernet port as bridge link #1. **Note** The default value for this parameter is 1.	This matches this port configuration to a specific bridge link number within the bridging configuration. If the bridge link you select is already used, a warning message appears, but your input is retained in the CMEM.
5	At the Router Interface Number: parameter, type in a number 1-4 to identity the router interface. For example, you can configure the Ethernet port as router interface #1. The default value for this parameter is 1.	This matches this port configuration to a router link number within the router configuration. If the router interface number you select is already used, a warning message appears, but your input is retained in the CMEM.
6	Type**;** and press Return to save the record.	This saves the record.
7	Perform a Node boot from the Boot menu.	This implements your changes, but if you want the new bridge link to be active, you must configure the Bridge Link record under the Configure Bridge menu. Go to the following step. By default, the bridge link is not activated until you activate it.
8	Select **Configure Bridge -> Bridge Link Parameters** from the CTP Main menu, to activate the bridge link.	The Bridge Link Parameters menu appears.

Step	***Action*** *(continued)*	***Result/Description***
9	Type **;** and press Return.	The record is saved.
10	Perform a Bridge Link boot from the Boot menu.	This enables the bridge link.
11	Configure the WAN bridge link to support Transparent Bridging and Source Route Bridging. Select Bridge Link Parameters and type in a WAN entry number from 5 to 36 to display the Bridge_Type parameter. Enter the string **BOTH_SR_AND_TB**.	This enables TB and SR on the WAN link.
12	Type **;** and press Return.	The record is saved.
13	Perform a Node boot to implement your changes.	Your changes are implemented.

■ Note

Duplicate bridge link or router interface numbers results in only the lowest numbered port being initialized.

Statistics

Bridge link statistics for the WAN bridge link show the status of Mixed LAN links as **Both TB and SRB Active** when the WAN bridge link is configured as BOTH_SR_AND_TB, and the Ethernet port successfully initialized.

The statistics screen displays information on both the Transparent Bridging operation and the Source Route Bridging operation on the WAN link. If the node is booted with only one port configured or active, then the statistics screen displays **TB Active** or **SR Active** only.

IP and IPX Support

A PathBuilder S24x, 26x, and 27x switch performing a Mixed LAN operation supports IP and IPX routing of traffic with no additional configuration needed.

Dual LAN Ethernet

What Is It?

The Dual LAN Ethernet feature lets your PathBuilder S24x, 26x, and 27x switch support up to two Ethernet LAN interfaces to perform bridging and routing of LAN traffic across multiple LANs.

Before Multiple Ethernet LAN, the PathBuilder S24x, 26x, and 27x switch supported only one Ethernet LAN port for remote bridging and routing of LAN traffic. However, with the Multiple Ethernet LAN feature, you can bridge and route LAN traffic locally and remotely using up to two LAN ports on each PathBuilder S24x, 26x, and 27x switch, as shown in Figure 55.

Note

It is recommended that you configure the first LAN card in your device as Bridge Link Number 1 or Router Interface Number 1. Failure to do so may cause your device to perform continuous resets when you power up the device after reinstalling an earlier release of operating software.

Sample Application

Figure 55 shows a sample application for the Multiple Ethernet LAN feature.

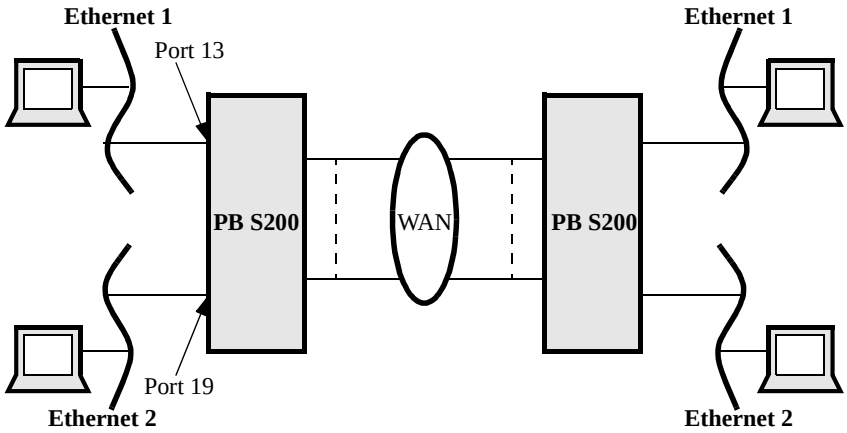


Figure 55. Example of Multiple Ethernet LAN

Limitations

The PathBuilder S24x, 26x, and 27x switch supports only two Ethernet LAN ports at one time. If you configure more than two Ethernet ports on a PathBuilder S24x, 26x, and 27x switch, the system initializes only the first two ports you configure during system powerup.

Bridging

In a Transparent Bridging environment, if you connect both Ethernet LAN ports to the same Ethernet segment, you must enable Spanning Tree. Failure to enable Spanning Tree in this configuration is a violation of the rules of Transparent Bridging.

Routing

In IP/IPX or AppleTalk routing environments, do not connect both Ethernet LAN ports to the same Ethernet segment with identical routing decision values. This is not supported.

How to Configure Dual Ethernet LAN

Follow these steps to configure a node for Multiple Ethernet LAN.

Step	Action	Result/Description
1	Make a local CTP connection to a PathBuilder S24x, 26x, and 27x switch.	The CTP is physically connected to the device you are configuring.
2	Select **Configure -> Port** from the CTP Main menu.	The Port record appears.
3	Configure the Port record as you normally do for an Ethernet LAN connection.	Two new parameters, Bridge Link Number and Router Interface, appear in the record.
4	At the Bridge Link Number: parameter, type in a number **1-4** to identify the bridge link, and press Return. **Note** The default value for this parameter is 1.	This matches this port configuration to a specific bridge link number within the bridging configuration. If the bridge link you select is already used, a warning message appears, but your input is retained in the CMEM.
5	At the Router Interface Number: parameter, type in a number 1-4 to identity the router interface. **Note** The default value for this parameter is 1.	This matches this port configuration to a router link number within the router configuration. If the router interface number you select is already used, a warning message appears, but your input is retained in the CMEM.
6	Type**;** and press Return to save the record.	This saves the record.
7	Perform a Node boot from the Boot menu.	This implements your changes, but if you want the new bridge link to be active, you must configure the Bridge Link record under the Configure Bridge menu. Go to the following step. By default, the bridge link is not activated until you activate it.
8	Select **Configure Bridge -> Bridge Link Parameters** from the CTP Main menu, to activate the bridge link.	The Bridge Link Parameters menu appears.
9	Type **;** and press Return.	The record is saved.

Step	***Action*** *(continued)*	***Result/Description***
10	Perform a Bridge Link boot from the Boot menu.	This enables the bridge link.

For Details on Parameters...

See the *PathBuilder S200 Series Basic Protocols* for details on Ethernet LAN port parameters for Multiple LAN Ethernet operation.

LAN Server Subsystem

What is It?

The LAN Server Subsystem (LSS) software lets PathBuilder S200 series switches such as the PathBuilder S200 series switch communicate with an IBM LAN Manager to provide the following support for Token Ring Source Route Bridging applications:

- Ring Error Monitor (REM)
- Configuration Report Server (CRS)
- Ring Parameter Server (RPS)
- LAN Bridge Server

What You Need to Configure

The LAN Server Subsystem (LSS) Record is configured for the Token Ring/Source Route Bridging LAN port. A Node boot is required to restart the LSS or implement LSS parameter changes.

Passwords

The default LSS link passwords for links 0 through 3 are initially set to “PASSWORD.” This password is used by the IBM LAN Network Manager to establish a connection to the 3Com bridge’s LSS. Default passwords can be changed by the LAN Manager. There is no facility to examine or change the passwords from the bridge’s human interface.

Also, it is recommended that you leave the parameter Calculation Interval at the default setting of 10 seconds to avoid conflict with the LNM.

Ring Error Monitor

A REM observes, collects, and analyzes hard error and soft error reports sent by stations on a single ring and assists in fault isolation and correction.

One or more ring error monitors can reside on a ring. If no REMs are on a particular ring, it is not possible to monitor errors for that ring.

One or more REMs can report to a LAN manager.

A REM has a functional address of C000000008.

Configuration Report Server

A CRS accepts commands from the LAN Manager to get station information, set station parameters, and remove stations from its ring. It also collects and forwards configuration reports generated by stations on its ring to the LAN manager. Information such as reporting a new active monitor and reporting a stored upstream address change are sent to the CRS.

A configuration report server has a functional address of C00000000010.

Ring Parameter Server

An RPS resides on each ring in a multiple-ring environment for which operational parameters are being managed, and provides three main services:

- Sends initialization information to new stations that are attaching to the ring.
- Ensures that stations on the ring have consistent values for operational parameters.
- Forwards registration information to LAN managers from stations attaching to the ring.

Statistics and Alarms

Statistics and status alarm thresholds maintained by the LSS are specific for the IBM LNM and can be accessed by the IBM LNM, but not from the CTP.

Configuring the LSS Record

Example of LCC Record

Figure 56 shows the LSS Record parameters used to configure a PathBuilder S200 series switch for LSS operation.

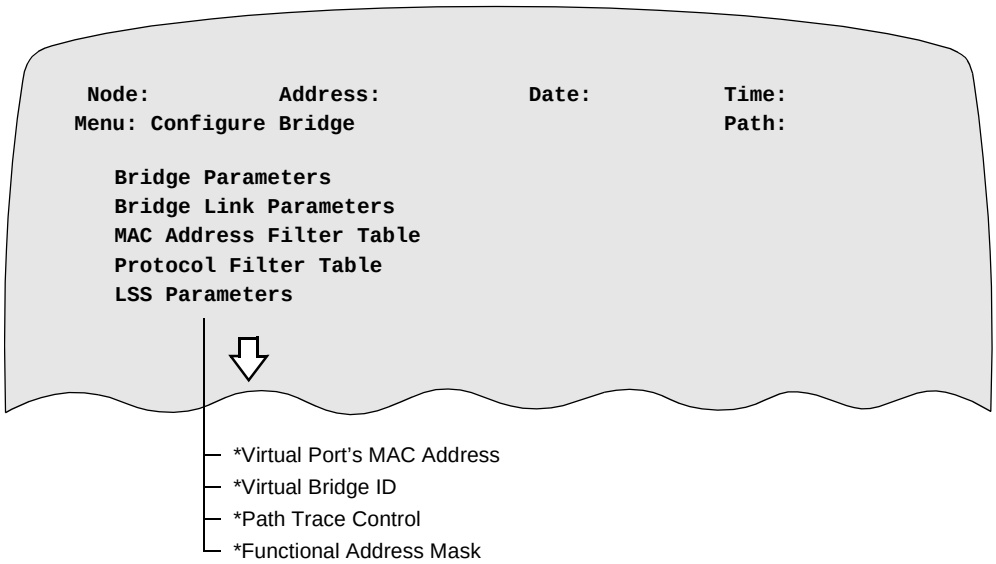


Figure 56. LAN Server Subsystem (LSS) Record Menu

Parameters

These parameters make up the LSS Record.

*Virtual Port's MAC Address

Range:	00-00-00-00-00-00 to FE-FF-FF-FF-FF-FF
Default:	00-00-00-00-00-00
Description:	Specifies the MAC address of the virtual LAN port of the virtual ring. This value defaults to a universally administered second address that is supplied by 3Com in the TRIM card PROM. This PROM address is called the Burned in Address (BIA). A value of zero (00-00-00-00-00-00) is used as the default when hardware is absent. When hardware is present and the MAC Address is configured to zero, it will be overwritten by the BIA. The LAN port can also be configured to a locally administered MAC address.

*Virtual Bridge ID

Range:	0 to 15
Default:	0
Description:	Represents the bridge ID of a virtual source routing bridge that connects the local TR LAN to the virtual TR LAN.

*Path Trace Control

Range:	ENABLE, DISABLE
Default:	DISABLE
Description:	Specifies whether or not the LBS is enabled to send the Path Trace notification frames to the IBM LAN Network Manager.

*Functional Address Mask

Range:	00000000 to 7FFFFFFF (hexadecimal)
Default:	0000001A
Description:	Used to enable or disable the LSS servers and represents a 31-bit map of functions where a specific bit identifies a function such as Configuration Report Server (CRS). Relevant bits should be set if the node supports these functions. • Configuration Report Server (CRS) = 00 00 00 10 • Ring Parameter Server (RPS) = 00 00 00 02 • Ring Error Monitor (REM) = 00 00 00 08 **Note** The LSS contains an LBS that is always enabled. A Node Boot is required to enable or disable the servers.

Bridge Statistics

Introduction

The Bridge Statistics section provides information about the LAN Port, Bridge Links, LAN Connection, and the Spanning Tree. Figure 57 shows the Bridge Statistics Menu screen.

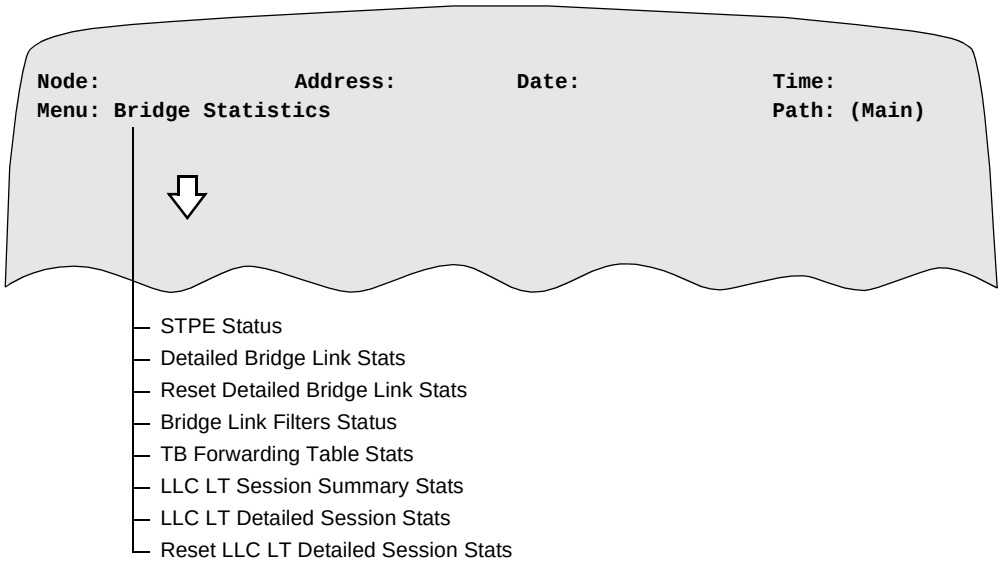


Figure 57. The Bridge Statistics Menu Screen

Spanning Tree Statistics

Spanning Tree (STPE) Status

Figure 58 shows the information displayed by the Spanning Tree Status report.

```
Node:            Address:                    Date:            Time:
Spanning Tree Statistics                                      Page: 1 of 1

STPE Bridge ID:  00:ff:ff:ff:00:00:00:00  Root Bridge ID: 00:ff:ff:ff:ff:ff:ff:ff
Root Path Cost   03                       Root Port: Bridge-Link
Max Age:         0                        Forward Delay: 0
Last Topological Change   09-AUG-1993 08:21:33
Topological Changes       0

      Bridge-Link   State          Priority   Path Cost
      ___________   _____          ________   _________
      1             Forwarding     128        1
      5             Forwarding     128        1
```

Figure 58. Spanning Tree Status

Descriptions for the Spanning Tree Status report

This table describes the screen terms for the Spanning Tree Statistics report.

Term	*Description*
STPE Control	Configured value of STPE Control. If STPE is configured for MAN, the rest of the parameters are not displayed.
STPE Bridge ID	The value of the bridge ID which is transmitted by the bridge in STPE PDUs.
Root Bridge ID	The root of the spanning tree as determined by the STPE.
Root Path Cost	The cost of the path to the root as seen from this bridge.
Root Port	The bridge link number that offers the lowest cost path from this bridge to the root bridge.
Max Age	The actual Max Age timeout value that this bridge is currently using.
Forward Delay	The actual Forward Delay value that this bridge is currently using. The amount of time before sending a regular (non-spanning tree) frame.
Last Topological Change	The time when the last topological change was detected.
Topological Changes	The number of topological changes since the last reset or restart.
Bridge Link	Number of specified bridge link.

Term *(continued)*	***Description***
State	The STPE view of the link's current state. The possible states are: • Disabled: The STPE is disabled. (If STPE Control parameter is MAN) • Blocking: The STE frames are blocked on this bridge link. • Listening: The STE frames are blocked. Listening to STPE PDUs. • Learning: The STE frames are blocked. Learning the topology from STPE PDUs. • Forwarding: The STE frames can be forwarded on this bridge link.
Priority	The value of STPE Priority parameter of the bridge link.
Path Cost	The value of STPE Path Cost parameter of the bridge link. A weight that is added to the overall links in a particular Ring-to-Ring path. The path with the lowest "cost" determines which path will be chosen between the Rings.

Detailed Bridge Link Statistics

Introduction

Figure 59 and Figure 60 show sample statistics screens.

```
Node:               Address:         Date:               Time:
Detailed Bridge Link Statistics: Bridge Link 01          Page:1 of 2

Bridge Link Status: Inactive
Bridge Type:        SRT     ST Status:         forwarding
Bridge Link Type:   LAN     Last Stat Reset:   01-MAY-1993 04:19:05
Max Frame Size:     205     Max Hop Count:     7
Local Ring Number:  1

SR:  Frame Summary:  Received        Transmitted
    SRF:             0               0
    ARE:             0               0
    STE:             0               4
    Frame Totals:    0               4

TB:  Frame Summary:  Received        Transmitted
    Unicast:         0               0
    Multicast:       0               0
    Broadcast:       0               0
    Frame Totals:    0               0
Press any key to continue ( ESC to exit ) ...
```

Figure 59. Detailed Bridge Link Statistics - First Page

```
Node:               Address:         Date:               Time:
Detailed Bridge Link Statistics: Bridge Link 01          Page:2 of 2

TB:  Frames Discarded link not in Forwarding State
     Inbound Discards:  0               Outbound Discards:  0

TB:  Frames Discarded due to unicast link protect being set
     Inbound Discards:  0               Outbound Discards:  0
TB:  Frames Discarded due to multicast link protect being set
     Inbound Discards:  0               Outbound Discards:  0

Filter Discards:       In          Out         RIF Error Discards:
  Source MAC Address:   0           0          Segment Mismatch:   0
Dest MAC Address:       0           0          Duplicate Segment:  0
  Protocol Filtered:    0           0          Hop Count Exceeded: 0
Total Filter Discards:  0           0



 Press any key to continue ( ESC to exit ) ...
```

Figure 60. Detailed Bridge Link Statistics - Second Page

Description of Screen Terms

This table describes Detailed Bridge Link Statistics terms.

Term	Description
Bridge Link Status	Following are the possible states: • Not Configured: This record is not configured. • No LAN Port: No physical LAN Port. • Active: Link is operational. • Congestion: Link is operational but congested. • Disabled: Disabled by Bridge Link disable command. • SW Disables: Disabled by the operating software because of internal error. • Inactive: Waiting to be Active after restart.
Bridge Type	Configured value of Bridge Type parameter of the Bridge Link.
ST Status	Spanning Tree state of a bridge link. This state controls what action a link takes on reception of a source route Spanning Tree Explorer Frame. • STPE Control = MAN: The configured value of the STPE state parameter is displayed. • STPE Control = AUTO: STPE view of the link's current state is displayed. • Disabled: LAN or WAN connection is inactive. • Blocking: The STE frames are blocked on this Bridge Link. • Listening: The STE frames are blocked. Learning the topology from STPE PDUs. • Forwarding: The STE frames can be forwarded on this bridge link.
Bridge Link Type	• LAN: If Bridge Link number is 1. • WAN: If Bridge Link number is 5 to 36.
Last Stat Reset	Date and time of the last statistics reset. Resetting the link statistics does not clear the last call information from the port statistics screens. This information is only cleared by a node boot.
Max Frame Size	The maximum size of the frame that this bridge link is configured to send and receive.
Max Hop Count	The maximum number of routing hops allowed in a source routed frame.
Local Ring Number	The ring number to which this bridge is locally attached.
Next Ring Number	The next Ring Number of the LAN to which the bridge route is bridging. This is the ring number to which the 3Com remote bridge is attached.

Term *(continued)*	***Description***
SR (Source Route): Frame Summary	Received/Transmitted: The number of Source Route frames received/sent by the bridge. • SRF: Specifically Routed Frames. • ARE: All Route Explorer. Also called all route broadcast. • STE: Spanning Tree Explorer. Also called Single Route Explorer (SRE) or single route broadcast. • Frame Totals: The total number of frames received and transmitted by the bridge.
Filter Discards	• In/Out: The number of frames that were discarded due to filtering action. • Source MAC Address: Filter discard due to source MAC Address match in filter table. • Dest MAC Address: Filter discard due to destination MAC Address match in filter table. • Protocol Filtered: Filter discard due to Protocol type MAC Address match in filter table. • Total Filter Discards: The total number of frame discards due to filter action.
RIF Error Discards	The number of frames that were discarded due to incorrect RIF: • Segment Mismatch: Frame is discarded because next ring indicated in RIF is not correct. • Duplicate Segment: Frame is discarded because the RIF listed the same LAN segment more than once. • Hop Count Exceeded: Frame is discarded because RIF exceeded maximum Hop Count Limit configured for the link.

Bridge Link Filter Summary

Example of Bridge Link Filter Summary

Figure 61 shows the information displayed by the Bridge Link Filter Summary. The filters from MAC Address Filter Tables and Protocol Filter Tables are sorted for a bridge link and displayed.

```
Node:                Address:          Date:                Time:
Bridge Link Filter Summary:  Bridge Link   5                 Page 1 of 1


 Bridge Link Filter Action:
    MAC Address:  Block
    Protocol:     Pass


 Active Filters:

    MAC Address      Source In      Source Out      Dest In       Dest Out
    080AB546787C     PASS              BLOCK          PASS           PASS
    01287D46787C     BLOCK             BLOCK          BLOCK          PASS


  Protocol Class       Value                 Incoming          Outgoing
    DSAP                8F                    PASS              PASS
    SNAP                0000010808            BLOCK             BLOCK

Press any key to continue  (ESC to exit)
```

Figure 61. Bridge Link Filter Summary Status

Description of Screen Terms

This table provides descriptions of the screen terms in the Bridge Link Filter Summary.

Term	*Description*
Bridge Link Filter Action:	• MAC Address: This field reports on the activity of the MAC filtering action. If the MAC Address Filter Action parameter is set to NONE, filtering is disabled. Pass or Block = Enabled. • Protocol: This field reports on the activity of the Protocol filtering action. If the Protocol Filter Action parameter is set to NONE, filtering is disabled. Pass or Block = Enabled.

Term (continued)	Description
Active Filters: MAC Address	• MAC Address: 6-byte value of MAC Address parameter from the MAC Filter Table. • Source In: Value (PASS or BLOCK) from the MAC Filter Table. Action to be taken on an inbound frame having the indicated MAC Source address. • Source Out: Value (PASS or BLOCK) from the MAC Filter Table. Action to be taken on an outbound frame having the indicated MAC Source address. • Destination In: Value (PASS or BLOCK) from the MAC Filter Table. Action to be taken on inbound frame for the indicated MAC Destination Address. • Destination Out: Value (PASS or BLOCK) from the MAC Filter Table. Action to be taken on outbound frame for the indicated MAC Destination address.
Active Filters: Protocol Class	• Protocol Class: Value (DSAP or SNAP) of Protocol Class parameter of a Protocol Filter Table. • Value: Represents the value of the Protocol parameter of a Protocol Filter Table. This value can be 1 byte (DSAP) or 5 bytes (SNAP), depending upon which type of protocol is involved in the frame. • Incoming: Value (PASS, BLOCK) from the Protocol Filter Table. Action to be taken on outbound frame for the indicated protocol value. • Outgoing: Value (PASS, BLOCK) from the Protocol Filter Table. Action to be taken on outbound frame for the indicated protocol value.
Note This screen can be several pages long depending on configuration.	

Transparent Bridge Forwarding Table Statistics

TB Forwarding Stats Example

TB Forwarding Table statistics are shown in Figure 62.

```
Node:               Address:         Date:               Time:
TB Forwarding Table Stats                                Page: 1 of 1

 Learned Entry Discards: 0                 Learned Entries: 0
 Available Entries:       7997              Maximum Entries: 3
 Aging Timer:   3600

 Forwarding Database:
   MAC Address            Bridge Link Number       Status
   03-00-FF-FF-FF-FF                               Other
   08-00-3E-00-1B-96                               Other
   FF-FF-FF-FF-FF-FF                               Other




Press any key to continue (ESC to exit)...
```

Figure 62. Transparent Bridge Forwarding Table Statistics

TB Forwarding Stats Descriptions

This table describes Transparent Bridging Forwarding Table Statistics attributes shown in Figure 62.

Term	Description
Learned Entry Discards	The number of Learned Address List entries that have been discarded due to lack of room in the forwarding database (the database size had been at its maximum allowed when the entry was learned).
Learned Entries	The total number of entries currently in the forwarding database (learned station table). The maximum number of entries is 8000.
Available Entries	The amount of space, in entries, that the forwarding database currently has available for additional entries.
Maximum Entries	The amount of space, in entries, that the forwarding database has available for entries since the last node boot.

Term *(continued)*	***Description***
Forwarding Database	• MAC Address: 6-byte value of MAC Address parameter from the MAC Filter Table. Indicates a MAC Address for the list of entries in the forwarding database displayed by the status/statistics screen. • Bridge Link Number: Indicates the corresponding bridge link number used to forward a frame with the given MAC Address. • Status: Indicates how the forwarding entry was learned. • CONF: This entry was learned from the permanent learned station address stored in CMEM. • LEARN: This entry was learned from the received frames on bridge links.

Transparent Bridge Detailed Bridge Link Statistics

Detailed Bridge Link Statistics

Figure 63 shows page 2 of the Detailed Bridge Statistics screen. This page reflects Transparent Bridging statistics when TB is configured on the node.

```
Node:               Address:         Date:               Time:
Detailed Bridge Link Statistics: Bridge Link 01          Page: 2 of 2

TB: Frames Discarded link not in Forwarding State
     Inbound Discards: 0                Outbound Discards: 0

TB: Frames Discarded due to unicast link protect being set
     Inbound Discards: 0                Outbound Discards: 0
TB: Frames Discarded due to multicast link protect being set
     Inbound Discards: 0                Outbound Discards: 0

Filter Discards:       In          Out         RIF Error Discards:
 Source MAC Address:    0           0          Segment Mismatch:   0
Dest MAC Address:       0           0          Duplicate Segment:  0
  Protocol Filtered:    0           0          Hop Count Exceeded: 0
Total Filter Discards:  0           0



 Press any key to continue ( ESC to exit ) ...
```

Figure 63. Detailed Bridge Link Statistics (TB) - Second Page

Detailed Bridge Link Statistics Terms-Transparent Bridge Second Page

This table describes the attributes for page 2 of the Detailed Bridge Link Statistics screen shown in Figure 63.

Term	*Description*
STPE State	Learning: The STPE frames are blocked. Learning the topology from STPE PDUs.

Term	Description (continued)
TB Frame Summary	Frames Received/Transmitted: • Unicast: This is a count of frames received/transmitted with an individual (non-group) MAC level address • Multicast: This is a count of the number of frames received/ transmitted with a group MAC level address • Broadcast: This is a count of the number of frames received/ transmitted with the broadcast MAC level address (FF-FF-FF-FF-FF-FF) • Frame Totals: This is a count of the number of frames received/transmitted of all types on this link
TB Frames Discarded	• Inbound: This counter indicates the number of received frames that are discarded due to the bridge link being in a non-forwarding state due to spanning tree configuration. • Outbound: This counter indicates the number of transmitted frames that are discarded due to the bridge link being in a non-forwarding state due to spanning tree configuration.
TB Filter Discards	Source MAC Address • IN: This counter is incremented when the inbound frame on a Bridge Link is not forwarded because of MAC Address Table filtering on the source address. • OUT: This counter is incremented when the outbound frame on a Bridge Link is not forwarded because of MAC Address Table filtering on the source address. • Destination MAC Address • IN: This counter is incremented when the inbound frame on a Bridge Link is not forwarded because of MAC Address Table filtering on the destination address. • OUT: This counter is incremented when the outbound frame on a Bridge Link is not forwarded because of MAC Address Table filtering on the destination address. • Protocol Filter • IN: This counter is incremented when the inbound frame on a Bridge Link is not forwarded because of Protocol Table Filtering. • OUT: This counter is incremented when the outbound frame on a Bridge Link is not forwarded because of Protocol Table Filtering. • Total Filter Discards • IN: This counter is the sum of Source MAC Address (in), Destination Address (in), and Protocol filter (in). • OUT: This counter is the sum of Source MAC Address (out), Destination Address (out), and Protocol filter (out).

LAN Connection Statistics

Example of LAN Connection Statistics Menu

The LAN Connection Statistics Menu screen is shown in Figure 64. Select the appropriate number to view a particular screen.

```
Node:                Address:         Date:                Time:
Menu:Lan Connection Statistics                             Path:(Main.5.9)

   LAN Connection Stats
   LAN Connection Summary Stats
   Reset LAN Connection Stats
```

Figure 64. LAN Connection Statistics Menu Screen

Example of Detailed LAN Connection Statistics

Figures 65 and 66 show the Detailed LAN Connection Statistics.

```
Node:                Address:         Date:                Time:
Detailed LAN Connection Statistics: LCON-5                 Page: 1 of 2

Last Statistics Reset: Date/Time

Transmit Data Summary:

Number of Packets Transmitted:    0
Average Transmit Packet Size:     0
Current Transmit Queue Depth:     0
Maximum Transmit Queue Depth:     0 at Date/Time

Receive Data Summary:

Number of Packets Received :      0
Average Receive Packet Size:      0

Discard Summary:

Transmit Packets Discarded Due to Max Frame Size Exceeded:0
Transmit Packets Discarded Due to Node Transit Delay: 0
Transmit Packets Discarded Due to Congestion:         0

Press any key to continue ( ESC to exit )
```

Figure 65. Detailed LAN Connection Statistics - First Page

```
Node:               Address:         Date:               Time:
Detailed LAN Connection Statistics: LCON-5              Page: 2 of 2

Call Summary

Connection Type:   SVC
Connection State:  Improper Config
Forwarders Connected:
Remote Address:
Number of auto-call attempts    0
Last clear cause code:          0 (Cleared by other end)
Last clear diagnostic code:     0 (No more information)

Packet Summary:            Transmit    Receive

Data                       0           0
Call Request               0           0
Call Accept                0           0
Clear Request              0           0
Clear Confirm              0           0
Reset Request              0           0
Reset Confirm              0           0

Press any key to continue ( ESC to exit )
```

Figure 66. Detailed LAN Connection Statistics - Second Page

Description of Screen Terms

This table describes screen terms for pages 1 and 2 of the Detailed LAN Connection Statistics shown in Figures 65 and 66.

Term	Description
Call Summary	This field provides information about the following: • Connection Type: Specifies whether the connection is an SVC or a PVC. • Connection State: Specifies the current state of the PVC or SVC. Possible states are: Unconfigured; Calling; Waiting; Connected; Autocall Failure; Software Disabled; Operator Disabled; Congested. This means either the Frame Relay link is receiving BECNs or the node is running low on Data Buffers. Or, if the LCON queue backs up due to too much traffic passing from the LAN to the WAN, the connection state may be Congested. • Forwarders Connected: Specifies which forwarders are currently connected to this LAN Connection: Source Route; Spanning Tree). • Remote Address: Specifies the called address of the remote WAN Adapter LAN Connection for connected SVCs. The possible states are: Blank for PVCs; blank for disconnected SVCs; No Mnemonic (for autocall SVCs whose mnemonic does not exist in the Mnemonic Table); Max Attempts (for Autocall SVCs that reached their autocall maximum attempts count). • Number of auto call attempts: Specifies the number of times the WAN Adapter attempted to autocall before it either succeeded or failed in establishing the connection. • Last clear cause code: This is the cause code in the call clear packet last received by the LAN connection and explains why the last call was cleared. • Last clear diagnostic code: This is the diagnostic code in the call clear packet last received by the LAN connection and explains why the call was cleared.

Term (continued)	Description
Packet Summary	• Data: Summary of each packet sent on the WAN and received from the WAN bridge link. • Call Request: Specifies the total number of Call Request Packets sent on the WAN and received from the WAN. • Call Accept: Specifies the total number of Call Accept Packets sent on the WAN and received from the WAN. • Clear Request: Specifies the total number of Clear Request Packets sent on the WAN. • Clear Confirm: Specifies the total number of Clear Confirmation Packets sent on the WAN and received from the WAN. • Reset Request: Specifies the total number of Reset Request Packets sent on the WAN and received from the WAN. • Reset Confirm: Specifies the total number of Reset Confirmation Packets sent on the WAN and received from the WAN.
Last Statistics Reset	The date and time of the last statistics reset. Resetting the statistics does not clear the last call information from the detailed port statistics screen. This information is cleared only on a node boot.
Transmit Data Summary	This field provides information on the transmission of packets and those awaiting transmission to the WAN. Totals are provided for: the number of packets transmitted, the average transmitted packet size in bytes, and the current and maximum transmit queue depths in packets.
Receive Data Summary	This field provides information on the number of packets received and the average size of the packets received from the WAN. Totals are provided for the number of packets received and the average received packet size in bytes.
Discard Summary	This field provides the following totals for packets discarded due to the following reasons: • Transmit Packets Discarded Due to Max Frame Size Exceeded. • Transmit Packets Discarded Due to Node Transit Delay. • Transmit Packet Discarded Due to Congestion (data was buffered more than 1 second.

Example of LAN Connection Summary Statistics

Figure 67 shows the LAN Connection Summary Statistics.

```
Node:                Address:          Date:                Time:
LAN Connection Summary Status                                Page: 1 of 1

LAN                  Bridge            Conn.        Remote
Connection           Link              Type         Destination
==================== ================  ===========  ====================
1 Waiting            5 Configured      SVC

Press any key to continue ( ESC to exit )
```

Figure 67. LAN Connection Summary Statistics

Description of Screen Terms

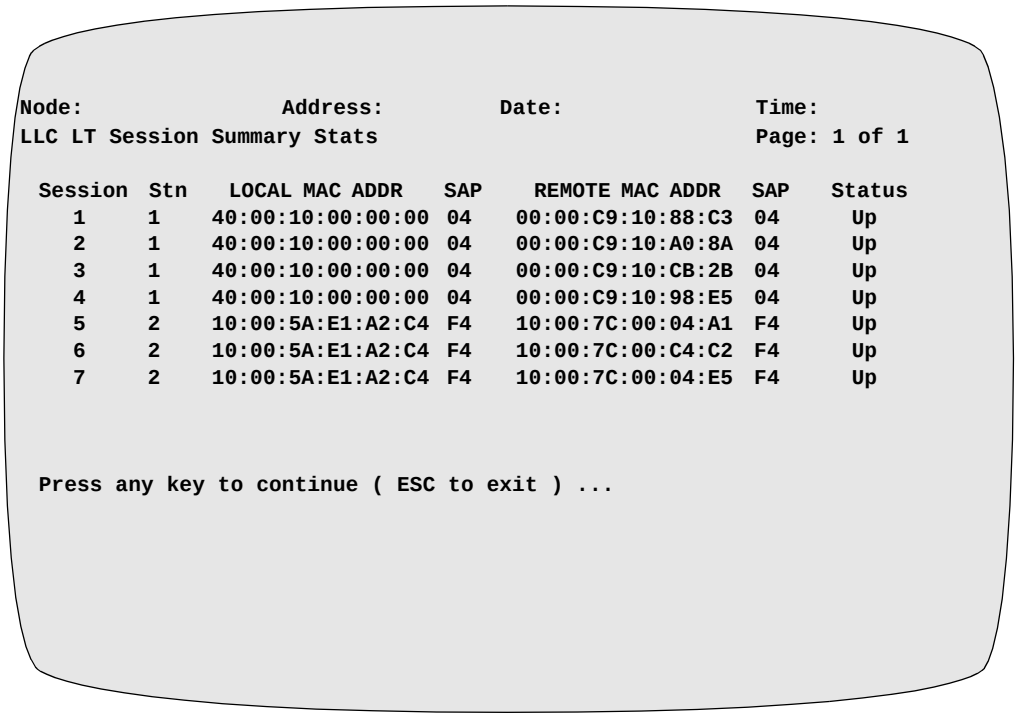
This table describes the screen terms for the LAN Connection Summary Statistics shown in Figure 67.

Term	*Description*
LAN Connection	Specifies the LAN Connection entry number and current state of a configured LAN Connection. The possible states are: Not Properly Configured; Not Connected; Calling; Waiting for Call; Connected; Waiting for Clear Confirmation; Disabled.
Bridge Link	Specifies the WAN Bridge Link number associated with this LAN connection. The possible current states of the WAN Bridge Link are: Not Applicable; Empty; Mismatch; Inactive; Active; Congested; Software Disabled; User Disabled.
Connection Type	Specifies whether the LAN Connection is a PVC, a Calling SVC, or a Called SVC.
Remote Destination	Specifies the remote destination that this LAN Connection is connected to (including the Remote Connection ID).

LLC2 LT Session Summary Statistics

Sample of Session Summary Statistics

Figure 68 shows a sample of the LLC2 LT Session Summary Statistics report.



```
Node:                Address:          Date:                Time:
LLC LT Session Summary Stats                                Page: 1 of 1

 Session  Stn    LOCAL MAC ADDR    SAP    REMOTE MAC ADDR   SAP    Status
    1     1    40:00:10:00:00:00  04    00:00:C9:10:88:C3  04      Up
    2     1    40:00:10:00:00:00  04    00:00:C9:10:A0:8A  04      Up
    3     1    40:00:10:00:00:00  04    00:00:C9:10:CB:2B  04      Up
    4     1    40:00:10:00:00:00  04    00:00:C9:10:98:E5  04      Up
    5     2    10:00:5A:E1:A2:C4  F4    10:00:7C:00:04:A1  F4      Up
    6     2    10:00:5A:E1:A2:C4  F4    10:00:7C:00:C4:C2  F4      Up
    7     2    10:00:5A:E1:A2:C4  F4    10:00:7C:00:04:E5  F4      Up


 Press any key to continue ( ESC to exit ) ...
```

Figure 68. Session Summary Statistics Screen

Description of Screen Terms

This table describes the screen terms for the Session Summary Statistics screen as shown in Figure 68.

Heading	*Description*
Session	Session number assigned between the MAC addresses. Maximum number of sessions supported is 64.
Stn	Refers to the entry number assigned to the LT session for the local MAC address during configuration. Maximum number of stations available is 64.
Local MAC ADDR	Refers to the MAC address assigned to the locally attached device to be spoofed (local is in reference to the bridge you are taking statistics from).
SAP	Refers to the Service Access Point used by the local MAC address for this session.
REMOTE MAC ADDR	Refers to the MAC address assigned to the remotely attached device to be spoofed (remote is in reference to the bridge you are taking statistics from).
SAP	Refers to the Service Access Point that is used by the remote MAC address for this session.

Heading *(continued)*	***Description***
Status	Indicates the session between the local and remote MAC addresses. • UP - MAC addresses are communicating using Local Termination. • DOWN - MAC addresses are not communicating. Session is the process of coming up or going down.

LLC2 LT Detailed Session Statistics

Sample of Detailed Session Statistics

Figures 69 and 70 show samples of the LLC2 LT Detailed Session Statistics report.

```
 Node:             Address:         Date:               Time:
 LLC LT Detailed Session Stats                          Page: 1 of 2

 Session Number: 1    Station Number: 1        LLC Profile Name: HOSt
 Local MAC: 40:00:10:00:00:00      Local SAP: 04         WAN Queue Depth: 0
 Remote MAC: 00:00:C9:10:88:C3     Remote SAP: 04        LAN Queue Depth: 0
 RIF: 0620,0021,0010
 Last Statistics Reset: Date/Time

Local Station Session Summary:
 TX Window:   7                Protocol State:   4
 Characters In:   3740798      Characters Out:   36107
 Frame Type      In          Out        Frame Type    In        Out
 Info:           17682       3980         UI:         0         --
 RR:             4018        6827         TEST:       0         --
 RNR:            0           1            XID:        1         --
 REJ:            0           0            DISC:       0         0
 SABME:          1           0            DM:         0         0
 UA:             0           1            FRMR:       0         0
 Frames received out of sequence:
 0 Bad Frames received: 0
 Frames dropped: 0

 Press any key to continue ( ESC to exit ) ...
```

Figure 69. Detailed Session Statistics Screen - Page 1

```
 Node:             Address:         Date:               Time:
 LLC LT Detailed Session Stats                          Page: 2 of 2
Remote Spoofer Session Summary:

 TX Window:   7       Protocol State:   4

 Frame Type      In          Out        Frame Type    In
 Out
 Info:           3982        17691        UI:         0           --
 RR:             6114        4064         TEST:       0           --
 RNR:            0           0            XID:        2           --
 REJ:            0           0            DISC:       0           0
 SABME:          0           1            DM:         0           0
 UA: 1 0 Frames received out of sequence: 0
 Bad Frames received: 0
 Frames dropped: 0


 Press any key to continue ( ESC to exit ) ...
```

Figure 70. Detailed Session Statistics Screen - Page 2

Description of Screen Attributes

This table describes the screen attributes for the Detailed Session Statistics screens as shown in Figures 69 and 70.

Heading	Description
Session Number:	Refers to the entry number assigned between MAC addresses. Maximum number of sessions is 64.
Station Number:	Entry Number on LLC LT Station Table of local MAC/SAP.
LLC Profile Name:	Profile name table that this station uses which references the T1, T2, Ti, N2, N3, TW values.
Local MAC:	MAC address of the local device.
Remote MAC:	MAC address of the remote device.
Local SAP:	SAP being used by local device.
Remote SAP:	SAP being used by the remote device.
WAN Queue Depth:	Indicates the number of packets queued for transmission to the WAN or waiting for acknowledgment from the remote spoofer.
LAN Queue Depth:	Indicates the number of packets queued for transmission to the LAN or waiting for acknowledgment from the local device.
RIF:	Routing information field used in all frames transmitted between the devices. This field contains the routing control field, ring number, and bridge number information.
Last Statistics Reset:	Last time statistics were reset.

Heading	Description (continued)
Local Station Session Summary	
TX Window:	Transmit window size obtained from the configuration for the local station.
Protocol State:	Number of the state for current session with local device.
Characters In:	Number of user data characters received by the spoofer from the locally attached LAN station.
Characters Out:	Number of user data characters transmitted by the spoofer to the locally attached LAN station.
Info:	Number of information frames received or transmitted by the local spoofer from or to the local device.
RR:	Number of RR frames received or transmitted by the local spoofer from or to the local device.
RNR:	Number of RNR frames received or transmitted by the local spoofer from or to the local device.
REJ:	Number of REJ frames received or transmitted by the local spoofer.
SABME	Number of SABME frames received or transmitted by the local spoofer from or to the local device.
UA:	Number of UA frames received or transmitted by the local spoofer to or from local device.
UI:	Number of UI frames received by the local spoofer from the local device.
TEST:	Number of Test frames received by the local spoofer from the local device.
XID:	Number of XID frames received by the local spoofer from the local device.
DISC:	Disconnect.
DM:	Number of DM frames received or transmitted by the local spoofer from or to the local device.
FRMR:	Number of FRMR frames received or transmitted by the local spoofer from the local device.
Frames received out of sequence:	Information frames received out of sequence from the local device.
Bad frames received:	Bad frames received from the local device. These frames are improper for various reasons.
Frames dropped:	Frames from the local device, dropped due to congestion (due to WAN queue full).

Heading	Description (continued)
Remote Spoofer Session Summary	
TX Window:	Transmit window size obtained from the configuration for LLC WAN parameters.
Protocol State:	Number of the state for current session with remote spoofer.
Info:	Number of information frames received or transmitted by the local spoofer to or from the remote spoofer.
RR:	Number of RR frames received or transmitted by the local spoofer to or from the remote spoofer.
RNR:	Number of RNR frames received or transmitted by the local spoofer to or from the remote spoofer.
REJ:	Number of REJ frames received or transmitted by the local spoofer from or to the remote spoofer.
SABME	Number of SABME frames received or transmitted by the local spoofer from or to the remote spoofer.
UA:	Number of Unnumbered Acknowledgment (UA) frames received or transmitted by the local spoofer to or from the remote spoofer.
UI:	Number of Unnumbered Information (UI) frames received by the local spoofer from the remote spoofer.
TEST:	Number of Test frames received by the local spoofer from the remote spoofer.
XID:	Number of XID frames received by the local spoofer from the remote spoofer.
DISC:	Disconnect.
DM:	Disconnect node.
Frames received out of sequence:	Number of frames received out of sequence from the remote spoofer.
Bad frames received:	Number of bad frames received from the remote spoofer.
Frames dropped:	Frames from the remote spoofer, dropped due to congestion (LAN queue full).

Reset Statistics

How to...

Reset Port Statistics: Consistent with PathBuilder S200 series switch, the reset port statistics prompts you to enter the number of the port to be reset. For TR port Number 55, all the statistical counters are set to zero.

Reset Bridge Link Stats: This command prompts you to enter the number of the bridge link to be reset. All the statistical counters of the selected bridge link are set to zero.

Reset All Stats: This command resets all the statistics of the PathBuilder S200 series switch. This includes statistics of the TR port and all bridge links.

Appendix A
Technical Support

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the very latest, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com FTP site
- 3Com Bulletin Board Service (3Com BBS)
- 3ComFacts℠ automated fax service

World Wide Web Site

Access the latest networking information on the 3Com Corporation World Wide Web site by entering the URL into your Internet browser:

http://www.3com.com/

This service provides access to online support information such as technical documentation and software library, as well as support options ranging from technical education to maintenance and professional services.

3Com FTP Site

Download drivers, patches, and software, across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com (or 192.156.136.12)**
- Username: **anonymous**
- Password: **<your Internet e-mail address>**

Note

A user name and password are not needed with Web browser software such as Netscape Navigator and Internet Explorer.

3Com Bulletin Board Service

The 3Com BBS contains patches, software, and drivers for 3Com products. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

Access by Analog Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	*Data Rate*	*Telephone Number*
Australia	Up to 14,400 bps	61 2 9955 2073
Brazil	Up to 14,400 bps	55 11 5181 9666
France	Up to 14,400 bps	33 1 6986 6954
Germany	Up to 28,800 bps	4989 62732 188
Hong Kong	Up to 14,400 bps	852 2537 5601
Italy	Up to 14,400 bps	39 2 27300680
Japan	Up to 14,400 bps	81 3 3345 7266
Mexico	Up to 28,800 bps	52 5 520 7835
P.R. of China	Up to 14,400 bps	86 10 684 92351
Taiwan, R.O.C.	Up to 14,400 bps	886 2 377 5840
U.K.	Up to 28,800 bps	44 1442 438278
U.S.A.	Up to 28,800 bps	1 408 980 8204

Access by Digital Modem

ISDN users can dial in to the 3Com BBS using a digital modem for fast access up to 56 Kbps. To access the 3Com BBS using ISDN, use the following number:

1 408 654 2703

3ComFacts Automated Fax Service

The 3ComFacts automated fax service provides technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3ComFacts using your Touch-Tone telephone:

1 408 727 7021

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, please call the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Below is a list of worldwide technical telephone support numbers:

Country	*Telephone Number*	*Country*	*Telephone Number*
Asia Pacific Rim			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or
Hong Kong	800 933 486		021 6350 1590
India	61 2 9937 5085	Singapore	800 6161 463
Indonesia	001 800 61 009	S. Korea	
Japan	0031 61 6439	From anywhere in S. Korea:	82 2 3455 6455
Malaysia	1800 801 777	From Seoul:	00798 611 2230
New Zealand	0800 446 398	Taiwan, R.O.C.	0080 611 261
Pakistan	61 2 9937 5085	Thailand	001 800 611 2000
Philippines	1235 61 266 2602		
Europe			
From anywhere in Europe, call:	+31 (0)30 6029900 phone +31 (0)30 6029999 fax		
From the following European countries, you may use the toll-free numbers:			
Austria	06 607468	Netherlands	0800 0227788
Belgium	0800 71429	Norway	800 11376
Denmark	800 17309	Poland	0800 3111206
Finland	0800 113153	Portugal	05 05313416
France	0800 917959	South Africa	0800 995014
Germany	0130 821502	Spain	900 983125
Hungary	00800 12813	Sweden	020 795482
Ireland	1 800 553117	Switzerland	0800 55 3072
Israel	177 3103794	U.K.	0800 966197
Italy	1678 79489		
Latin America			
Argentina	541 312 3266	Colombia	571 629 4847
Brazil	55 11 523 2725, ext. 422	Mexico	01 800 849 2273
North America	1 800 NET 3Com (1 800 638 3266)		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	*Telephone Number*	*Fax Number*
Asia, Pacific Rim	65 543 6342	65 543 6348
Europe, South Africa, and Middle East	011 44 1442 435860	011 44 1442 435718
From the following European countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	06 607468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0130 821502	
Hungary	00800 12813	
Ireland	1800553117	
Israel	177 3103794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	05 05313416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
Latin America	1 408 326 2927	1 408 764 6883
U.S.A. and Canada	1 800 876 3266, option 2	1 408 764 7120

3/26/98

Index

H

I

L

M

N

O

P

R

S

T

U

V

W

X