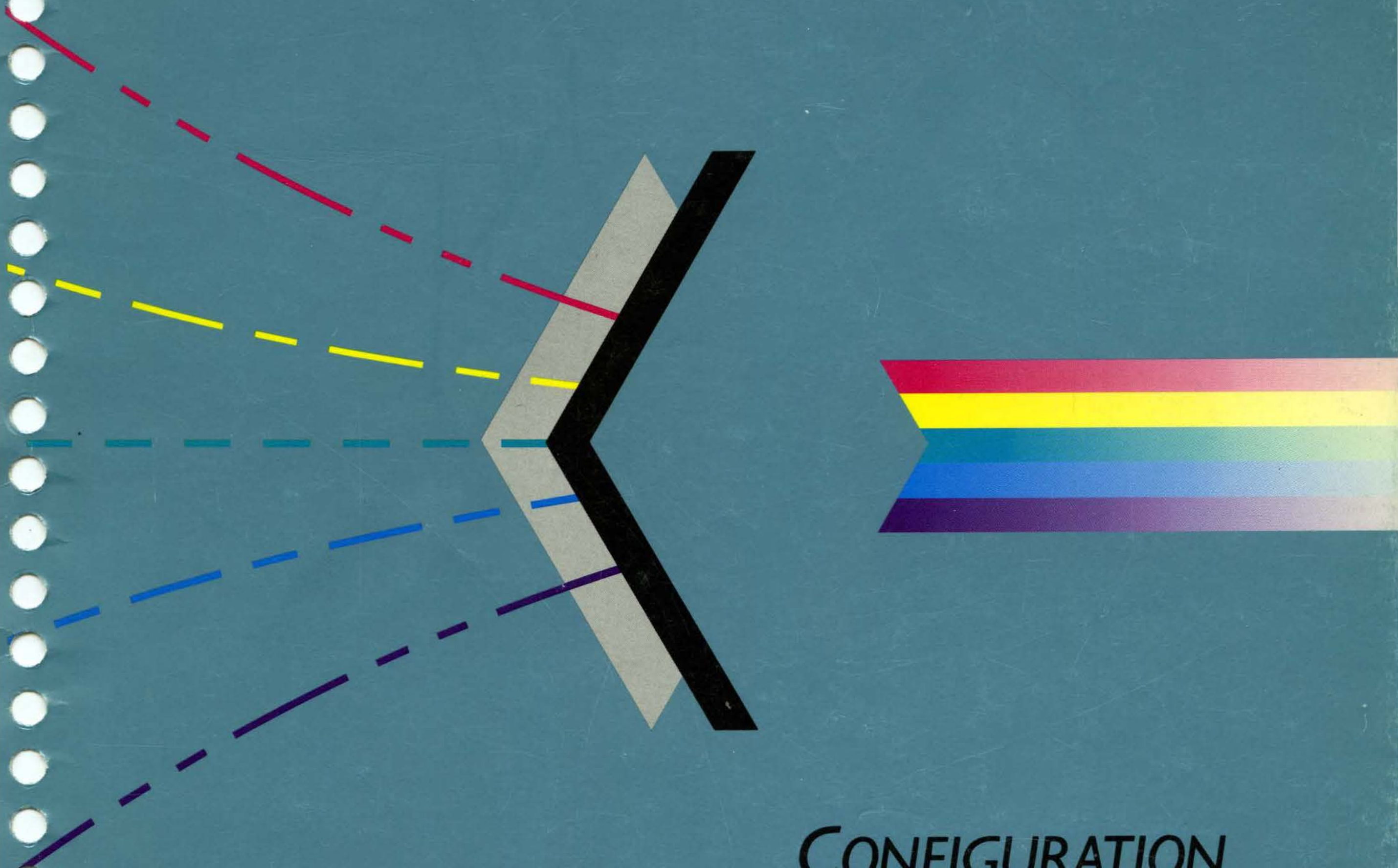
WELLFLEET communications



CONFIGURATION GUIDE

VOLUME I

Wellfleet Configuration Guide

Volume I

Wellfleet Communications, Inc.

Printed in U.S.A.

December 1991

Part # 103608 Rev. A

Please address questions about technical matters to our 24-Hour Customer Support Line:

Inside Massachusetts:	617-275-2400
Outside Massachusetts:	1-800-2LANWAN

Please address comments about this manual to:

Technical Publications
Wellfleet Communications, Inc.
15 Crosby Drive
Bedford, MA 01730
Tel: (617) 275-2400
Fax: (617) 275-5001

Information presented in this document is subject to change without notice.

Table of Contents

List of Figures

List of Tables

Preface

Purpose of this Guide

The information contained in this guide documents Software Release 5.70.

This information enables you to describe your network to the Wellfleet multiprotocol router. An accurate description of your network is a prerequisite for efficient and reliable network interconnection. This information also provides you with the ability to describe future changes in network topology or capability, thus ensuring that the router can accommodate your present and future networking needs.

Audience

This guide is intended for experienced network managers and other technicians who install the router. Such individuals should be thoroughly familiar with the network topology within which the router operates.

Depending on application software requirements, managers and technicians should be acquainted with media-access-control (MAC) level transparent and source routing bridges, the Internet protocol suite (commonly called TCP/IP), the Xerox Network Systems Internet Transport Protocols (commonly called XNS), the Internetwork Packet Exchange Protocol (IPX, Novell's implementation of XNS), the AppleTalk protocol suite, and/or DECnet architecture and routing.

Organization

The *Wellfleet Configuration Guide* provides a series of step-by-step procedures that lead you through the configuration process.

The guide, which consists of two separate volumes, contains fifteen chapters and six appendixes. Volume I contains Chapters 1 through 10 while Volume II contains Chapters 11 through 15 and Appendixes A through E. Both volumes provide inclusive Tables of Contents, Lists of Figures, Lists of Tables, and Indexes.

Volume I contains the following sections:

Chapter 1, *Getting Started*, provides an overview of the configuration process. It also tells you how to use the console keyboard to enter required data, and how to access the Main Menu and Configuration Menu to begin system configuration.

Chapter 2, *Setting Administrative Parameters*, tells you how to assign values to system parameters, describes session modes, and tells you how to configure a user session.

Chapter 3, *Loading Software*, tells you how to load routing protocols (the AppleTalk Router, the Bridge, the DECnet Router, the IPX Router, the TCP/IP Router, and the XNS Router).

Chapter 4, *Setting Physical Layer Parameters*, describes the physical lines that connect the router to local devices or to long-haul transmission facilities, and tells you how to use the Configuration Editor to describe various types of lines.

Chapter 5, *Setting Data-Link Layer Parameters*, provides a description of circuits and circuit functions and tells you how to configure various circuit types.

Chapter 6, *Configuring X.25 Service*, provides a description of X.25 service, and tells you how to configure X.25 packet-switched service.

Chapter 7, *Building Circuit Groups*, describes circuit group functions and tells you how to assign individual circuits to circuit groups.

Chapter 8, *Configuring the Bridge*, provides a description of the bridge, along with a set of procedures to configure bridge software.

Chapter 9, *Configuring TCP/IP*, provides a description of internet routing, along with procedures to configure IP router software.

Chapter 10, *Configuring SNMP*, tells you how to configure the multiprotocol router to run the Simple Network Management Protocol agent software.

Volume II contains the following sections:

Chapter 11, *Configuring DECnet Phase IV*, provides a description of DECnet Phase IV routing, in addition to a set of procedures to configure DECnet Phase IV router software.

Chapter 12, *Configuring XNS*, provides a description of XNS routing, along with procedures to configure XNS router software.

Chapter 13, *Configuring IPX*, provides a description of IPX routing, along with procedures to configure IPX router software.

Chapter 14, *Configuring AppleTalk*, provides a description of AppleTalk routing, along with procedures to configure AppleTalk router software.

Chapter 15, *Implementing config*, describes how to boot the router with a network-specific configuration file.

Appendix A, *File Management*, describes Configuration Editor and Network Command Language Interpreter commands that enable you to abort, examine, save, copy, and modify the configuration file.

Appendix B, *Session Modes*, describes printer, disk-logging, and telnet sessions.

Appendix C, *Line and Circuit Charts*, provides a series of tables that you can use to record line- and circuit-specific information.

Appendix D, *auto config*, describes the automatic configuration feature. This feature provides for the initial establishment of a bridge-only configuration without operator intervention.

Appendix E, *Hardware Configuration*, provides information of configuring Wellfleet Link Modules.

Associated Documents

You may wish to refer to the following documents:

- *Wellfleet Installation Guide*

  This guide explains how to install and boot the Wellfleet multiprotocol router.

- *Wellfleet Operator's Guide*

  This guide explains how to operate the router. It documents the Network Control Language (NCL) Interpreter and the system management information base (MIB). It also provides a listing of all event messages generated during router operations.

- *Wellfleet Overview Guide*

  This guide provides an introduction to internetworking technologies and provides a capsule description of the Wellfleet hardware and software product line.

Notation

Wellfleet documentation follows these standards for typography:

Type of Text	Components	Example
`user input`	Typewriter font bold in text	Use the **`dir`** command.
`user input`	Typewriter font regular in offset text	**sw->**`dir`
`Command names`	Typewriter font bold	Use the **`enable`** command.
`[KEYNAMES]`	Typewriter font bold in brackets []; (usually uppercase)	Press the **`[RETURN]`** key.
`Filenames`	Typewriter font oblique	Use the *`config`* file.
System output	Helvetica bold	**Zone name table full**
Command syntax:	Required arguments in angle brackets; optional arguments in curly braces divided by vertical bars	<addr> {...|...|...}
`[RETURN]` key symbol	Right angle arrow symbol	↵
Document titles	Italic	*Operator's Guide*
Chapter/section titles	Italic	Refer to the chapter entitled *Configuring the Bridge.*

1 Getting Started

This chapter provides some preliminary, but necessary, information that you need to know before you configure the multiprotocol router. It first introduces the configuration editor, explains the use of the console keyboard to enter data, and provides a brief description of the configuration process. It then tells how to display the Main Menu, how to select the Configuration Editor from the Main Menu, and how to create a configuration file (hereafter referred to as `config`).

1.1 Before You Begin

Prior to configuring the router, be certain to do the following:

- ❐ Thoroughly acquaint yourself with your network topology.
- ❐ Install the router as described in the *Installation Guide.*

  Strict adherence to installation procedures ensures router and network integrity and facilitates the configuration process.

1.2 Configuration Editor

You use the Configuration Editor to provide the router with network-descriptive data; the router, in turn, formats this data and stores it in a file called `config`. Subsequently, each time the router boots, it accesses `config` to acquaint itself with the network topology.

The Configuration Editor creates, opens, modifies, and closes `config`. Consisting of a hierarchical series of menus, screens, and prompts, it solicits required network-specific data. Appendix A, *File Management*, contains ancillary information on Configuration Editor commands.

1.3 Console Keyboard

You use the console keyboard to respond to Configuration Editor requests for data. Requests take one of two forms. Some require you to select from two or more supplied options (for example **Yes** or **No**, **Balanced** or **Unbalanced**, **1**, **1.5** or **2**). You use the `[RIGHTARROW] (⇒)` and `[LEFTARROW] (⇐)` keys to examine available options. Pressing the `[RIGHTARROW]` displays the next available option, while pressing the `[LEFTARROW]` displays the previous option. When the option you wish to choose is displayed, press the **[RETURN]** key to enter it into *config* and move the cursor to the next menu, screen, or prompt.

Other requests require you to enter alphanumeric data using the typewriter portion of your console keyboard. Such requests, for example, may ask for a circuit name, for a physical device address, or for a protocol-specific address. To respond, enter the data from the keyboard and then press the **[RETURN]** key to enter it into *config* and move the cursor to the next menu, screen, or prompt.

If you make a mistake, you can use the **[DELETE]** or **[BACKSPACE]** key to reposition the cursor; you then enter corrected data. Refer to Appendix A, *File Management*, for additional information on modifying *config*.

1.4 Configuration Process

The configuration process consists of five major steps:

1. Define administrative parameters

   Administrative parameters serve two functions. They specify how software entities and services initialize when power is applied, and they define the user interface.

2. Load application software

   Application software modules provide network bridging and routing services.

3. Establish communication channels

   Communication channels define both the physical layer and data-link layer connections between the router and various network components.

4. Customize application software modules

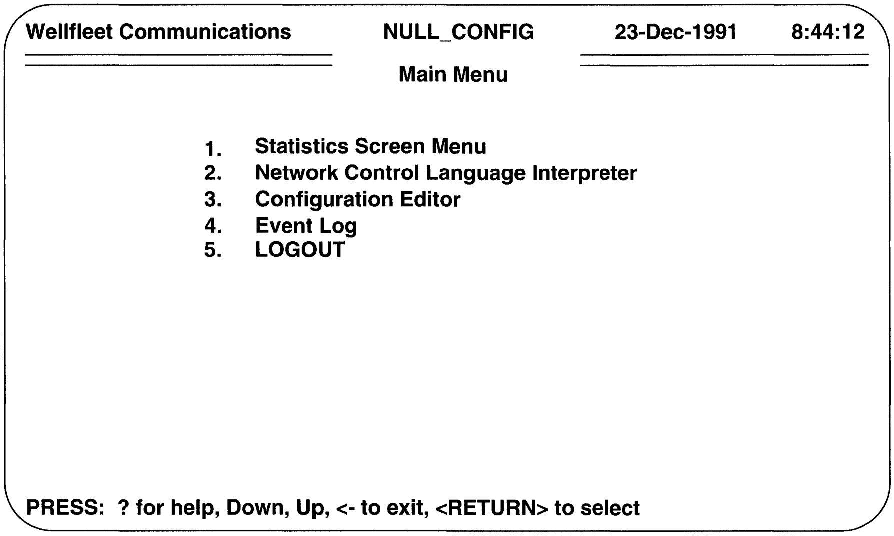
   Application software modules require network-specific data in order to provide bridging, routing, and/or network-management services.

5. Implement *config*

   After customizing the application software modules, you complete the configuration process by saving *config* and then booting the router.

1.5 The Main Menu

To display the Main Menu, boot the router as described in the *Installation Guide*. After the router boots, if you have previously enabled password protection, the screen prompts for a password. (The *Operator's Guide* tells you how to enable or disable password protection.) At the **Password** prompt, enter the password, then press **[RETURN]**. In response, the screen displays the Main Menu (Figure 1-1). If you have not previously assigned password protection, the screen displays the Main Menu immediately.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991    8:44:12
                                 Main Menu

                 1.   Statistics Screen Menu
                 2.   Network Control Language Interpreter
                 3.   Configuration Editor
                 4.   Event Log
                 5.   LOGOUT

PRESS:  ? for help, Down, Up, <- to exit, <RETURN> to select
```

Figure 1-1 Main Menu

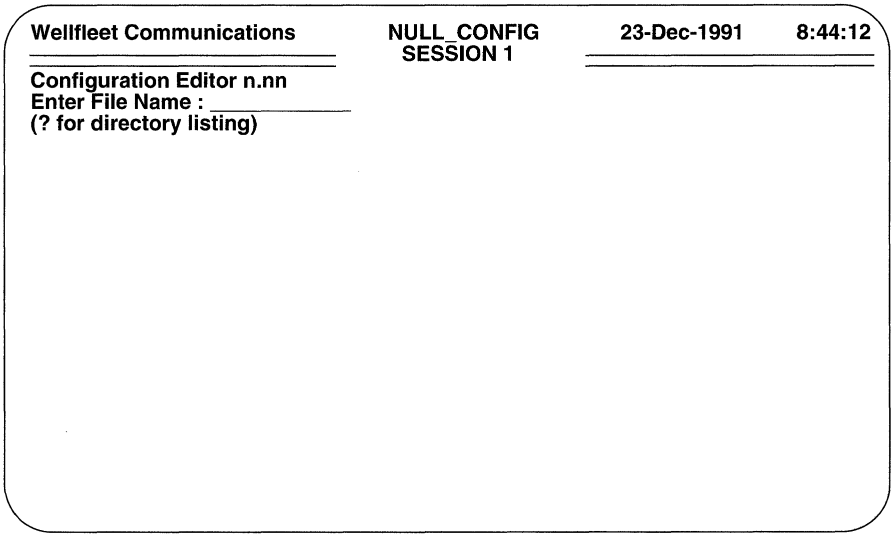
Of the four major items listed on the Main Menu (**Statistics Screen Menu**, **Network Control Language Interpreter**, **Configuration Editor**, and **Event Log**), this guide documents only the Configuration Editor. For information on the other items, refer to the *Operator's Guide.*

1.6 Accessing the Configuration Editor

You begin the configuration process from the Main Menu. Use the `[UPARROW]` (⇑) or `[DOWNARROW]` (⇓) to position the cursor at **Configuration Editor**, and press `[RETURN]`, or simply press `<3>`. The screen prompts for a file name, as shown in Figure 1-2.

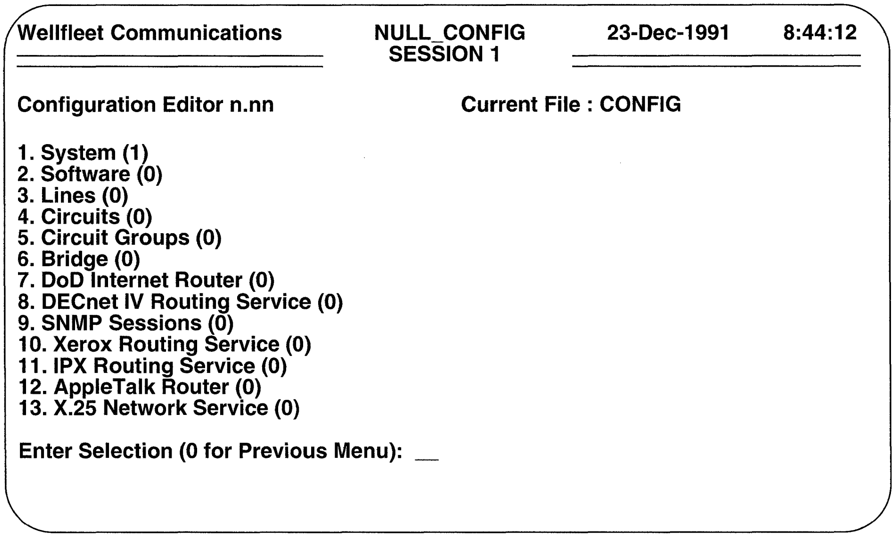
1.7 Creating *`config`*

You create *`config`* from the Configuration Editor Access Screen. To begin, enter `CONFIG` at **Enter File Name**, then press `[RETURN]`. The screen displays the Configuration Menu. Figure 1-3 shows a sample Configuration Menu which lists all possible menu items. The menu displayed on your screen lists only the application software modules supplied with your router.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1
Configuration Editor n.nn
Enter File Name : ___________
(? for directory listing)
```

Figure 1-2 Configuration Editor Access Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor n.nn                      Current File : CONFIG

1. System (1)
2. Software (0)
3. Lines (0)
4. Circuits (0)
5. Circuit Groups (0)
6. Bridge (0)
7. DoD Internet Router (0)
8. DECnet IV Routing Service (0)
9. SNMP Sessions (0)
10. Xerox Routing Service (0)
11. IPX Routing Service (0)
12. AppleTalk Router (0)
13. X.25 Network Service (0)

Enter Selection (0 for Previous Menu): __
```

Figure 1-3 Sample Configuration Menu

The Configuration Menu allows you to enter required network-specific data. Depending on your particular network topology and on the application or network-management software you want to install, you may need to access all, or only some, of the items on your Configuration Menu.

Menu items 1 through 5 (corresponding to Steps 1, 2, and 3 of the configuration process) are required for all routers. These items assign global parameter values, enable various session modes, load the application software modules, and define the physical and data-link layer connections between the router and network devices.

The additional menu items (corresponding to Step 4 of the configuration process) provide you with the mechanism for tailoring application and/or network-management software modules to your specific requirements. You access only those items that correspond to the application or network-management software modules you wish to enable.

Each menu item shown in Figure 1-3 is briefly described below; Chapters 2 through 15 discuss each item in detail.

1. System

   Assigns values to administrative parameters. Refer to Chapter 2, *Setting Administrative Parameters*, for detailed information.

2. Software

   Loads application software modules (routing, bridging, and network management protocols); refer to Chapter 3, *Loading Software*, for detailed information.

3. Lines

   Defines the router's physical layer connections; refer to Chapter 4, *Setting Physical Layer Parameters*, for detailed information.

4. Circuits

   Defines the router's data-link layer connections; refer to Chapter 5, *Setting Data-Link Layer Parameters*, for detailed information.

5. Circuit Groups

   Further defines data-link layer connections; refer to Chapter 7, *Building Circuit Groups*, for detailed information.

6. Bridge

   Configures the Bridge; refer to Chapter 8, *Configuring the Bridge*, for detailed information.

7. DoD Internet Router

   Configures the IP Router; refer to Chapter 9, *Configuring TCP/IP*, for detailed information.

8. DECNET IV Routing Service

   Configures the DECnet Phase IV router; refer to Chapter 11, *Configuring DECnet Phase IV*, for detailed information.

9. SNMP Sessions

   Configures network management agent software; refer to Chapter 10, *Configuring SNMP*, for detailed information.

10. Xerox Routing Service

    Configures the XNS router; refer to Chapter 12, *Configuring XNS*, for detailed information.

11. IPX Routing Service

    Configures the IPX router; refer to Chapter 13, *Configuring IPX*, for detailed information.

12. AppleTalk Router

    Configures the AppleTalk router; refer to Chapter 14, *Configuring AppleTalk*, for detailed information.

13. X.25 Network Service

    Configures X.25 packet switched services; refer to Chapter 6, *Configuring X.25 Service*, for detailed information.

2 Setting Administrative Parameters

To begin the configuration process, you assign values to administrative parameters. Certain administrative parameters, called global parameters, specify how the multiprotocol router initializes software services and how it reacts to system or network failure. Other administrative parameters, called session parameters, define the interface between the router and an input/output device or devices. This chapter first explains the assignment of values to global parameters; it then describes the various session modes. Finally, it explains the assignment of values to user-session parameters.

2.1 Setting Global Parameters

The global parameters are listed in Table 2-1.

Table 2-1: Global Parameters

Parameter	Function
System Name	identifies the multiprotocol router
Auto Enable	specifies the initialization state
Automatic Reboot	specifies response to a failure
Enable Logging	creates a log of router operations

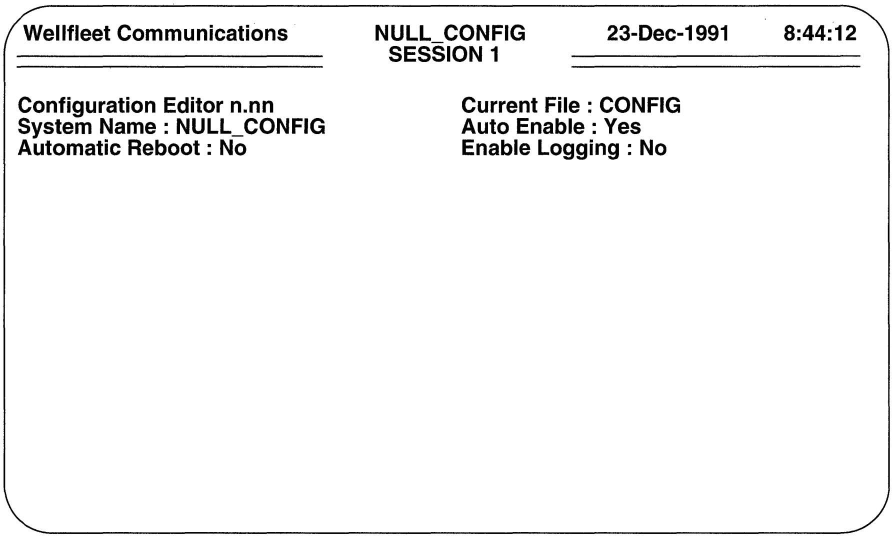
You set global parameters from the Configuration Menu. To begin, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The console screen displays the following prompt:

Action (--> for selections) : Previous Display

Press the `[RIGHTARROW]` to display **Modify**, then press `[RETURN]`. The screen displays the Global Parameters Screen (Figure 2-1).

- ❐ **System Name** identifies the router.

  Enter the name of the router. Do not use the `[SPACE]` character and ensure that the name contains no more than twelve alphanumeric characters.



```
Wellfleet Communications        NULL_CONFIG         23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor n.nn                 Current File : CONFIG
System Name : NULL_CONFIG                 Auto Enable : Yes
Automatic Reboot : No                     Enable Logging : No
```

Figure 2-1 Global Parameters Screen

- **Auto Enable** determines the state of the application software and circuits after the router boots.

  Yes, the default, specifies that the router, when booting, conditionally enables the resident application software modules (such as the Bridge or the IP Router) and all circuits.

  No specifies that the router does not enable the resident application software and circuits. If you choose **No**, you will need subsequently to enable application software and circuits manually with the NCL `ENABLE` command.

- **Automatic Reboot** determines the response to a router failure.

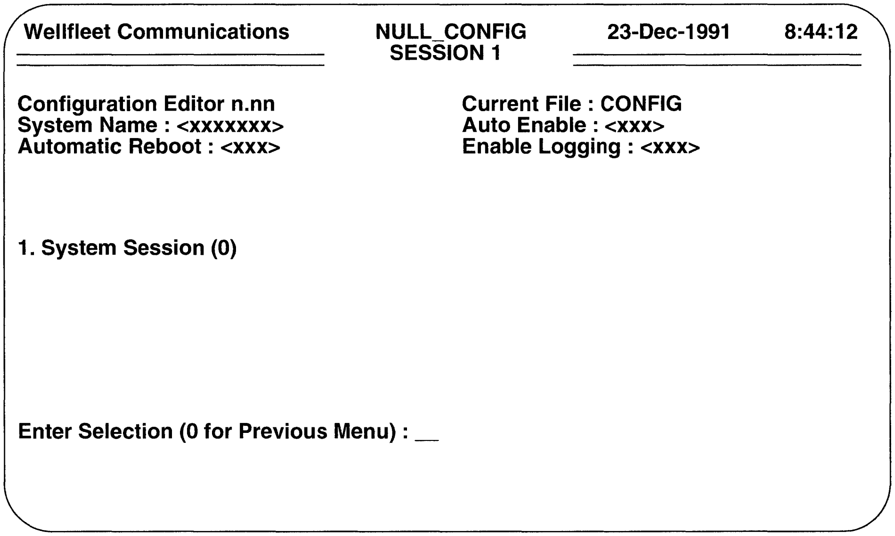
  No, the default, specifies that the router does not reboot in the event of a failure. Consequently, you would need to reboot manually. **Yes** specifies that the router automatically attempts to reboot in the event of failure.

- **Enable Logging** creates the log file, a file containing a sequential record of router-generated event messages.

  By default, the file is named *log*, and contains a maximum of 50 entries. Each file entry consists of a single event message.

  Yes creates the log file. **No** disables logging.

After you enable or disable logging, the console screen displays the Sessions Access Screen (Figure 2-2) to prompt for session data.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor n.nn                     Current File : CONFIG
System Name : <xxxxxxx>                       Auto Enable : <xxx>
Automatic Reboot : <xxx>                      Enable Logging : <xxx>


1. System Session (0)



Enter Selection (0 for Previous Menu) : __
```

Figure 2-2 Sessions Access Screen

2.2 Assigning the Session Mode

Session modes correspond to the input/output device(s) that transmit data to and/or receive data from the router. There are four session modes:

User mode

Employs a directly connected console or terminal device (or a similar device connected to the router with a modem) in an interactive fashion to exchange data with the router.

Telnet mode

Employs the Internet virtual terminal protocol (*telnet*) to establish a connection between a remote IP host and the router. Telnet mode is identical to user mode save for the connection type.

Disk logging mode

Employs file space on the system disk to store router-generated event messages.

Printer mode

Employs a hard-copy device to collect router-generated event messages. Like disk logging mode, printer mode is unidirectional (data flow is from the router to the hard-copy device) and non-interactive.

Because creation of `config` generally involves the user mode, only that mode is described in this chapter. Refer to Appendix B for information on establishing disk logging, telnet, or printer sessions.

2.3 Setting User-Session Parameters

The user-session parameters are: listed in Table 2-2.

Table 2-2: User Session Parameters

Parameter	Function
Event Filter Level	specifies console screen displays
Device ID	identifies a physical connector
Terminal	specifies a terminal type
Flow Control	enables XON/XOFF protocol
Baud Rate	specifies the data transfer rate
Parity	enables parity checking
Bit/Char	specifies word length
Stop Bits	specifies inter-character spacing
Enable Modem Control	enables modem signalling
Screen Refresh Rate	specifies the screen update cycle

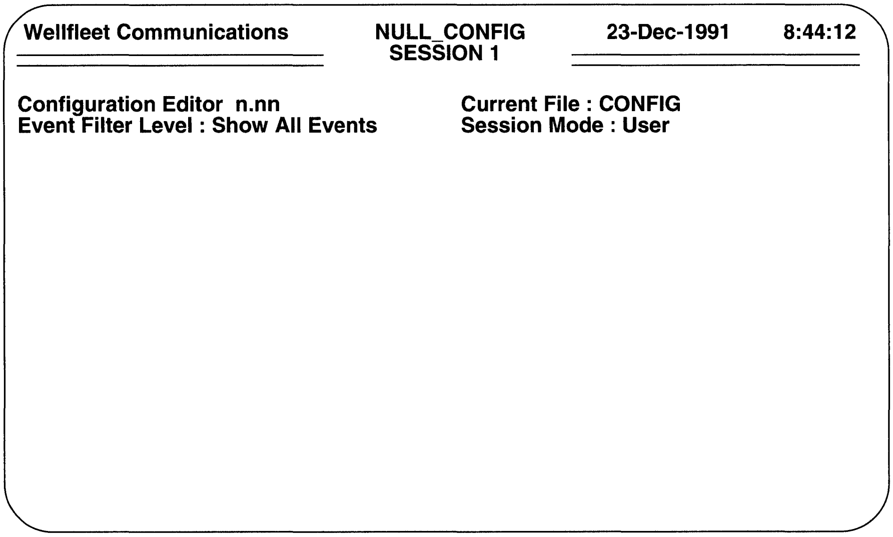
You set user-session parameters from the Sessions Access Screen. To begin, enter `<1>` at **Enter selection (0 for Previous Menu)**. The console screen displays the following prompt:

No System Session record(s) found
Do you wish to add System Session record(s)?

Press **`[RETURN]`** to accept the default response, **Yes**. The console screen displays the Session Selection Screen (Figure 2-3).

❒ **Event Filter Level** specifies which router-generated event messages are displayed on the screen.

While the router operates, it generates event messages in response to changes in network service, changes in performance, and the occurrence of anomalous events. Event messages are always written to the RAM-based Event Log. The *Operator's Guide* tells you how to access and interpret the Event Log. In addition, you can set the **Event Filter Level** parameter to have all, or some, of these messages displayed on the console screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Event Filter Level : Show All Events          Session Mode : User
```

Figure 2-3 Session Selection Screen

Event messages have five levels of severity:

Major	A service has appeared or disappeared
Warning	A service has behaved unexpectedly
Performance	A service has upgraded/degraded
Information	General system information
Debug	Installation/diagnostic information

There are six available responses to **Event Filter Level**:

Debug Events	Displays all event messages
Show All Events	Displays Major/Warning/Performance/Info
Not INFO	Displays Major/Warning/Performance
PERF and MAJOR	Displays Major/Performance
Just MAJOR	Displays Major
Drop All	Displays no event messages

Press the `[RIGHTARROW]` to select the response that displays the messages you want to see on the screen, then press `[RETURN]`.

❐ **Session Mode** specifies the session type.

Press `[RETURN]` to select, **User**.

After you specify a User session, the console screen displays the User-Session Parameters Screen (Initial) shown in Figure 2-4.

❐ **Device ID** identifies the physical port on the System I/O board to which the console is connected.

The available responses (with each response identifying a connector on the System I/O board) are:

Console **Printer**
Modem1 **Modem2**

Select the appropriate port.

❐ **Terminal** identifies the type of console device.

The available responses are:

ANSI **VT100**

If your console is ANSI-compatible, select **ANSI**. If the console is a VT100, or VT100-compatible, select **VT100**.

The console screen displays the User-Session Parameters Screen (Final) shown in Figure 2-5.

❐ **Flow Control** enables or disables XON/XOFF protocol, which controls the rate of data transfer between the console and the router.

The available responses are **XON/OFF** (enabling the protocol) and **None** (disabling the protocol).

❐ **Baud Rate** sets the rate of data transfer between the console and the router.

The available responses are:

9600 **2400** **300**
4800 **1200**

❐ **Parity** assigns a value to the eighth bit of each ASCII character transmitted by the router.

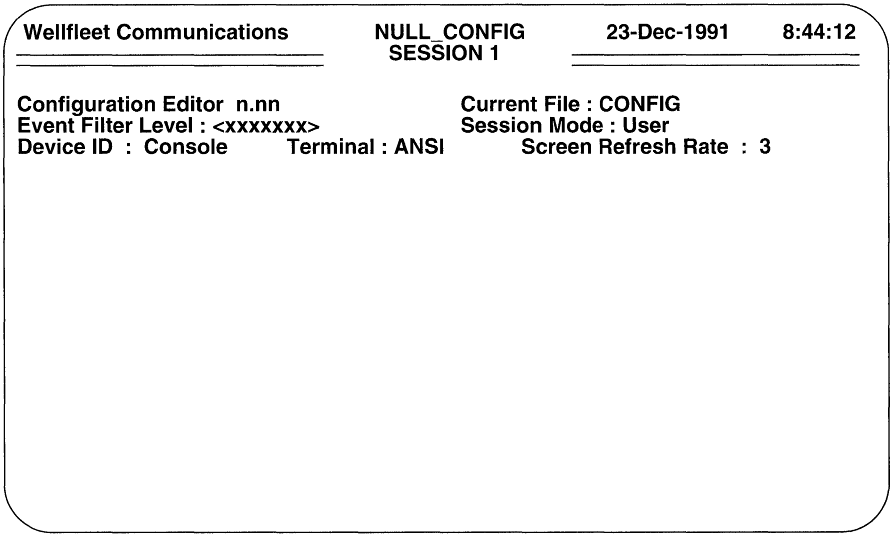
The available responses are:

None **Odd** **Even**

❐ **Bit/Char** specifies the number of bits in each ASCII character received or transmitted by the router.

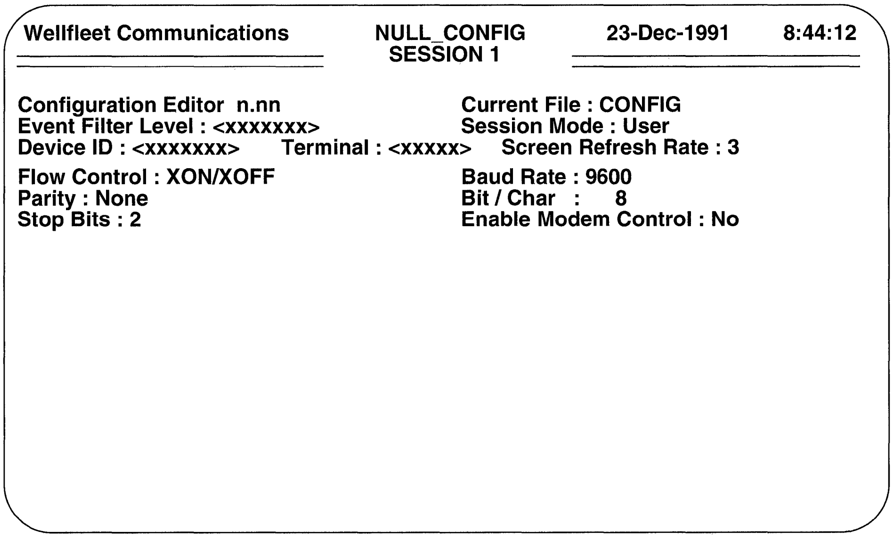
The available responses are:

8 **7**



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Event Filter Level : <xxxxxxx>                 Session Mode : User
Device ID  :  Console       Terminal : ANSI        Screen Refresh Rate  :  3
```

Figure 2-4 User-Session Parameters Screen (Initial)



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Event Filter Level : <xxxxxxx>                 Session Mode : User
Device ID : <xxxxxxx>     Terminal : <xxxxx>   Screen Refresh Rate : 3
Flow Control : XON/XOFF                        Baud Rate : 9600
Parity : None                                  Bit / Char  :     8
Stop Bits : 2                                  Enable Modem Control : No
```

Figure 2-5 User-Session Parameters Screen (Final)

❐ **Stop Bits** specifies the number of bits that follow each ASCII character received or transmitted by the router.

The available responses are:

2

1

1.5

❐ **Enable Modem Control** specifies the type of connection between the console device and the router.

The available responses are:

No

Yes

If the console is directly connected to the router, simply press `[RETURN]`; if the console/router connection is accomplished through a modem, select **Yes**.

❐ **Screen Refresh Rate** specifies the rate (in seconds per cycle) at which the node updates the display of various reporting metrics. You can access these metrics from the Statistics Screen Menu. The *Operator's Guide* tells you how to access and interpret reporting metrics.

The available responses are:

3

5

10

20

30

45

60

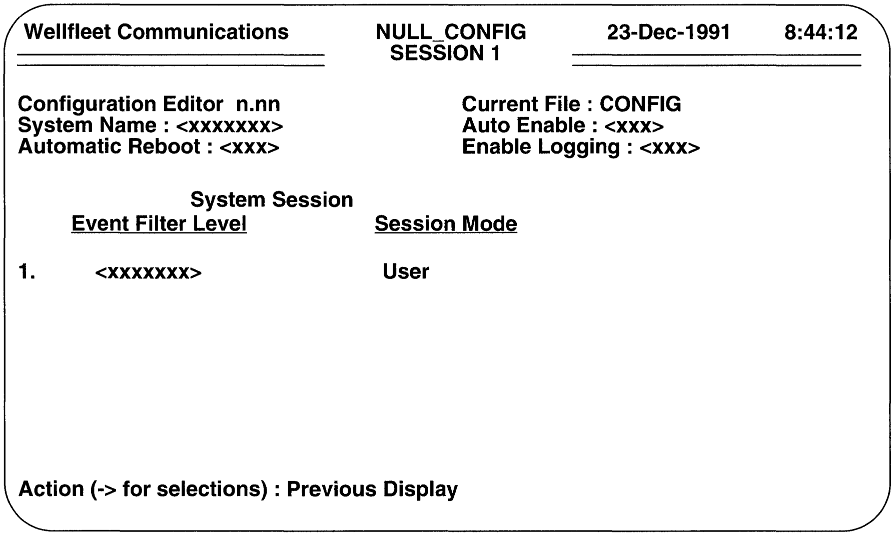
1

When the screen displays **Hit Return to Continue**, press `[RETURN]` to display the Sessions Access Screen (Figure 2-2) which now echoes the values you assigned to the **System Name**, **Auto Enable**, **Automatic Reboot**, and **Enable Logging** parameters.

System Session (1) verifies the creation of a single session record. This record contains the values you assigned to user-session parameters. To obtain a listing of all sessions, you can enter `<1>` at **Enter Selection (0 for Previous Menu)**. The console screen displays the Sessions Summary Screen (Figure 2-6).

The Sessions Summary Screen lists all sessions that you have configured, along with the associated event filter level. If you wish, you can use the **BROWSE** command (refer to Appendix A) to obtain a complete listing of session-specific parameters.

Or, you can use the **ADD** command to configure a printer, disk logging, or telnet session (Refer to Appendix B). If you do not want to establish additional sessions at this time, however, press [`RETURN`] twice to revert to the Configuration Menu.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                    SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
System Name : <xxxxxxx>                     Auto Enable : <xxx>
Automatic Reboot : <xxx>                    Enable Logging : <xxx>

                    System Session
     Event Filter Level               Session Mode

1.       <xxxxxxx>                     User




Action (-> for selections) : Previous Display
```

Figure 2-6 Sessions Summary Screen

3 Loading Software

This chapter tells you how to load application software (routing or bridging protocols).

The system diskette provides a copy of up to six routing/bridging modules:

- ❐ AppleTalk Router
- ❐ Bridge
- ❐ DECnet Phase IV Router
- ❐ IPX Router
- ❐ TCP/IP Router
- ❐ XNS Router

As part of the boot process, the multiprotocol router loads copies of routing/bridging software into the memory of Advanced Communication Engines (ACEs) housed within the router cabinet. Which software is loaded to which ACE is determined by instructions in `config`. The procedures contained in this chapter tell you how to prepare the portion of `config` that provides these load instructions.

3.1 Loading Software to the Master Slot

The software parameters are listed in Table 3-1.

Table 3-1: Software Load Parameters

Parameter	Function
Software	specifies a routing, bridging, or management protocol
Slot	specifies an ACE board

You first load routing/bridging modules to Slot 2 (the so-called “master slot”). If the router uses the AppleTalk Router, the DECnet Phase IV Routing Service, the IPX Routing Service, the TCP/IP Router, or the XNS Routing Service, you must load a copy of each module to the master slot. Additionally, if the router bridges traffic through the master slot, you must load a copy of the Bridge module to Slot 2.

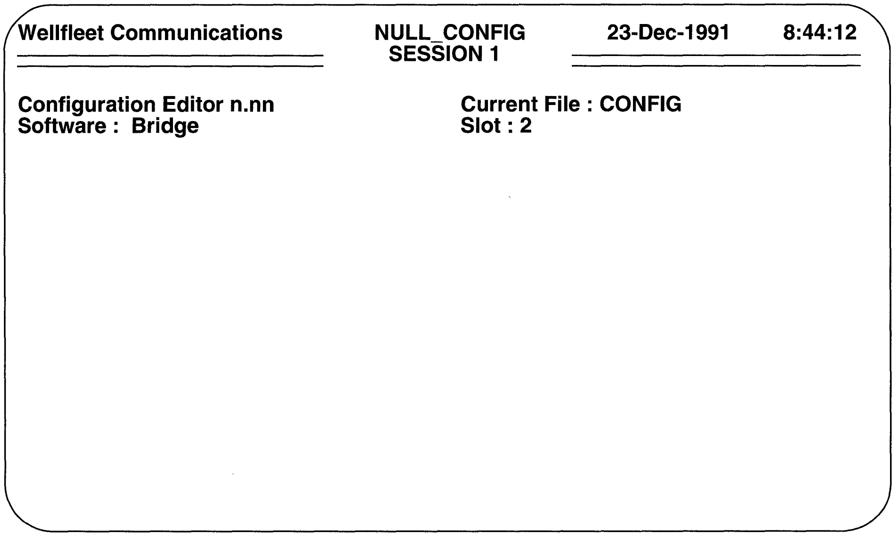
NOTE

Do not load Bridge software to any slot (including the master slot) that does not bridge traffic. Load the bridge software only to slots that actually participate in bridging.

You load routing software one application at a time (and in any order) from the Configuration Menu. To begin, enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Software record(s) found
Do you wish to add Software record(s)?

Press `[RETURN]` to accept the default response, **Yes**. The screen displays the Software Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor n.nn                   Current File : CONFIG
Software :  Bridge                          Slot : 2
```

Figure 3-1 Software Screen

- ❒ **Software** identifies the routing software loaded to the master slot.

  Select the software application that you wish to load to Slot 2.

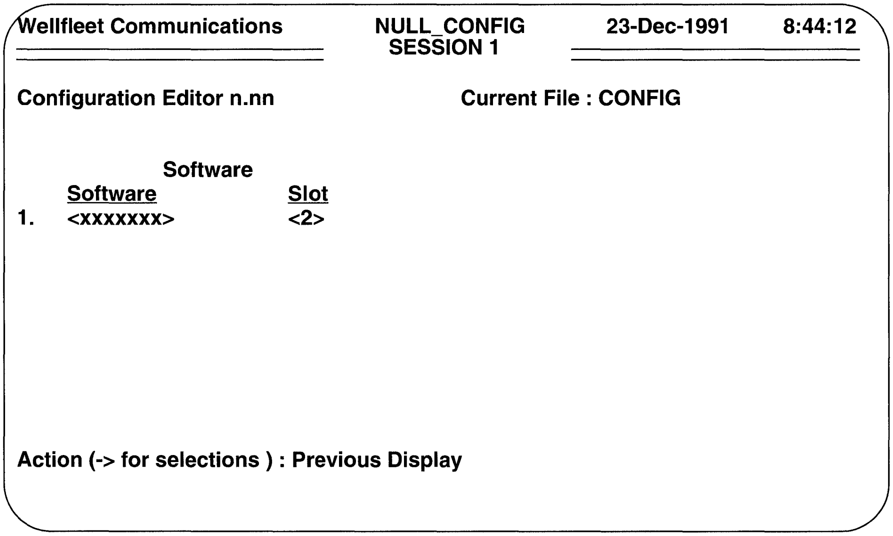
- ❒ **Slot** identifies the master slot.

  Press `[RETURN]` to accept the default value, **2**.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Configuration Menu.

After loading the initial software application to the master slot, you use the Configuration Editor **ADD** command to load additional software applications (if required) to Slot 2. You load additional applications from the Configuration Menu. To begin, enter **<2>** at **Enter Selection (0 for Previous Menu)**.

The screen displays the Routing/Bridging Software Summary Screen, which provides a list of all the routing software that you have previously loaded to Slot 2.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor n.nn                    Current File : CONFIG


                Software
     Software                Slot
1.   <xxxxxxx>               <2>







Action (-> for selections ) : Previous Display
```

Figure 3-2 Software Summary Screen

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`; the screen again displays the Software Screen. Now follow the same procedure described in this section to load an additional routing/bridging module to the master slot; repeat this procedure until you have loaded all required software to the master slot.

3.2 Loading Additional Software

After loading copies of the routing software to the master slot, you load additional copies of the software to other slots. If protocol traffic (for example, IP packets) is to be routed through a specific ACE, you must load matching routing software to that ACE.

You again load software from the Configuration Menu. Begin by entering **<2>** at the **Enter Selection (0 for Previous Menu)** prompt. In response, the screen displays the Software Summary Screen. At **Action (-> for selections)**, press the

[RIGHTARROW] to display **Add**, then press [RETURN]; the screen displays the Software Screen.

As you did previously, you use this screen to set two parameters:

- ❐ **Software** identifies the routing software that you wish to load.

  Select the software application that you wish to load.

- ❐ **Slot** identifies the slot number that houses the ACE into whose memory the software is loaded.

  Depending upon the model, the router contains 2, 5, or 14 PCB slots. On models with two or five slots, slot numbers are assigned from bottom to top, with the bottom slot designated Slot 1 and the topmost slot designated either Slot 2 or Slot 5. On 14-slot models, slot numbers are assigned from right to left (when viewed from the back of the cabinet), with the right-most slot designated Slot 1.

NOTE

Within any router, Slot 1 always contains the System I/O board Do not load routing/bridging software to Slot 1.

Press the [RIGHTARROW] to display the appropriate slot number (from **3** to **14**), then press [RETURN].

When the screen prompts **Hit Return to Continue**, press [RETURN] to go back to the Configuration Menu. Now follow the procedure described in this section to load an additional routing/bridging module; repeat this procedure until you have loaded all required software.

4 Setting Physical Layer Parameters

This chapter tells you how to describe the physical layer connections between the multiprotocol router and network devices. Such connections are called *lines*. Lines are physical layer entities that provide connections between the router and local area networks and/or long-haul transmission facilities. When you set physical layer parameters, you provide the router with information describing the mechanical, electrical, and procedural characteristics of these connections.

There are six types of lines: Ethernet (IEEE 802.3) lines, synchronous lines, T1 (DS1) lines, E1 (CEPT) lines, token ring lines, and fiber distributed data interface (FDDI) lines.

The following sections provide a series of step-by-step procedures describing how to establish an initial Ethernet/IEEE 802.3 (called simply "Ethernet" in this guide), synchronous, T1, E1, token ring, or FDDI line. They also describe how to establish additional lines of the same type. Depending on your network topology, you may need to refer to all, or only some of, these sections.

4.1 Establishing Ethernet Lines

The Ethernet line parameters are listed in Table 4-1.

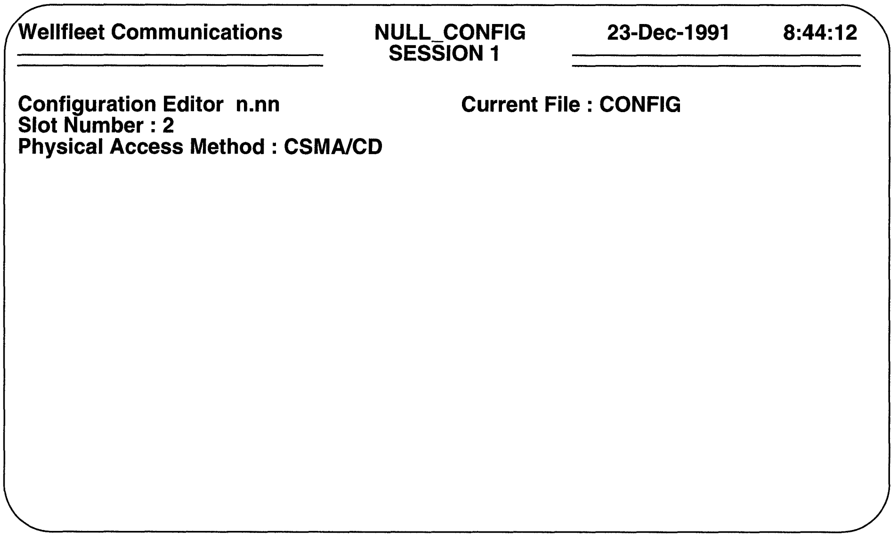
Table 4-1: Ethernet Line Parameters

Parameter	Function
Slot Number	specifies a link module
Physical Access Method	specifies a line access protocol
Connector	specifies a physical connector
Circuit Name	specifies a circuit name

You establish an Ethernet line from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Lines record(s) found
Do you wish to add Lines record(s)?

Press `[RETURN]` to display the Line Parameters Screen (Figure 4-1).



```
Wellfleet Communications         NULL_CONFIG        23-Dec-1991      8:44:12
                                  SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Slot Number : 2
Physical Access Method : CSMA/CD
```

Figure 4-1 Line Parameters Screen

❒ **Slot Number** identifies the backplane slot that houses the physical connector for the Ethernet line that you are establishing.

Select the appropriate slot number.

❒ **Physical Access Method** specifies the line type.

To establish an Ethernet line, press `[RETURN]` to select, **CSMA/CD** (Carrier Sense Multiple Access/with Collision Detection).

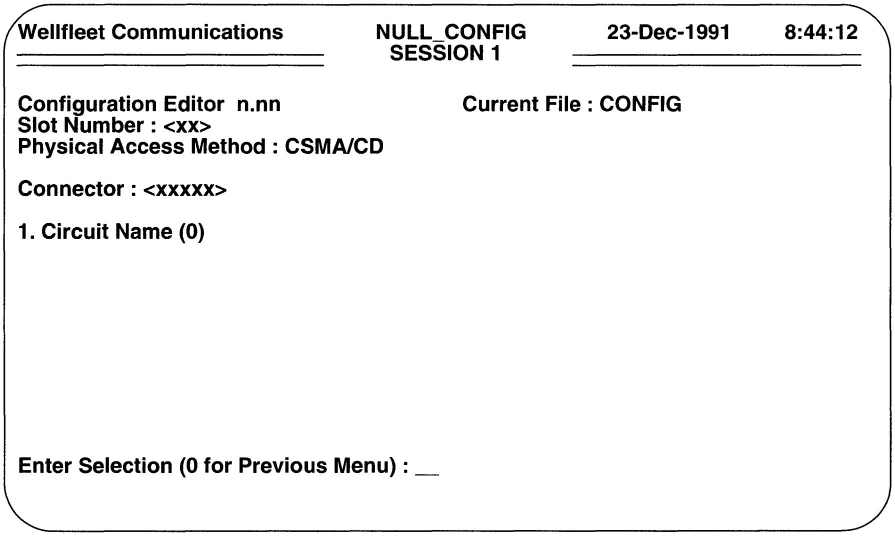
The screen prompts for **Connector.**

❒ **Connector** identifies the specific physical connector to the Ethernet medium.

If you are establishing a line terminated by a connector labeled either XCVR or XCVR1, select **XCVR1**. If you are establishing a line terminated by a connector labeled XCVR2, select **XCVR2**.

After you press `[RETURN]`, the screen displays the Ethernet Circuit Access Screen (Figure 4-2) to prompt for a circuit name.

You must assign a unique circuit name to each Ethernet line. Later, you will use this unique name to assign circuit-specific, data-link layer parameters and to configure application software modules.



```
Wellfleet Communications        NULL_CONFIG      23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Slot Number : <xx>
Physical Access Method : CSMA/CD

Connector : <xxxxx>

1. Circuit Name (0)






Enter Selection (0 for Previous Menu) : __
```

Figure 4-2 Ethernet Circuit Access Screen

Circuit names consist of up to 12 characters. You can use any printable character *except for the period (.)* when assigning a circuit name. Because you use circuit names later in the configuration process, it is vital that you maintain an accurate record of line and circuit names. You may wish to use the *Ethernet Line Summary Chart* in Appendix C to maintain a record of line and circuit names.

To assign a circuit name, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays:

> **No Circuit Name record(s) found**
> **Do you wish to add Circuit Name record(s)?**

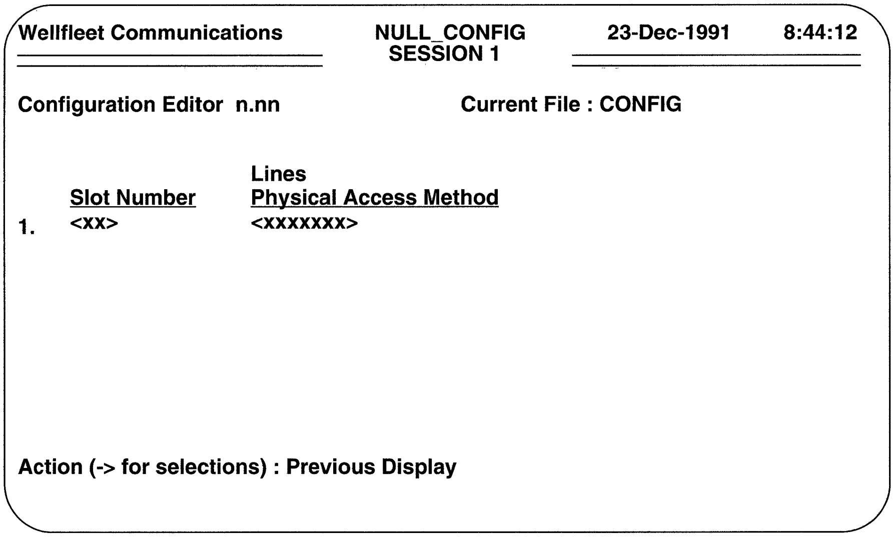
Press `[RETURN]`. When the screen prompts for **Circuit Name**, enter a circuit name, then press `[RETURN]`.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to display the Ethernet Circuit Access Screen. This screen echoes your responses to **Slot Number**, **Physical Access Method**, and **Connector**. **Circuit Name (1)** verifies that you have assigned a circuit name to this Ethernet line.

Enter `<0>` at **Enter Selection (0 for Previous Menu)** to return to the Configuration Menu.

4.2 Adding Ethernet Lines

You establish additional Ethernet lines from the Configuration Menu. Enter <3> at **Enter Selection (0 for Previous Menu)**. As you have already established an Ethernet Line, the screen displays the Lines Summary Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG


                         Lines
     Slot Number         Physical Access Method
1.   <XX>                <XXXXXXX>






Action (-> for selections) : Previous Display
```

Figure 4-3 Lines Summary Screen

The Line Summary Screen lists the slot number and physical access method for all previously configured lines. Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Line Parameters Screen. Now follow the procedure described in Section 4.1 to establish an additional Ethernet line; repeat this procedure until you have established all Ethernet lines.

4.3 Establishing Synchronous Lines

The synchronous line parameters are listed in Table 4-2.

You establish a synchronous line from the Configuration Menu. Enter <3> at **Enter Selection (0 for Previous Menu)**. If you have not previously configured any lines, the screen displays the following:

No Lines record(s) found
Do you wish to add Lines record(s)?

Press `[RETURN]` to display the Line Parameters Screen.

Table 4-2: Synchronous Line Parameters

Parameter	Function
Slot Number	specifies a link module
Physical Access Method	specifies a line access protocol
Connector	specifies a physical connector
Signal Mode	specifies a transmission type
Clock Source	specifies internal or external clocking
Clock Speed	specifies timing
RTS/CTS Control	enables RTS/CTS flow control
Circuit Name	specifies a circuit name

However, if you have previously established lines, the screen displays the Lines Summary Screen. To move to the Line Parameters Screen, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

- ❒ **Slot Number** identifies the backplane slot that houses the physical connector for the synchronous line that you are establishing. Select the appropriate slot number.
- ❒ **Physical Access Method** specifies the line type.

  To establish a synchronous line, press the `[RIGHTARROW]` to display **SYNC**, then press `[RETURN]`.

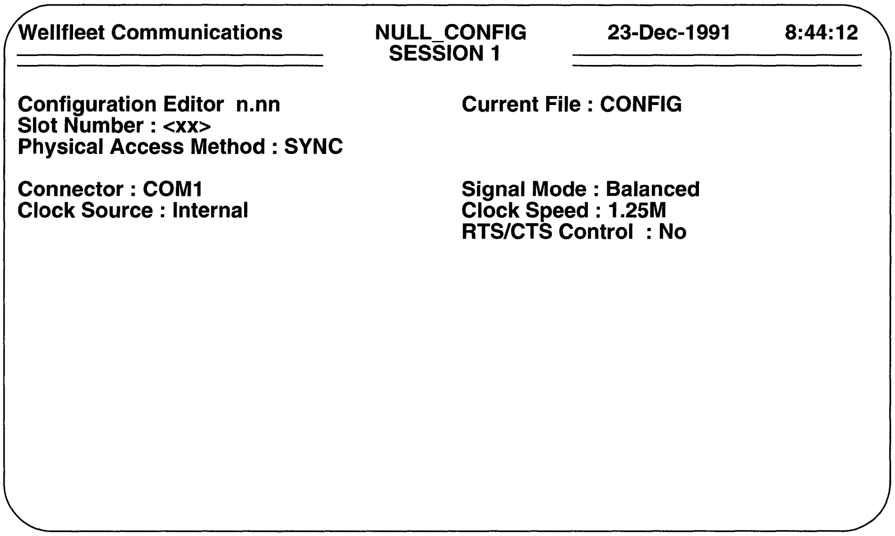
The screen displays the Synchronous Line Parameters Screen (Figure 4-4).

- ❒ **Connector** identifies the specific physical connector to which the synchronous line interfaces.

  The available responses are: **COM1**, **COM2**, **COM3**, **COM4**.

  Select the appropriate response.
- ❒ **Signal Mode** selects between balanced and unbalanced transmission.

  Balanced transmission (**Balanced**) uses two conductors to carry signals; unbalanced transmission (**Unbalanced**) uses a single conductor to carry a signal, with a ground providing the return path. Select the appropriate response on the basis of the signaling mode of the connected device.



```
Wellfleet Communications          NULL_CONFIG       23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Slot Number : <xx>
Physical Access Method : SYNC

Connector : COM1                            Signal Mode : Balanced
Clock Source : Internal                     Clock Speed : 1.25M
                                            RTS/CTS Control  : No
```

Figure 4-4 Synchronous Line Parameters Screen

- ❒ **Clock Source** identifies the origin of the synchronous timing signals.

  The available responses are: **Internal** (indicating that the router supplies required timing signals) and **External** (indicating that an external network device supplies required timing signals).

  In virtually all field applications, network devices provide timing signals. In these instances, select **External**.

NOTE

The upper limit for external clocking is 6.144 Mb/s.

Some test environments, however, do require an internal clock. In these instances select **Internal**.

- ❒ **Clock Speed** specifies the speed of the internal clock.

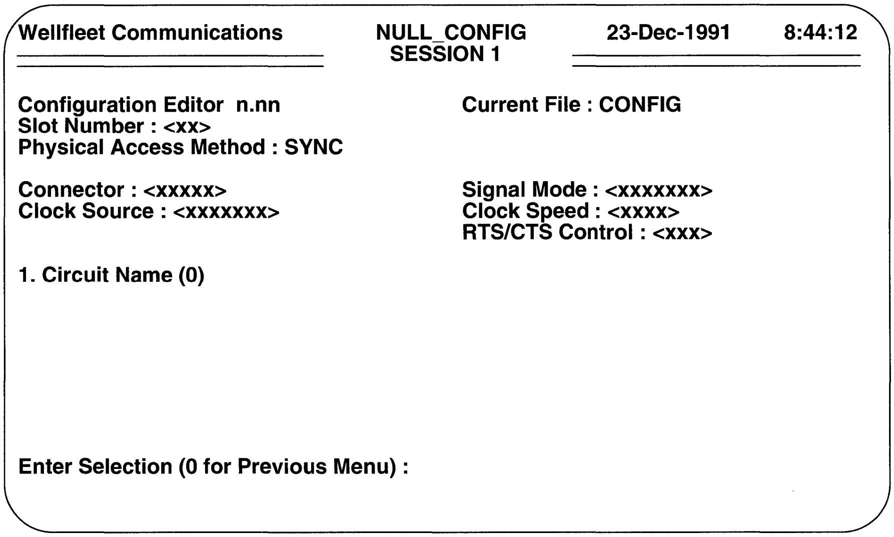
  If the external network provides timing signals (**Clock Source** is **External**), this parameter is non-functional. Press `[RETURN]` to accept the default value.

  If the router provides timing signals, select the value that equals the data transmission rate across the synchronous line.

- ❐ **RTS/CTS Control** enables or disables RTS/CTS flow control.

  If the connected device (for example, a modem) uses RTS/CTS flow control, select **Yes**; otherwise, select **No**.

The screen displays the Synchronous Circuit Access Screen to prompt for a circuit name.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Slot Number : <xx>
Physical Access Method : SYNC

Connector : <xxxxx>                            Signal Mode : <xxxxxxx>
Clock Source : <xxxxxxx>                       Clock Speed : <xxxx>
                                               RTS/CTS Control : <xxx>

1. Circuit Name (0)





Enter Selection (0 for Previous Menu) :
```

Figure 4-5 Synchronous Circuit Access Screen

You must assign a unique circuit name to each synchronous line. Later, you will use this unique name to assign circuit-specific parameters and to configure application software modules.

Circuit names consist of up to 12 characters. You can use any printable character *except for the period (.)* when assigning a circuit name. Because you use circuit names later in the configuration process, it is very important that you maintain an accurate record of line and circuit names. You may wish to use the *Synchronous Line Summary Chart* in Appendix C to maintain a record of line and circuit names.

To assign a circuit name, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Circuit Name record(s) found
Do you wish to add Circuit Name record(s)?

Press `[RETURN]`. After the screen prompts for **Circuit Name**, enter a circuit name, then press `[RETURN]`.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to display the Synchronous Circuit Access Screen. The screen echoes your responses to **Slot Number**, **Physical Access Method**, **Connector**, **Signal Mode**, **Clock Source**, **Clock Speed**, and **RTS/CTS Control**. **Circuit Name (1)** verifies that you have assigned a circuit name to this synchronous line. Enter `<0>` at **Enter Selection (0 for Previous Menu)** to return to the Configuration Menu.

4.4 Adding Synchronous Lines

You establish additional synchronous lines from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Lines Summary Screen. This screen lists the slot number and physical access method for all configured lines.

Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Line Parameters Screen. Now follow the procedure described in Section 4.3 to establish an additional synchronous line; repeat this procedure until you have established all synchronous lines.

4.5 Establishing T1 Lines

The T1 line parameters are listed in Table 4-3.

Table 4-3: T1 Line Parameters

Parameter	Function
Slot Number	specifies a link module
Physical Access Method	specifies a line access protocol
Connector	specifies a physical connector
Frame Type	specifies frame format
Line Buildout	conditions signal attenuation
B8ZS Supported	enables binary 8 zeros suppression
Clock Mode	specifies the transmit clock
Circuit 1 Name	specifies the first T1 circuit
Circuit 2 Name	specifies the second T1 circuit
MiniDACS Configuration	allocates DS0 channels

You establish a T1 line from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured any lines, the screen displays the following:

No Lines record(s) found
Do you wish to add Lines record(s)?

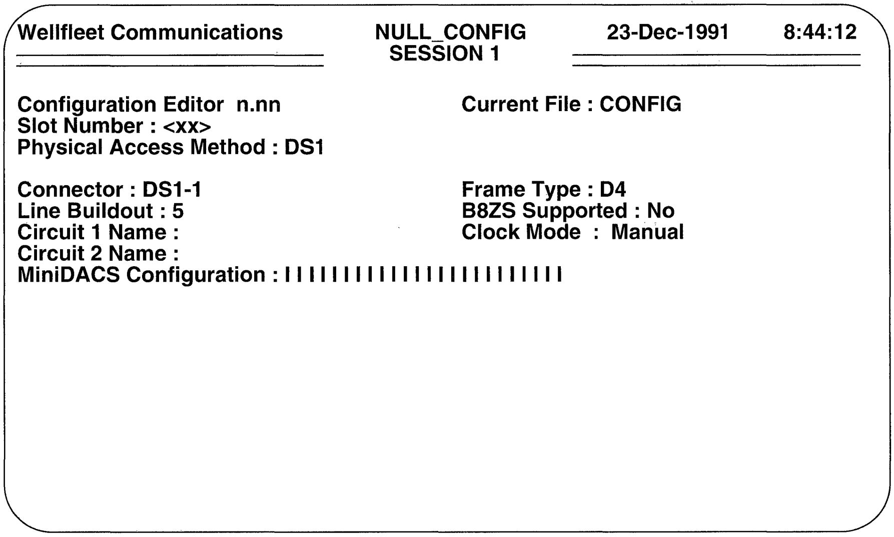
Press `[RETURN]` to display the Line Parameters Screen.

However, if you have previously established lines, the screen displays the Lines Summary Screen. To move to the Line Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

- ❐ **Slot Number** identifies the backplane slot that houses the physical connector for the T1 line that you are establishing. Select the appropriate slot number.
- ❐ **Physical Access Method** specifies the line type.

  To establish a T1 line, press the `[RIGHTARROW]` to display **DS1**, then press `[RETURN]`.

The screen displays the T1 Line Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Slot Number : <xx>
Physical Access Method : DS1

Connector : DS1-1                             Frame Type : D4
Line Buildout : 5                             B8ZS Supported : No
Circuit 1 Name :                              Clock Mode  :  Manual
Circuit 2 Name :
MiniDACS Configuration : IIIIIIIIIIIIIIIIIIIIIIII
```

Figure 4-6 T1 Line Parameters Screen

❐ **Connector** identifies the specific physical connector to which the T1 line interfaces.

The available responses are: **DS1-1** or **DS1-2**. Select the appropriate response.

❐ **Frame Type** differentiates between two tariffed framing formats: **D4** or **ESF** (Extended Super Frame).

The D4 framing format is commonly used by channel banks. It transmits superframes consisting of 12 individual D4 frames. D4 provides two bits for rudimentary signaling functions. The ESF framing format, used by some PBXs, transmits superframes consisting of 24 individual D4 frames. ESF provides four bits for signaling functions, synchronization, and error checking.

Select the appropriate response on the basis of the frame format required by the attached T1 equipment.

❐ **Line Buildout** conditions generated signals (from 6 Volts to 3 Volts, peak-to-peak) in order to overcome signal attenuation.

Because attenuation correlates with line length, use the keyboard to enter the approximate length of the cable (from 1 to 655 feet) connecting the associated T1 device.

❐ **B8ZS Supported** enables or disables binary 8 zeros suppression (a scheme to maintain sufficient ones-density within the T1 data stream).

Synchronization between connected T1 devices is accomplished by means of the received signal. The absence of a sufficient number of logical ones within the received signal can cause carrier loss.

Select **Yes** (enable B8ZS) or **No** (disable B8ZS) on the basis of the ability of the connected device to implement binary 8 zeros suppression.

❐ **Clock Mode** specifies the source of the T1 transmit clock.

Three responses are available: **Manual**, **Slave**, or **Master**.

Manual (the default) selects the clock source on the basis of hardware jumpers on the T1 printed circuit board (refer to the *Installation Guide* for additional information on jumper settings and on T1 clocking). **Slave** overrides the jumper settings and places the T1 connection is slave mode. In slave mode, the transmit clock is derived from the received data stream. **Master** also overrides the jumper settings, but places the T1 connection in master mode. In master mode, the transmit clock is internally generated.

Select the clocking mode on the basis of network requirements.

❐ **Circuit 1 Name** identifies the first circuit carried by the T1 line.

Like Ethernet and synchronous lines, each T1 line requires an associated and unique circuit name. Unlike Ethernet and synchronous lines, however, a single T1 line can carry a second circuit. If you establish a second circuit, it too requires a unique circuit name. Later, you will use these unique names to assign circuit-specific parameters and to configure application software modules.

Circuit names consist of up to 12 characters. You can use any printable character ***except for the period (.)*** when assigning a circuit name. Because you use circuit names later in the configuration process, it is very important that you maintain an accurate record of line and circuit names. You may wish to use the *T1 Line Summary Chart* in Appendix C to maintain a record of line and circuit names.

Enter the circuit name from the keyboard, then press `[RETURN]`.

❐ **Circuit 2 Name** identifies the second circuit carried by the T1 line.

If you are enabling a second circuit, enter its name, otherwise press `[RETURN]`.

❐ **MiniDACS Configuration** assigns each T1 channel to a specific function.

The string of 24 **I**s represents the default state of each of the 24 DS0 channels. Channel assignment options are as follows:

I	--	Idles the channel (default)
D	--	Assigns the channel to data pass through
V	--	Assigns the channel to voice pass through
1	--	Assigns the channel to Circuit 1
2	--	Assigns the channel to Circuit 2

With the cursor positioned on the first **I** (DS0 channel 1), press the `[RIGHTARROW]` to display the desired channel assignment, then press `[RETURN]`. The cursor moves one position to the right (DS0 channel 2).

Continue in this fashion until you have assigned each of the 24 DS0 channels.

When you finish, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the Configuration Menu.

4.6 Adding T1 Lines

You establish additional T1 lines from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Lines Summary Screen. This screen lists the slot number and physical access method for all configured lines.

Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Line Parameters Screen. Now follow the procedure described in Section 4.5 to establish an additional T1 line; repeat this procedure until you have established all T1 lines.

4.7 Establishing E1 Lines

The E1 line parameters are listed in Table 4-4.

Table 4-4: E1 Line Parameters

Parameter	Function
Slot Number	specifies a link module
Physical Access Method	specifies a line access protocol
Connector	specifies a physical connector
Clock Mode	specifies the transmit clock
HDB3 Supported	enables high-density bipolar coding
Circuit 1 Name	specifies the first E1 circuit
Circuit 2 Name	specifies the second E1 circuit
Slot 1-31 Configuration	allocates E1 channels

You establish an E1 line from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured any lines, the screen displays the following:

No Lines record(s) found
Do you wish to add Lines record(s)?

Press `[RETURN]`. The screen displays the Line Parameters Screen.

However, if you have previously established lines, the screen displays the Lines Summary Screen. To move to the Line Parameters Screen, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

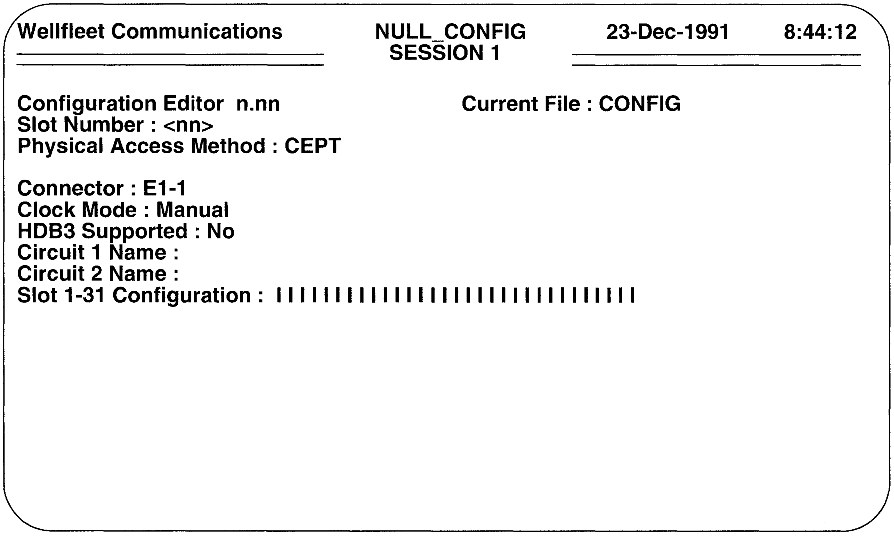
- ❐ **Slot Number** identifies the backplane slot that houses the physical connector for the E1 line that you are establishing.

  Select the appropriate slot number.

- ❐ **Physical Access Method** specifies the line type.

  To establish an E1 line, press the `[RIGHTARROW]` to display **CEPT**, then press `[RETURN]`.

The screen displays the E1 Line Parameters Screen (Figure 4-7).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Slot Number : <nn>
Physical Access Method : CEPT

Connector : E1-1
Clock Mode : Manual
HDB3 Supported : No
Circuit 1 Name :
Circuit 2 Name :
Slot 1-31 Configuration : I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I I
```

Figure 4-7 E1 Line Parameters Screen

- ❒ **Connector** identifies the specific physical connector to which the E1 line interfaces.

  The available responses are: **E1-1** or **E1-2**.

  Select the appropriate response.

- ❒ **Clock Mode** specifies the source of the E1 transmit clock.

  Three responses are available: **Manual**, **Slave**, or **Master**.

  Manual (the default) selects the clock source on the basis of hardware jumpers on the E1 printed circuit board (refer to the *Installation Guide* for additional information on jumper settings and on E1 clocking). **Slave** overrides the jumper settings and places the E1 connection is slave mode. In slave mode, the transmit clock is derived from the received data stream. **Master** also overrides the jumper settings, but places the E1 connection in master mode. In master mode, the transmit clock is internally generated.

  Select the clocking mode on the basis of network requirements.

- ❒ **HDB3 Supported** enables or disables High Density Bipolar coding (a scheme to maintain sufficient ones-density within the E1 data stream).

  Synchronization between connected E1 devices is maintained by means of the received signal; the signal edges provide the timing information. The presence of an extended string of logical zeros within the received signal can cause synchronization loss. To guard against such loss, HDB3 substitutes a known bit pattern for every occurrence of a string of four consecutive logical zeros within the CEPT data stream.

Select **Yes** (enable HDB3) or **No** (disable HDB3) based on the ability of the connected device to implement High Density Bipolar coding.

- ❑ **Circuit 1 Name** identifies the first circuit carried by the E1 line.

  Like Ethernet and synchronous lines, each E1 line requires an associated and unique circuit name. Unlike Ethernet and synchronous lines, however, a single E1 line can carry a second circuit. If you establish a second circuit, it too requires a unique circuit name. Later, you will use these unique names to assign circuit-specific parameters and to configure application software modules.

  Circuit names consist of up to 12 characters. You can use any printable character *except for the period (.)* when assigning a circuit name. Because you use circuit names later in the configuration process, it is very important that you maintain an accurate record of line and circuit names. You may wish to use the *E1 Line Summary Chart* in Appendix C to maintain a record of line and circuit names.

  Enter the circuit name from the keyboard, then press `[RETURN]`.

- ❑ **Circuit 2 Name** identifies the second circuit carried by the E1 line.

  If you are enabling a second circuit, enter its name, otherwise press `[RETURN]`.

- ❑ **Slot 1-31 Configuration** assigns each E1 channel to a specific function.

  The string of 31 **I**s represents the default state of E1 channels 1 through 31 (channel 0 is reserved for signalling). Channel assignment options are as follows:

I	--	Idles the channel (default)
D	--	Assigns the channel to data pass through
V	--	Assigns the channel to voice pass through
1	--	Assigns the channel to Circuit 1
2	--	Assigns the channel to Circuit 2

  With the cursor positioned on the first **I** (E1 channel 1), press the `[RIGHTARROW]` to display the desired channel assignment, then press `[RETURN]`. The cursor moves one position to the right (channel 2).

  Continue in this fashion until you have assigned each of the 31 CEPT channels.

When you finish, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the Configuration Menu.

4.8 Adding E1 Lines

You establish additional E1 lines from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Lines Summary Screen.

Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Line Parameters Screen. Now follow the procedure described in Section 4.7 to establish an additional E1 line; repeat this procedure until you have established all E1 lines.

4.9 Establishing Token Ring Lines

The token ring line parameters are listed in Table 4-5.

Table 4-5: Token Ring Line Parameters

Parameter	Function
Slot Number	specifies a link module
Physical Access Method	specifies a line access protocol
Ring Interface	specifies a ring service type
Circuit Name	specifies a circuit name

You establish a token ring line from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured any lines, the screen displays the following:

No Lines record(s) found
Do you wish to add Lines record(s)?

Press `[RETURN]` to display the Line Parameters Screen.

However, if you have previously established lines, the screen displays the Lines Summary Screen. To move to the Line Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

- **Slot Number** identifies the backplane slot that houses the physical connector for the token ring line that you are establishing.

  Select the appropriate slot number.

- **Physical Access Method** specifies the line type.

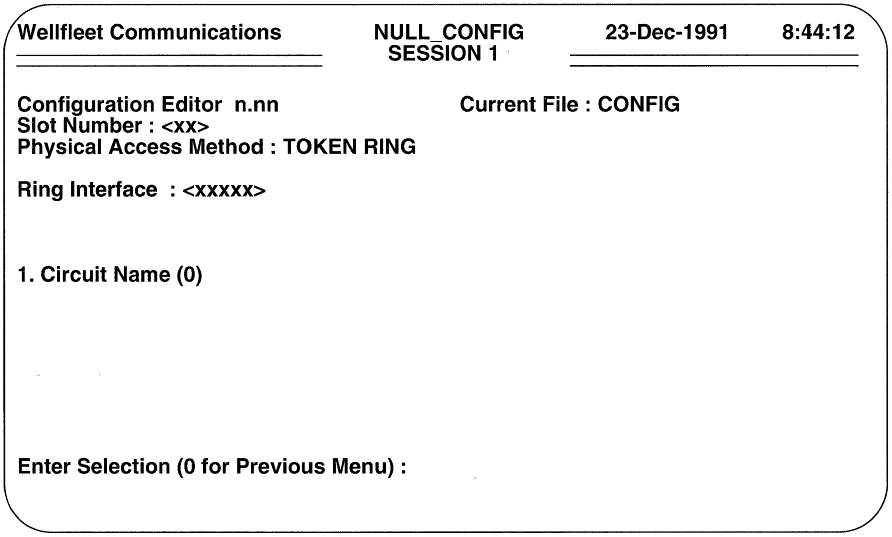
  To establish a token ring line, press the `[RIGHTARROW]` to display **TOKEN RING**, then press `[RETURN]`.

The screen prompts for **Ring Interface**.

- ❐ **Ring Interface** specifies the type of token ring service.

  Depending upon the token ring service offered by the attached network, select 4 Mbs service (**4 Mbps**), 16 Mbs service (**16 Mbps**), or 16 Mbs service with the Early Token Release option (**16 Mbps ETR**).

After you press `[RETURN]`, the screen displays the Token Ring Circuit Access Screen to prompt for a circuit name.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Slot Number : <xx>
Physical Access Method : TOKEN RING

Ring Interface  : <xxxxx>


1. Circuit Name (0)






Enter Selection (0 for Previous Menu) :
```

Figure 4-8 Token Ring Circuit Access Screen

You must assign a unique circuit name to each token ring line. Later, you will use this unique name to assign circuit- specific parameters and to configure application software modules.

Circuit names consist of up to 12 characters. You can use any printable character *except for the period (.)* when assigning a circuit name. Because you use circuit names later in the configuration process, it is very important that you maintain an accurate record of line and circuit names. You may wish to use the *Token Ring Line Summary Chart* in Appendix C to maintain a record of line and circuit names.

To assign a circuit name, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

> **No Circuit Name record(s) found**
> **Do you wish to add Circuit Name record(s)?**

Press [RETURN]. After the screen prompts for **Circuit Name**, enter a circuit name, then press [RETURN].

When the screen displays **Hit Return to Continue**, press [RETURN]. The screen again displays the Token Ring Circuit Access Screen. The screen echoes your responses to **Slot Number**, **Physical Access Method**, and **Ring Interface**. **Circuit Name (1)** verifies that you have assigned a circuit name to this token ring line.

Enter <0> at **Enter Selection (0 for Previous Menu)** to return to the Configuration Menu.

4.10 Adding Token Ring Lines

You establish additional token ring lines from the Configuration Menu. Enter <3> at **Enter Selection (0 for Previous Menu)**. The screen displays the Lines Summary Screen.

Press the [RIGHTARROW] to display **Add**, then press [RETURN] to display the Line Parameters Screen. Now follow the procedure described in Section 4.9 to establish an additional token ring line; repeat this procedure until you have established all token ring lines.

4.11 Establishing FDDI Lines

Depending on the type of FDDI link module (FDDI VME or FDDI MODULE) installed within the multiprotocol router, use the following sections to establish an FDDI line.

4.11.1 FDDI VME Lines

The FDDI VME line parameters are listed in Table 4-6.

You establish an FDDI VME line from the Configuration Menu. Enter <3> at **Enter Selection (0 for Previous Menu)**. If you have not previously configured any lines, the screen displays the following:

No Lines record(s) found
Do you wish to add Lines record(s)?

Press [RETURN] to accept the default. The screen displays the Line Parameters Screen.

However, if you have previously established lines, the screen displays the Lines Summary Screen. To move to the Line Parameters Screen, at **Action (-> for selections)**, press the [RIGHTARROW] to display **Add**, then press [RETURN].

Table 4-6: FDDI VME Line Parameters

Parameter	**Function**
Slot Number	specifies an ACE processor board
Physical Access Method	specifies a line access protocol
Board Number	specifies the FDDI controller address
Circuit Name	specifies a circuit name

❒ **Slot Number** identifies the backplane slot that houses the hosting ACE processor board for the FDDI VME line that you are establishing.

Select the appropriate slot number.

NOTE

Other line types (Ethernet, synchronous, T1, E1, token ring, and FDDI MODULE) are supported by a set of two PCBs: an advanced communications engine (ACE) and a link interface, collectively referred to as an intelligent link module (ILI). An FDDI VME line, in contrast, is supported by a set of three PCBs: an ACE (referred to as the hosting ACE), an FDDI controller, and a fiber optical interface board (FOIB). When configuring an FDDI VME line, ensure that you set the **Slot Number** parameter to the slot that contains the hosting ACE, not the slot that contains the FOIB.

❒ **Physical Access Method** specifies the line type.

To establish an FDDI VME line, press the `[RIGHTARROW]` to display **FDDI (VME)**, then press `[RETURN]`.

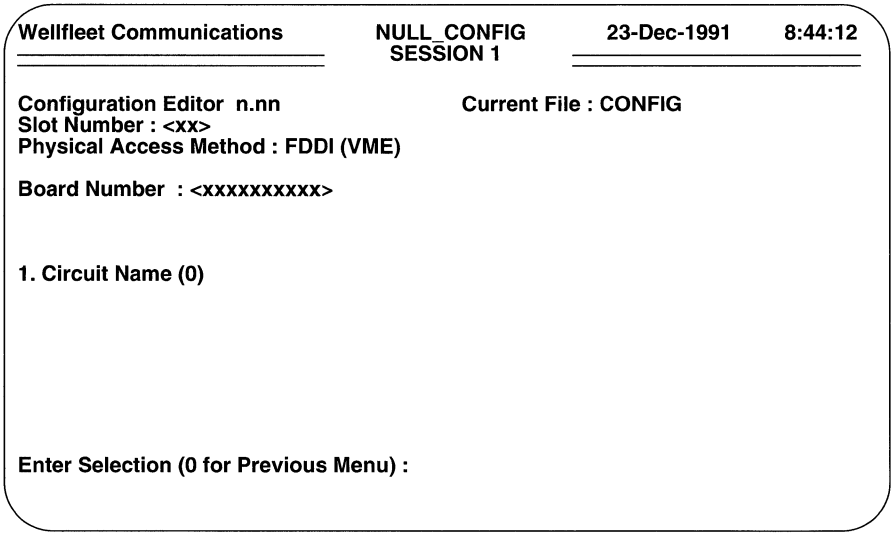
The screen prompts for **Board Number**.

❒ **Board Number** specifies the hardware (VMEbus) address of the FDDI controller.

If your router contains a single factory installed FDDI 3-board set, press `[RETURN]` to accept the default response, **1 (short addr 0000)**.

If your router contains more than one FDDI board set, or if you have manually changed the factory-set address jumpers, you must specify the actual FDDI hardware address. Refer to the *Installation Guide* for information on setting and determining FDDI hardware addresses. After determining the address, select from the available responses, **1 (short addr 0000)**, **3 (short addr 0400)**, and **2 (short addr 0200)**.

After you specify the board address, the screen displays the FDDI (VME) Circuit Access Screen to prompt for a circuit name.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Slot Number : <xx>
Physical Access Method : FDDI (VME)

Board Number  : <xxxxxxxxxx>


1. Circuit Name (0)






Enter Selection (0 for Previous Menu) :
```

Figure 4-9 FDDI (VME) Circuit Access Screen

You must assign a unique circuit name to each FDDI VME line. Later, you will use this unique name to assign circuit-specific parameters and to configure application software modules.

Circuit names consist of up to 12 characters. You can use any printable character *except for the period (.)* when assigning a circuit name. Because you use circuit names later in the configuration process, it is very important that you maintain an accurate record of line and circuit names. You may wish to use the *FDDI VME Line Summary Chart* in Appendix C to maintain a record of line and circuit names.

To assign a circuit name, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

> **No Circuit Name record(s) found**
> **Do you wish to add Circuit Name record(s)?**

Press `[RETURN]`. After the screen prompts for **Circuit Name**, enter a circuit name, then press `[RETURN]`.

When the screen displays **Hit Return to Continue**, press `[RETURN]`. The screen again displays the FDDI (VME) Circuit Access Screen.

The screen echoes your responses to **Slot Number, Physical Access Method**, and **Board Number**. **Circuit Name (1)** verifies that you have assigned a circuit name to this FDDI line.

Enter `<0>` at **Enter Selection (0 for Previous Menu)** to return to the Configuration Menu.

You establish additional FDDI VME lines from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Lines Summary Screen.

Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Line Parameters Screen. Now follow the previously described procedure to establish an additional FDDI VME line; repeat this procedure until you have established all FDDI VME lines.

4.11.2 FDDI MODULE Lines

The FDDI MODULE line parameters are listed in Table 4-7.

Table 4-7: FDDI MODULE Line Parameters

Parameter	Function
Slot Number	specifies a link module
Physical Access Method	specifies a line access protocol
Bridge Type	specifies bridge encapsulation or translation
Circuit Name	specifies a circuit name

You establish an FDDI MODULE line from the Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured any lines, the screen displays the following:

No Lines record(s) found
Do you wish to add Lines record(s)?

Press `[RETURN]` to display the Line Parameters Screen.

However, if you have previously established lines, the screen displays the Lines Summary Screen. To move to the Line Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

❒ **Slot Number** identifies the backplane slot that houses the physical connector for the FDDI MODULE line that you are establishing. Select the appropriate slot number.

- ❒ **Physical Access Method** specifies the line type.

  To establish an FDDI MODULE line, press the `[RIGHTARROW]` to display **FDDI (MODULE)**, then press `[RETURN]`.

The screen prompts for **Bridge Type**.

- ❒ **Bridge Type** selects between bridge encapsulation or translation.

  The translating bridge enables the interconnection of Ethernet and FDDI networks as shown in Figure 4-10.

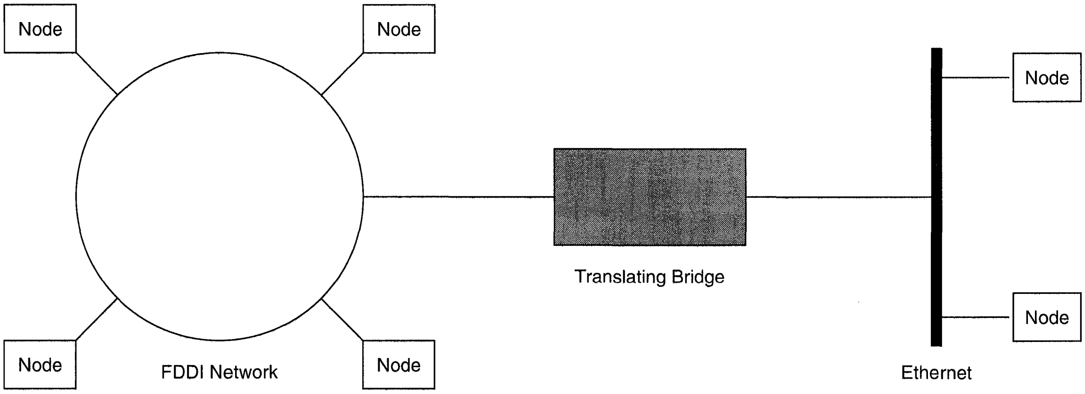


Figure 4-10 Translating Bridge

The encapsulating bridge implementation (shown in Figure 4-11) enables the interconnection of similar networks (for example, Ethernets) over a "backbone" FDDI network. Within such a topology a bridge "encapsulates" an original message into a new message type (in this case, an FDDI-specific packet) for travel across the backbone. At the destination, the message is removed from the FDDI packet and transmitted in its original form.

After you specify the bridge type (**Encapsulating** or **Translating**), the screen displays the FDDI (MODULE) Circuit Access Screen (Figure 4-12) to prompt for a circuit name.

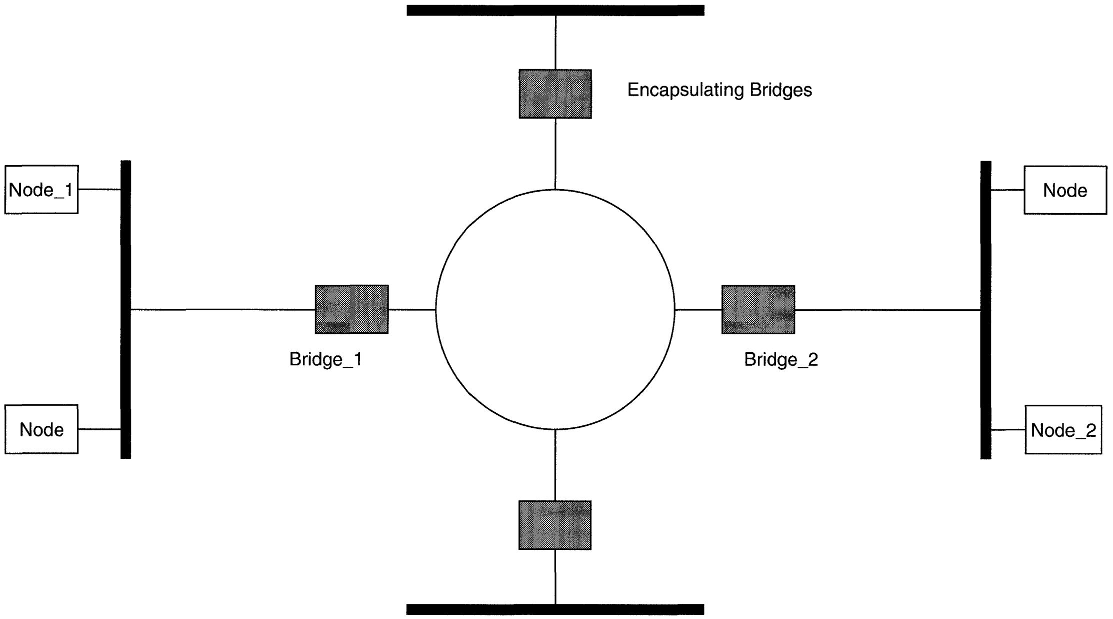


Figure 4-11 Encapsulating Bridges

Circuit names consist of up to 12 characters. You can use any printable character *except for the period (.)* when assigning a circuit name. Because you use circuit names later in the configuration process, it is very important that you maintain an accurate record of line and circuit names. You may wish to use the *FDDI MODULE Line Summary Chart* in Appendix C to maintain a record of line and circuit names.

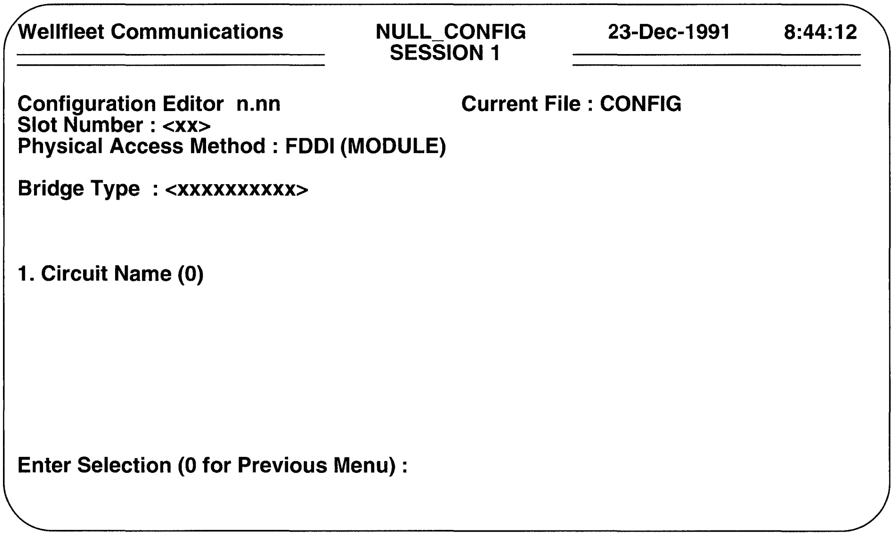
To assign a circuit name, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

> **No Circuit Name record(s) found**
> **Do you wish to add Circuit Name record(s)?**

Press `[RETURN]`. After the screen prompts for **Circuit Name**, enter a circuit name, then press `[RETURN]`.

When the screen displays **Hit Return to Continue**, press `[RETURN]`. The screen again displays the FDDI (MODULE) Circuit Access Screen.

The screen echoes your responses to **Slot Number**, **Physical Access Method**, and **Board Number**. **Circuit Name (1)** verifies that you have assigned a circuit name to this FDDI line.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Slot Number : <xx>
Physical Access Method : FDDI (MODULE)

Bridge Type  : <xxxxxxxxxx>


1. Circuit Name (0)






Enter Selection (0 for Previous Menu) :
```

Figure 4-12 FDDI (MODULE) Circuit Access Screen

Enter <0> at **Enter Selection (0 for Previous Menu)** to return to the Configuration Menu.

You establish additional FDDI MODULE lines from the Configuration Menu. Enter <3> at **Enter Selection (0 for Previous Menu)**. The screen displays the Lines Summary Screen.

Press the [RIGHTARROW] to display **Add**, then press [RETURN] to display the Line Parameters Screen. Now follow the previously described procedure establish an additional FDDI MODULE line; repeat this procedure until you have established all FDDI MODULE lines.

5 Setting Data-Link Layer Parameters

This chapter tells you how to configure circuits.

When you established lines, you defined the physical layer connections between the multiprotocol router and network devices. You now define the data-link layer connections in terms of *circuits*. Circuits take the bit stream or "bandwidth" provided by the physical layer and condition it to provide a reliable transmission medium.

There are seven types of circuits.

LAN Circuits

Provide a transmission channel between the router and a CSMA/CD (carrier sense multiple access with collision detection) medium.

Point-to-Point Circuits

Provide a transmission channel between the router and a single long-haul medium terminated by a peer router at the remote site. Point-to-point circuits use HDLC (high-level data-link control) protocol to exchange data and control packets.

Ring Circuits

Provide a transmission channel between the router and a token ring and/or FDDI medium.

Pt to Pt Protocol (PPP) Circuits

Provide a transmission channel over synchronous media (V.35, T1, or E1) between the router and a remote PPP peer device. The transmission channel supports the Point-to-Point Protocol service as defined in Internet Request for Comments (RFC) 1171, 1172, and 1220.

SMDS Circuits

Provide a transmission channel over V.35 (synchronous media) between the router and an SMDS (Switched Multi-megabit Data Service) data service unit (DSU) or switch.

Frame Relay Circuits

Provide a transmission channel between the router and a Frame Relay network.

LAPB Circuits

Provide a transmission channel between the router and a public or private packet-switched X.25 network.

The following sections provide a series of instructions that describe how to configure LAN, point-to-point, ring, Point-to-Point Protocol (PPP), SMDS, and Frame Relay circuits. Refer to Chapter 6, *Configuring X.25 Service*, for instructions on configuring LAPB circuits.

5.1 Configuring LAN (Ethernet) Circuits

The LAN circuit parameters are listed in Table 5-1.

Table 5-1: LAN Circuit Parameters

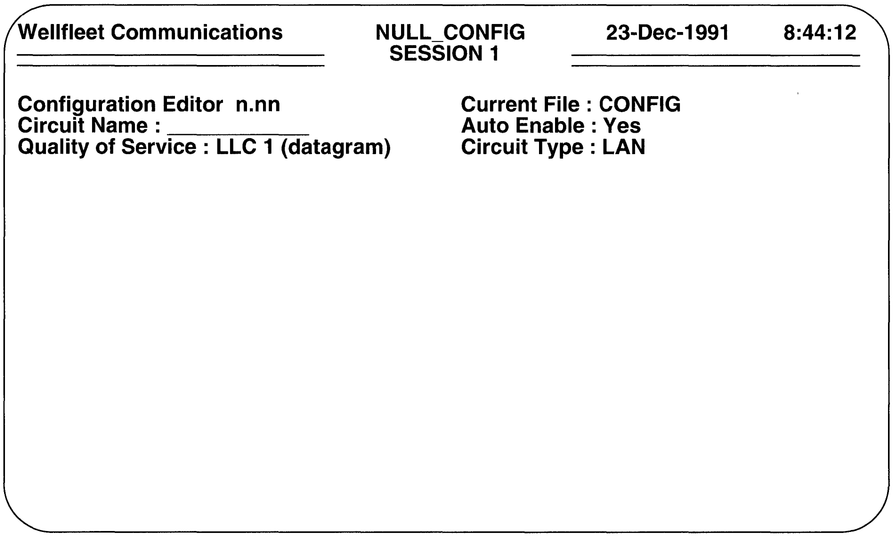
Parameter	Function
Circuit Name	specifies a LAN (Ethernet) circuit
Auto Enable	specifies the initialization state
Quality of Service	specifies datagram service
Circuit Type	specifies a LAN (Ethernet) circuit
LAN Address	specifies a MAC-level address
XCVR Polling	tests transceiver integrity

Before configuring a LAN circuit, refer to the *Ethernet Line Summary Chart.* Any circuit listed on these charts must be configured as a LAN circuit. You may also wish to use the *Ethernet Circuit Summary Chart* (also in Appendix C) to maintain a record of LAN circuit parameters.

You configure a LAN circuit from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Circuits record(s) found
Do you wish to add Circuits record(s)?

Press `[RETURN]` to display the Circuit Parameters Screen (Figure 5-1).



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Name : ___________                  Auto Enable : Yes
Quality of Service : LLC 1 (datagram)       Circuit Type : LAN
```

Figure 5-1 Circuit Parameters Screen

❒ **Circuit Name** identifies the LAN circuit.

Enter the circuit name (taken from the *Ethernet Line Summary Chart*).

❒ **Auto Enable** specifies the initial state of the LAN circuit.

This circuit-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the circuit when the router boots.

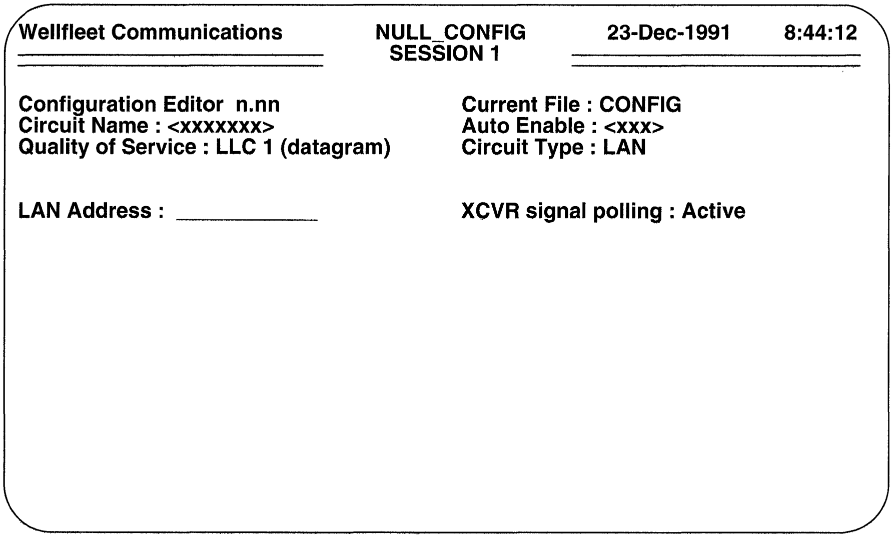
When global auto enable is **No**, the circuit is unconditionally disabled You will later need to enable the circuit with NCL commands after the router boots.

When global auto enable is **Yes**, the circuit is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable) or **No** (disable), then press `[RETURN]`. If you select **No**, you will later need to enable the circuit with NCL commands after the router boots.

❒ **Quality of Service** is **LLC1 (datagram)** for LAN circuits.

❒ **Circuit Type** is **LAN** for LAN circuits.

After you specify a LAN circuit, the screen displays the LAN Circuit Parameters Screen (Figure 5-2).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                       Current File : CONFIG
Circuit Name : <xxxxxxx>                         Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)            Circuit Type : LAN

LAN Address : ___________                        XCVR signal polling : Active
```

Figure 5-2 LAN Circuit Parameters Screen

- **LAN Address** specifies the 48-bit Ethernet address of the router.

  All routers are shipped with a unique universally administered address written in read-only memory (ROM). This address has a high-order (most significant 24-bits) value of 0000A2, hexadecimal, and a low-order (least significant 24-bits) value unique to the router. You can use this default address, by pressing `[RETURN]`.

NOTE

The router ignores the value of the **LAN Address** on circuits which support AppleTalk, DECnet, IPX, XNS, or the Bridge (*with the spanning tree algorithm enabled*). In such instances, the bridging/routing software asserts an internally-generated LAN address.

If the router uses only the IP Router, or if it uses the IP Router in conjunction with the Bridge (*with the spanning tree algorithm disabled*), you can assign an Ethernet address of your choosing. Because each LAN device within your network requires a unique 48-bit address, it is imperative that you guard against duplicated addresses. To assign a user-supplied LAN address, enter the address (in 12-character hexadecimal format) and then press `[RETURN]`.

NOTE

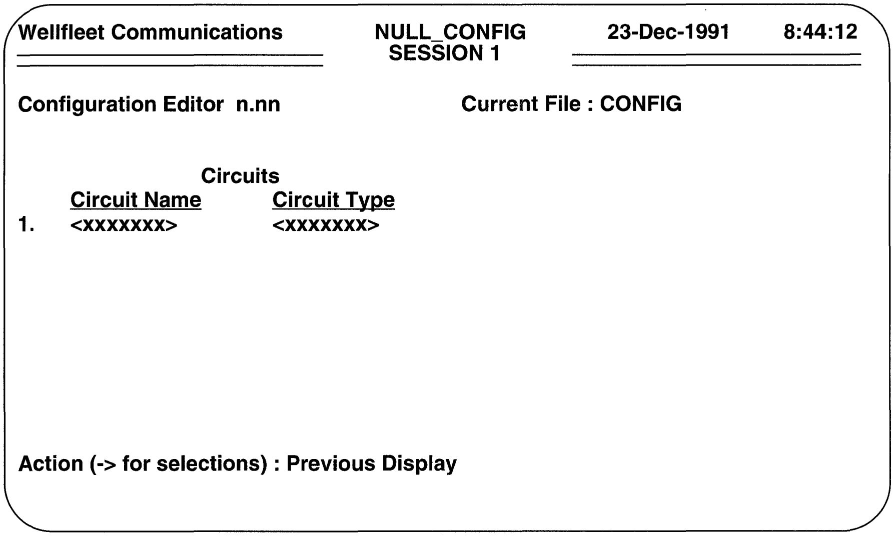
When assigning a user-supplied LAN address, ensure that the least significant bit of the most significant byte is clear (equal to zero). When LAN addresses are "sent across the wire" their bit order is reversed. Consequently, the least significant bit of the most significant byte is transmitted first. A logical one in the first bit position of a destination address designates a broadcast or multicast address.

- ❒ **XCVR signal polling** enables the transmission of periodic self- addressed messages. These messages (sent at 5-second intervals) verify proper transceiver operations. Transmission of these messages is called signal polling.

  XCVR signal polling *must* be set to **Active** (thus enabling message transmission). With transmission of such messages enabled, the circuit generates an event message with a severity level of *Warning* in response to transceiver failure. Press `[RETURN]` to accept the default response, **Active**.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Configuration Menu.

You configure additional LAN circuits from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. Because you have already configured a LAN circuit, the screen displays the Circuits Summary Screen (Figure 5-3). This screen lists each previously configured circuit along with its circuit type. Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Circuit Parameters Screen. Now follow the previously described procedure to configure an additional LAN circuit. Repeat this procedure until you have configured all LAN circuits.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991    8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG


                      Circuits
        Circuit Name         Circuit Type
1.      <xxxxxxx>            <xxxxxxx>








Action (-> for selections) : Previous Display
```

Figure 5-3 Circuits Summary Screen

5.2 Configuring Point-to-Point Circuits

The point-to-point circuit parameters are listed in Table 5-2.

Table 5-2: Point-to-Point Circuit Parameters

Parameter	Function
Circuit Name	identifies the point-to-point circuit
Auto Enable	specifies the initialization state
Quality of Service	assigns LLC1 or LLC2 service
Circuit Type	specifies a point-to-point circuit
Point to Point Address	specifies a physical address
Minimum Frame Spacing	specifies frame spacing
Remote Signal and Sense	verifies end-to-end integrity
Data Link Layer Protocol	enables transparent pass-through service

Before configuring a point-to-point circuit, refer to the *Synchronous Line Summary Chart*, the *T1 Line Summary Chart* , and the *E1 Line Summary Chart* n Appendix C. Any listed circuit *not* providing PPP Protocol, SMDS, Frame Relay, or X.25 service must be configured as a point-to-point circuit.

You may wish to use the *Point-to-Point Circuit (LLC1 Service) Summary Chart* and *Point-to-Point Circuit (LLC2 Service) Summary Chart* to maintain records of point-to-point circuit parameters.

You configure a point-to-point circuit from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured circuits, the screen displays the following:

No Circuits record(s) found
Do you wish to add Circuits record(s)?

Press `[RETURN]` to display the Circuit Parameters Screen.

However, if you have previously configured circuits, the screen displays the Circuits Summary Screen. To move to the Circuit Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

❒ **Circuit Name** identifies the point-to-point circuit.

Enter the circuit name (taken from the *Synchronous Line Summary Chart*, the *T1 Line Summary Chart*, or the *E1 Line Summary Chart.*

❒ **Auto Enable** specifies the initial state of the point-to-point circuit.

This circuit-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the point-to-point circuit when the router boots.

When global auto enable is **No**, the point-to-point circuit is unconditionally disabled You will later need to enable the circuit with NCL commands after the router boots.

When global auto enable is **Yes**, the circuit is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable) or **No** (disable), then press `[RETURN]`. If you select **No**, you will later need to enable the circuit with NCL commands after the router boots.

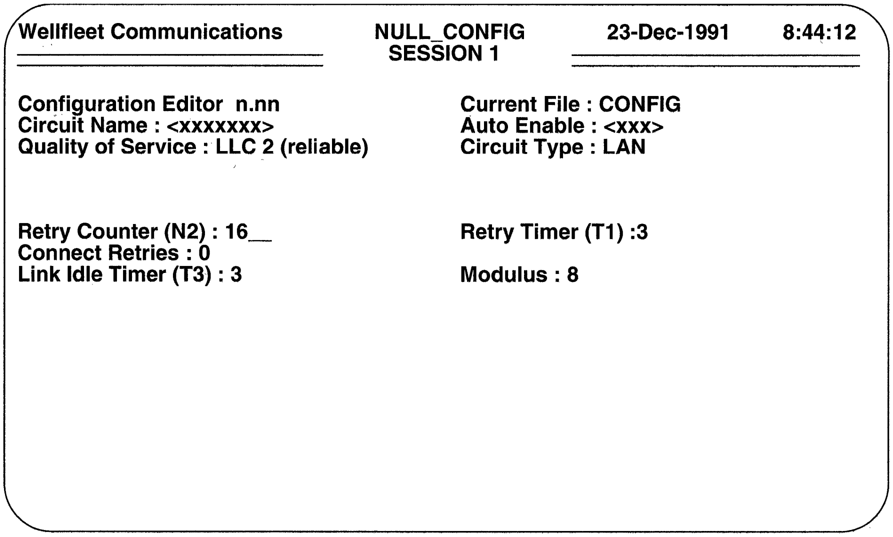
❒ **Quality of Service** specifies the link-level control protocol.

Select either **LLC 1 (datagram)** or **LLC 2 (reliable)**.

LLC 1 (datagram), specifies connectionless datagram service. **LLC 2 (reliable)** specifies connection-oriented service which provides error detection and error recovery by retransmission.

To select datagram service, press `[RETURN]` to accept the default, **LLC 1 (datagram)**. The cursor moves to the **Circuit Type** field.

To select reliable service, press the `[RIGHTARROW]` to display **LLC 2 (reliable)**, then press `[RETURN]`. The screen displays the LLC2 Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Circuit Name : <xxxxxxx>                     Auto Enable : <xxx>
Quality of Service : LLC 2 (reliable)        Circuit Type : LAN


Retry Counter (N2) : 16__                    Retry Timer (T1) :3
Connect Retries : 0
Link Idle Timer (T3) : 3                     Modulus : 8
```

Figure 5-4 LLC2 Parameters Screen

The LLC2 parameters are listed in Table 5-3.

- **Retry Counter (N2)** specifies the number of possible retransmissions of the same frame after expiration of the Retry (T1) Timer.

  To accept the default value of 16, press `[RETURN]`; to assign a different value, enter the value from the keyboard.

- **Retry Timer (T1)** specifies the allowable interval between the issuance of a command and the reception of an acknowledgment. In the absence of an acknowledgment, the router retransmits the command upon expiration of the T1 timer.

  To accept the default value of 3 (seconds), press `[RETURN]`; to assign a different value, enter the value from the keyboard.

Table 5-3: LLC2 Parameters

Parameter	Function
Retry Counter (N2)	specifies frame retransmissions
Retry Timer (T1)	specifies the send/acknowledge interval
Connect Retries	specifies connection attempts
Link Idle Timer (T3)	specifies circuit idle time
Modulus	specifies the size of the HDLC control field
Window Size	specifies unacknowledged packets

- ❐ **Connect Retries** operates with the Retry Counter and Retry Timer to govern the number of retransmission attempts in the event of an unacknowledged packet. After expiration of the Retry Timer, LLC2 transmits up to N2 control messages in an attempt to acquire a response from the remote end of the circuit. If an acknowledgment is still outstanding, LLC2 iterates the loop the number of times designated by **Connect Retries**.

  A value of 0 (the default) specifies infinite retries. To accept the default value, press **[RETURN]**; to assign a different value, enter the value from the keyboard.

- ❐ **Link Idle Timer (T3)** specifies the idle time (in seconds) after which the point-to-point circuit is disconnected.

  To accept the default value of 3 seconds, press **[RETURN]**; to assign a different value, enter the value from the keyboard.

- ❐ **Modulus** specifies the length, in bits, of the HDLC packet control field (Figure 5-5).

  8 specifies an 8-bit control field; 128 specifies a 16-bit control field.

  The size of the control field determines the number of unacknowledged packets that may be pending at any one time. An 8-bit field provides three bits for message sequencing, and thus allows a maximum of seven outstanding packets. A 16-bit field provides seven bits for sequencing, and thus allows a maximum of 127 unacknowledged packets.

Flag	**.....**	**Flag**	**Address**	**Control**	**I**	**FCS**	**Flag**

KEY:

Flag Frame	**8-bit sequence (01111110)**
Address Frame	**8/16 bits in length**
Control Frame	**16 bits if Modulus is 128, else 8 bits**
I (Information) Frame	**Contains n bytes of data**
FCS Frame	**32-bit frame check sequence**
Flag Frame	**8-bit sequence (01111110)**

Figure 5-5 HDLC Frame Format

- **Window Size** enables you to specify an exact number of packets that may be unacknowledged at any one time. **Modulus** has previously enabled a maximum number of unacknowledged packets.

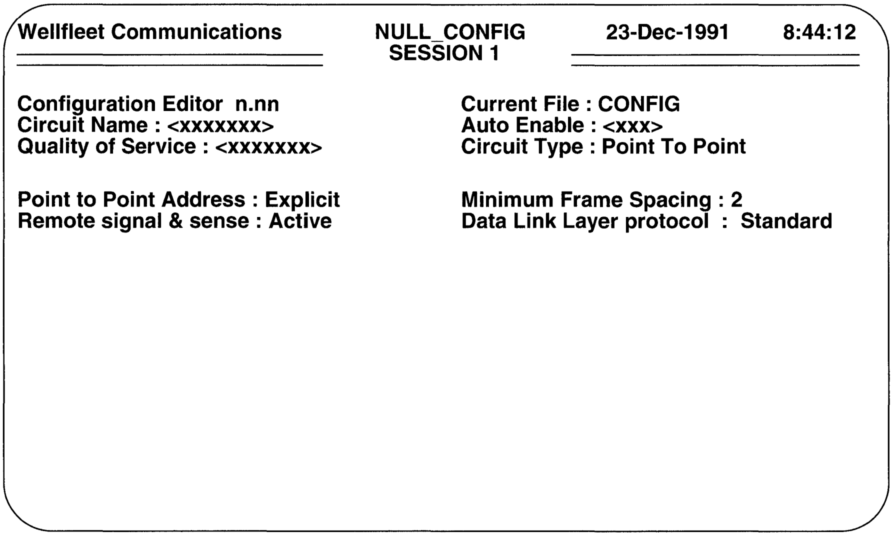
  Select from the available responses: 7 (the default), 1, and 3 -- if you have previously set **Modulus** to 8; or 7 (the default), 15, 31, 63, and 127 --if you have previously set **Modulus** to 128.

- **Circuit Type** is **Point to Point** for point-to-point circuits.

After you specify a point-to-point circuit, the screen displays the Point-to-Point Circuit Parameters Screen (Figure 5-6).

- **Point to Point Address** prompts for a 1-byte value, which is used in the address field of the HDLC packet. Conventionally, one end of a point-to-point circuit is designated DCE and is assigned an address of 01; the other end of the circuit is designated DTE and is assigned an address of 03.

  There are three available responses: **Explicit**, **DCE**, and **DTE**. To enable conventional addressing, designate one end of the point-to-point circuit as **DCE** and designate the other end as **DTE**.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Circuit Name : <xxxxxxx>                       Auto Enable : <xxx>
Quality of Service : <xxxxxxx>                 Circuit Type : Point To Point

Point to Point Address : Explicit              Minimum Frame Spacing : 2
Remote signal & sense : Active                 Data Link Layer protocol  :  Standard
```

Figure 5-6 Point-to-Point Circuit Parameters Screen

Conventional addressing, however, is inadequate in the case of multiple communication channels enabled by a common satellite link (refer to Figure 5-7). As shown, a common satellite relay-link provides a virtual point-to-point link between routers A and X, B and Y, and C and Z.

The worst case scenario consists of routers A, B, and C being designated as DCE (address = 01), and routers X, Y, and Z being designated DTE (address = 03). If A (for example) transmits a frame across the virtual point-to-point circuit to X, the satellite broadcast is monitored not only by X (the intended recipient) but also by Y and Z. Because X, Y, and Z all perceive a properly addressed frame, all three accept delivery and attempt to process frame contents with unpredictable results.

Explicit addressing avoids such confusion by enabling the assignment of unique addresses to each end of a point-to-point circuit. To select explicit addressing, press `[RETURN]` to accept the default value, **Explicit.** The console screen prompts for a local and remote address pair (Figure 5-8).

At **Local Address**, enter a unique decimal value from 00 through 99 (avoid the conventional address values of 01 or 03), then press `[RETURN]`. The cursor moves to **Remote Address.** Enter another unique decimal value from 00 to 99, then press `[RETURN]`. Make certain to reverse local and remote address values when you configure the device at the other end of the point-to-point circuit.

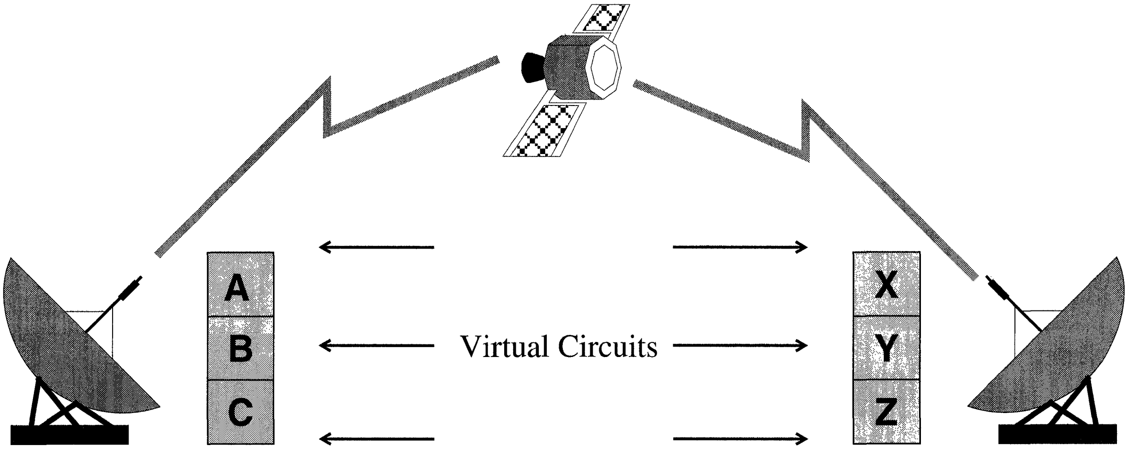
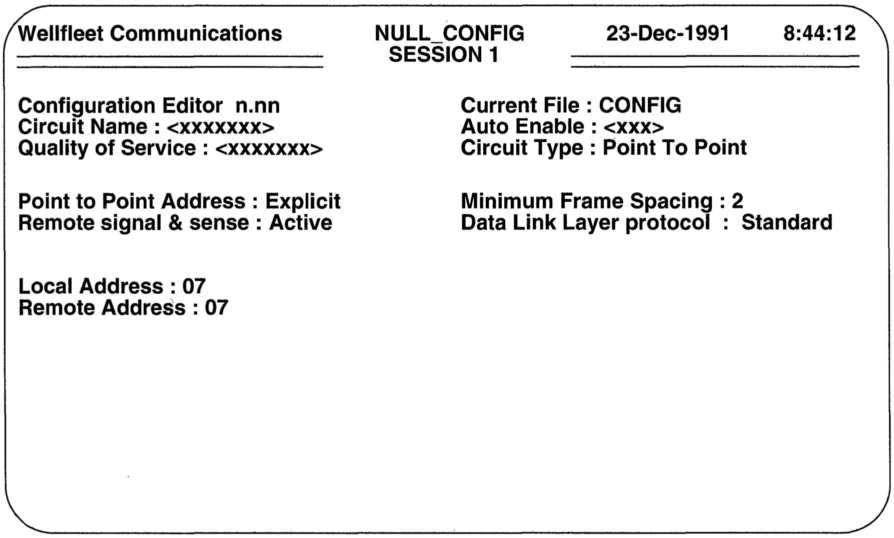


Figure 5-7 Satellite Broadcast (Sample Topology)



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991    8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Name : <xxxxxxxx>                   Auto Enable : <xxx>
Quality of Service : <xxxxxxxx>             Circuit Type : Point To Point

Point to Point Address : Explicit           Minimum Frame Spacing : 2
Remote signal & sense : Active              Data Link Layer protocol  :  Standard

Local Address : 07
Remote Address : 07
```

Figure 5-8 Explicit Addressing Parameters Screen

- ❒ **Minimum Frame Spacing** specifies the minimum number of flag sequences prefixed to an HDLC packet transmitted by the router.

  Note in Figure 5-5 that an HDLC packet is prefixed by a variable number of 8-bit flag sequences, and is terminated by a single instance of the same flag. Therefore, the number of flags transmitted between sequential packets is the sum of the constant 1 (the trailing flag) and the variable number of leading flags.

  After determining the minimum number of flags to transmit between each packet, reduce this number by one (to account for the terminating flag), press the `[RIGHTARROW]` to display this or the closest available value, then press `[RETURN]`.

- ❒ **Remote signal & sense** *must* be set to **Active**. This setting enables a proprietary protocol that detects any failure in end- to-end connectivity.

- ❒ **Data Link Layer protocol** enables/disables a proprietary protocol that provides a transparent point-to-point *pass-through* service for any synchronous traffic (such as IBM's SNA) across the multiprotocol router.

NOTE

The *pass-through* protocol uses the Bridge as its transport mechanism; you must configure the Bridge on slots which have *pass-through* service enabled.

With the proprietary *pass-through* protocol enabled, traffic across the circuit is restricted to explicitly configured addresses which terminate the point to point link; all other Bridge traffic is filtered from the *pass-through* interface.

If you do not want to enable the proprietary protocol, press `[RETURN]` to accept the default response, **Standard**.

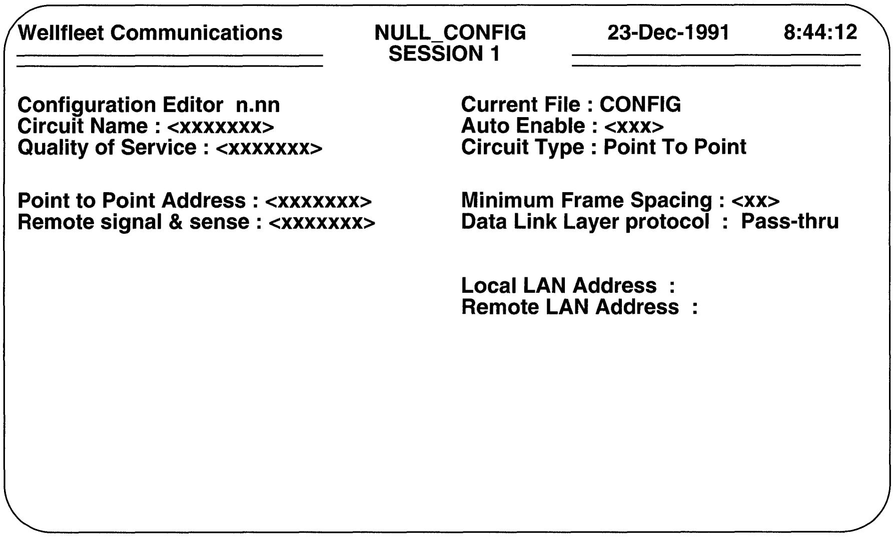
If you do want to enable the proprietary protocol, press the `[RIGHTARROW]` to display **Pass-Thru** and then press `[RETURN]`. The screen then prompts for LAN addresses (Figure 5-9).

- ❒ **Local LAN Address** is the 48-bit Ethernet address of the local end of the point to point link.

- ❒ **Remote LAN Address** is the 48-bit Ethernet address of the remote end of the point to point link.

NOTE

With the *pass-through* protocol enabled, the router ignores the **Quality of Service** and **Point to Point Address** parameters; in addition, it disables **Remote signal & sense**. Consequently, the *pass-through* interface provides no end-to-end flow control or activity detection.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Circuit Name : <xxxxxxx>                   Auto Enable : <xxx>
Quality of Service : <xxxxxxx>             Circuit Type : Point To Point

Point to Point Address : <xxxxxxx>         Minimum Frame Spacing : <xx>
Remote signal & sense : <xxxxxxx>          Data Link Layer protocol  :  Pass-thru

                                           Local LAN Address  :
                                           Remote LAN Address  :
```

Figure 5-9 Pass-Through Protocol Parameters Screen

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Configuration Menu.

You configure additional point-to-point circuits from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Circuits Summary Screen. Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Circuit Parameters Screen. Now follow the previously described procedure to configure an additional point-to-point circuit; repeat this procedure until you have configured all point-to-point circuits.

5.3 Configuring Ring Circuits

Token ring and FDDI circuits are referred to a s ring circuits. Ring circuit parameters are listed in Table 5-4.

Table 5-4: Ring Circuit Parameters

Parameter	Function
Circuit Name	identifies the ring circuit
Auto Enable	specifies the initialization state
Quality of Service	assigns LLC1 service
Circuit Type	specifies a ring circuit
LAN Address	specifies a MAC-level address
XCVR Polling	tests hardware integrity

Before configuring a ring circuit, refer to the *Token Ring Line Summary Chart*, the *FDDI VME Line Summary Chart*, and the *FDDI MODULE Line Summary Chart* in Appendix C. Any circuit listed on these charts must be configured as a ring circuit. You may also wish to use the *Ring Circuit Summary Chart* (also in Appendix C) to maintain a record of ring circuit parameters.

You configure a ring circuit from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured circuits, the screen displays the following:

No Circuits record(s) found
Do you wish to add Circuits record(s)?

Press `[RETURN]` to display the Circuit Parameters Screen.

However, if you have previously configured circuits, the screen displays the Circuits Summary Screen. To move to the Circuit Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

- ❐ **Circuit Name** identifies the ring circuit.

  Enter the circuit name (taken from the *Token Ring Line Summary Chart*, the *FDDI VME Line Summary Chart*, or the *FDDI MODULE Line Summary Chart*).

- ❐ **Auto Enable** specifies the initial state of the ring circuit.

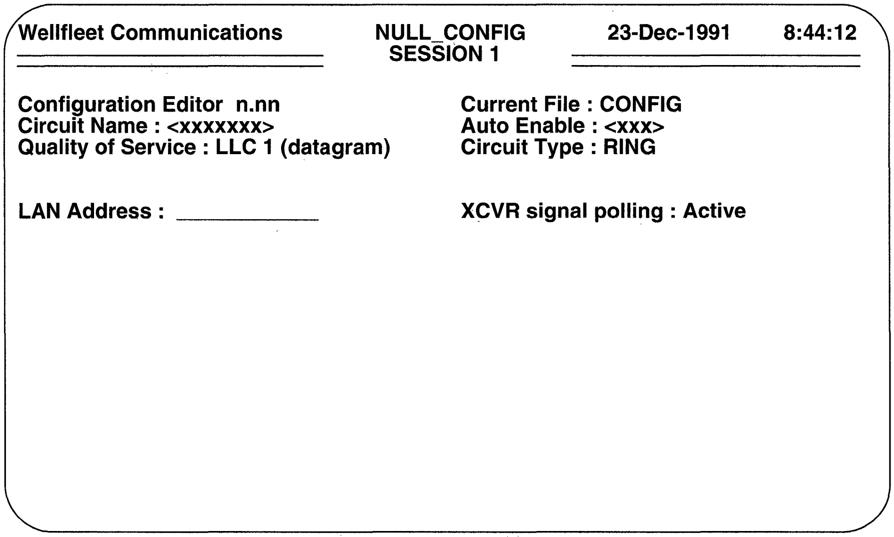
  This circuit-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the ring circuit when the router boots.

When global auto enable is **No**, the ring circuit is unconditionally disabled You will later need to enable the circuit with NCL commands after the router boots.

When global auto enable is **Yes**, the circuit is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable) or **No** (disable), then press `[RETURN]`. If you select **No**, you will later need to enable the circuit with NCL commands after the router boots.

- ❒ **Quality of Service** is **LLC1** for ring circuits.
- ❒ **Circuit Type** is **RING** for ring circuits.

After you specify a ring circuit, the screen displays the Ring Circuit Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991    8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Name : <xxxxxxx>                    Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)       Circuit Type : RING

LAN Address : ___________                   XCVR signal polling : Active
```

Figure 5-10 Ring Circuit Parameters Screen

- ❒ **LAN Address** specifies the 48-bit address of the router.

  All routers are shipped with a unique universally administered address written in read-only memory (ROM). This address has a high-order (most significant 24-bits) value of 0000A2, hexadecimal, and a low-order (least significant 24-bits) value unique to the router. You can use this default address, by pressing `[RETURN]`.

NOTE

The router ignores the value of the **LAN Address** on circuits which support AppleTalk, DECnet, IPX, XNS, or the Bridge (*with the spanning tree algorithm enabled*). In such instances, the bridging/routing software asserts an internally-generated LAN address.

If the router uses only the IP Router, or if it uses the IP Router in conjunction with the Bridge (*with the spanning tree algorithm disabled*), you can assign a MAC-level address of your choosing. Because each ring device within your network requires a unique address, it is imperative that you guard against duplicated addresses. To assign a user-supplied address, enter the address (in 12-character hexadecimal format) at **LAN Address** and then press `[RETURN]`.

NOTE

When assigning a user-supplied address, ensure that the least significant bit of the most significant byte is clear (equal to zero). When LAN addresses are "sent across the wire" their bit order is reversed. Consequently, the least significant bit of the most significant byte is transmitted first. A logical one in the first bit position of a destination address designates a broadcast or multicast address.

❒ **XCVR signal polling** enables the transmission of periodic self- addressed messages. These messages (sent at 5-second intervals) verify hardware integrity operations. Transmission of these messages is called signal polling.

XCVR signal polling must be set to **Active** (thus enabling message transmission). With transmission of such messages enabled, the circuit generates an event message with a severity level of *Warning* in response to polling failure. Press `[RETURN]` to accept the default response, **Active**.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Configuration Menu.

You configure additional ring circuits from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. Because you have already configured a ring circuit, the screen displays the Circuits Summary Screen. This screen lists each previously configured circuit along with its circuit type. Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Circuit Parameters Screen. Now follow the previously described procedure configure an additional ring circuit. Repeat this procedure until you have configured all ring circuits.

5.4 Configuring PPP Circuits

Point to Point Protocol (PPP), as defined in the Internet Request for Comments (RFC) 1171, 1172 and 1220 provides a method for routing or bridging datagrams over serial point-to-point links.

NOTE

The router's PPP implementation supports the establishment of PPP connections over synchronous media to include V.35, T1, and E1 lines.

PPP provides three major functions: datagram encapsulation, the establishment of a data-link layer connection between local and remote PPP peers, and the establishment of protocol-specific network layer connections between local and remote PPP peers.

PPP encapsulates datagrams as shown in Figure 5-11 within an HDLC-like frame that conveys addressing, control, and protocol identification information. Each frame is prefixed by a variable number of flags (hexadecimal 7E) and terminated by a single instance of the same flag.

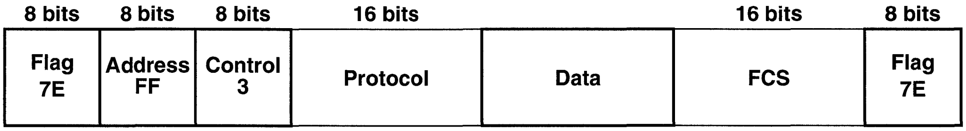


Figure 5-11 PPP Encapsulation

Data-link layer connection is provided by the Link Control Protocol (LCP) that establishes, configures, manages, and terminates the connection. LCP services are supported through the exchange of three packet types: Link Establishment packets which facilitate link establishment and the negotiation of initial configuration options; Link Termination packets which close a PPP connection, and; Link Maintenance packets which manage and debug the PPP link. LCP also provides optional link quality determination services which allow remote PPP peers to monitor and evaluate link quality.

Network layer connection is provided by a suite of Network Control Protocols (NCP). NCP protocols facilitate the multiplexing of network layer protocols (for example, IP or IPX) over a single point-to-point link. Table 5-4 lists Protocol field values used by the router. Values in the Cxxx range identify the LCP or associated protocols; values in the 8xxx range identify NCP protocols; while values in the 0xxx range identify the network protocol of specific datagrams.

Table 5-5: PPP Protocol Field Values

Protocol Field Value	Protocol	Protocol Field Value	Protocol
C021	LCP	8031	Bridged/Encapsulated Control Protocol
C023	UPAP	0021	IP
8021	IP Control Protocol	0025	XNS
8025	XNS Control Protocol	0027	DECnet Phase IV
8027	DECnet Phase IV Control Protocol	0029	AppleTalk
8029	AppleTalk Control Protocol	002B	IPX
802B	IPX Control Protocol	0031	Bridge/Encapsulated traffic

The PPP circuit parameters are listed in Table 5-6.

NOTE

While the PPP implementation provides support for all protocol suites (AppleTalk, Bridge, DECnet Phase IV, IPX, TCP/IP, and XNS) over PPP circuits, AppleTalk over PPP requires a Wellfleet router at both ends of the circuit. Wellfleet routers do not support the AppleTalk Control Protocol and, consequently, use a proprietary PPP code to pass AppleTalk traffic.

Before configuring a circuit, refer to the *Synchronous Line Summary Chart*, the *T1 Line Summary Chart*, and the *E1 Line Summary Chart*. Any circuit listed on these charts as providing Point-to-Point Protocol service must be configured as a PPP circuit. You may also wish to use the *PPP Circuit Summary Chart* (also in Appendix C) to maintain a record of PPP circuit parameters.

Table 5-6: PPP Circuit Parameters

Parameter	Function
Circuit Name	identifies the PPP circuit
Auto Enable	specifies the initialization state
Quality of Service	assigns LLC1 service level
Circuit Type	specifies a PPP circuit
LQM Time (secs)	specifies the link quality monitoring report period
Desired Link Quality	specifies acceptable line quality
Min Frame Spacing	specifies frame spacing
Extended (32-bit) CRC	selects an error-detection method
Max Pkt Size	specifies the maximum size of the PPP frame
IP Address	assigns an IP address to the PPP circuit
LCP Active Open	specifies the connection establishment method
LCP Auto Restart	specifies response to data-link layer failure
Use UPAP	enables the User Password Authentication Protocol

You configure a PPP circuit from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured circuits, the screen displays the following:

```
No Circuits record(s) found
Do you wish to add Circuits record(s)?
```

Press `[RETURN]` to display the Circuit Parameters Screen.

If you have previously configured circuits, the screen displays the Circuits Summary Screen. To move to the Circuit Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

❒ **Circuit Name** identifies the PPP circuit.

Enter the circuit name (taken from the *Synchronous Line Summary Chart*, the *T1 Line Summary Chart*, or the *E1 Line Summary Chart*.

❒ **Auto Enable** specifies the initial state of the PPP circuit.

This circuit-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the PPP circuit when the multiprotocol router boots.

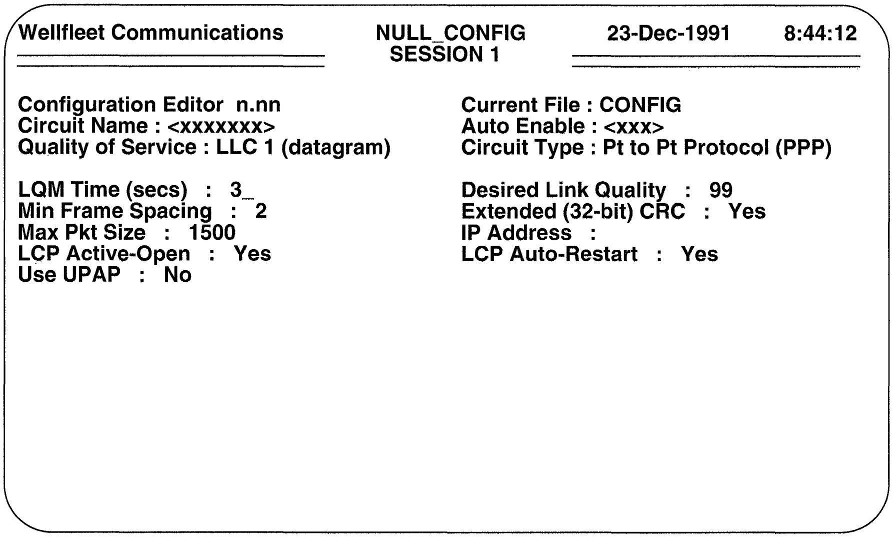
When global auto enable is **No**, the PPP circuit is unconditionally disabled. You will later need to enable the circuit with NCL commands after the router boots.

When global auto enable is **Yes**, the circuit is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable) or **No** (disable), then press `[RETURN]`. If you select **No**, you will later need to enable the circuit with NCL commands after the router boots.

❐ **Quality of Service** is **LLC1** for PPP circuits.

❐ **Circuit Type** is **Pt to Pt Protocol (PPP)** for PPP circuits.

After you specify a PPP circuit, the screen displays the PPP Circuit Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Circuit Name : <xxxxxxx>                       Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)          Circuit Type : Pt to Pt Protocol (PPP)

LQM Time (secs)  :  3_                         Desired Link Quality  :  99
Min Frame Spacing  :  2                        Extended (32-bit) CRC  :  Yes
Max Pkt Size  :  1500                          IP Address  :
LCP Active-Open  :  Yes                        LCP Auto-Restart  :  Yes
Use UPAP  :  No
```

Figure 5-12 PPP Circuit Parameters Screen

❐ **LQM Time (secs)** specifies the link-quality-monitoring report period.

Link-quality-monitoring (a PPP initial configuration option described in RFC 1172) refers to the process by which PPP determines the frequency and magnitude of data loss across the circuit. With link-quality-monitoring enabled, both ends of a PPP circuit can exchange Link-Quality-Report packets. Such packets serve two functions. Firstly, they provide a "keep-alive" indication to assure the local end that the remote PPP peer is operational. Secondly, Link-Quality-Report packets contain a series of counters providing dynamic information on the number of octets and data-link frames received and transmitted.

If you do not wish to enable link-quality-monitoring or if the remote PPP peer does not issue Link-Quality-Report packets, enter `0` and then press **[RETURN]**.

If you do wish to enable link-quality-monitoring, **LQM Time (secs)** specifies the maximum interval (in seconds) between Link-Quality-Report packets generated by the remote end of the PPP circuit. Failure to receive a Link-Quality-Report packet within the expected interval may indicate failure in the PPP link.

NOTE

The remote PPP peer is free to generate Link-Quality-Report packets more rapidly than specified by the **LQM Time (secs)** parameter. However, it must generate packets at least as frequently as specified by **LQM Time (secs)**.

In order to avoid declaring link failure in the light of a (possibly) single lost Link-Quality-Report packet, the multiprotocol router waits until five link-quality-report periods have elapsed without the receipt of a Link-Quality-Report packet before declaring the link down. For example, if **LQM Time (secs)** is set to a value of 3, the multiprotocol router declares the link down after a 15 second interval between the receipt of Link-Quality-Report packets.

Upon declaring the link down, PPP closes all active network layer (NCP) and data-link layer (LCP) connections. If the **LCP Auto-Restart** parameter is set to **Yes**, it then attempts to re-establish the LCP connection. If the **LCP Auto-Restart** parameter is set to **No**, PPP makes no attempt to re-establish the LCP connection (thus leaving it up to the remote PPP peer to restart LCP).

Enter the link-quality-monitoring period in seconds and then press **[RETURN]**.

❒ **Desired Link Quality** provides a metric to measure circuit reliability.

The Link-Quality-Report packets exchanged by PPP peers contain counts of received and transmitted octets and packets thus allowing both PPP implementations to monitor data loss across the link. **Desired Link Quality** specifies an "acceptable" percentage of data loss. The percentage is determined by dividing the constant 1 by the value of **Desired Link Quality**.

For example, the default value, **99**, specifies an acceptable loss of approximately 1% (1/99=.0101). Table 5-7 lists a range of **Desired Link Quality** parameter values along with the resulting data loss percentages.

Table 5-7: PPP Link Quality Values

Desired Link Quality Value	"Acceptable" Loss Percentage
1	100
2	50
4	25
5	20
10	10
20	5
50	2
100	1
200	0.5
250	0.4
300	0.3
500	0.2
999	0.1
0	0

If no link-quality-monitoring is needed or desired, set **Desired Link Quality** to **1**, indicating that for every octet or packet transmitted an octet or packet may be lost.

If the loss of any octets or packets is unacceptable, set **Desired Link Quality** to **0**, indicating that the multiprotocol router should declare the link "unreliable" whenever a single octet or packet is lost.

Upon declaring the link unreliable, the multiprotocol router closes all active network layer (NCP) connections, but continues to exchange Link-Quality-Report packets with the remote PPP peer. When the packet exchange indicates acceptable line reliability, the multiprotocol router re-establishes NCP connections.

Enter the link quality metric and then press `[RETURN]`.

❒ **Min Frame Spacing** specifies the minimum number of flag sequences prefixed to the HDLC-like packet transmitted by PPP.

A PPP packet is prefixed by a variable number of 8-bit flag sequences, and is terminated by a single instance of the same flag. The number of flags transmitted between sequential packets is the sum of the constant 1 (the trailing flag) and the variable number of leading flags.

After determining the minimum number of flags to transmit between each packet, reduce this number by one (to account for the terminating flag), press the `[RIGHTARROW]` to display this or the closest available value, then press `[RETURN]`.

❒ **Extended (32-bit) CRC** specifies an error detection scheme.

PPP implementations may use either a 16-bit (standard) or 32-bit (extended) frame check sequence (FCS) to detect errors in the PPP-encapsulated packet.

Select **Yes** to use the extended 32-bit FCS, or **No** to use the standard 16-bit FCS.

❒ **Max Pkt Size** specifies the maximum size of the PPP frame transmitted by the router.

The PPP frame consists of one octet of address information, one octet of control information, two octets of protocol information, a variable number of information octets, and (depending on the setting of the **Extended (32-bit) CRC** parameter) two or four octets of FCS information. While RFC 1172 specifies that all PPP implementations must be able to receive frames 1500 octets in length, it allows for the transmission of smaller frames.

If so desired, you can adjust this parameter downward to transmit smaller packets.

❒ **IP Address** specifies the 32-bit internet address of the PPP circuit.

Enter the IP address in dotted decimal notation.

❒ **LCP Active-Open** specifies whether PPP actively initiates the establishment of the LCP connection.

Yes indicates that PPP attempts to establish the LCP connection as soon as the physical link is ready. **No** indicates that PPP waits for the remote peer to establish the LCP connection.

NOTE

At least one of the PPP peers must be configured to “actively” open the LCP connection.

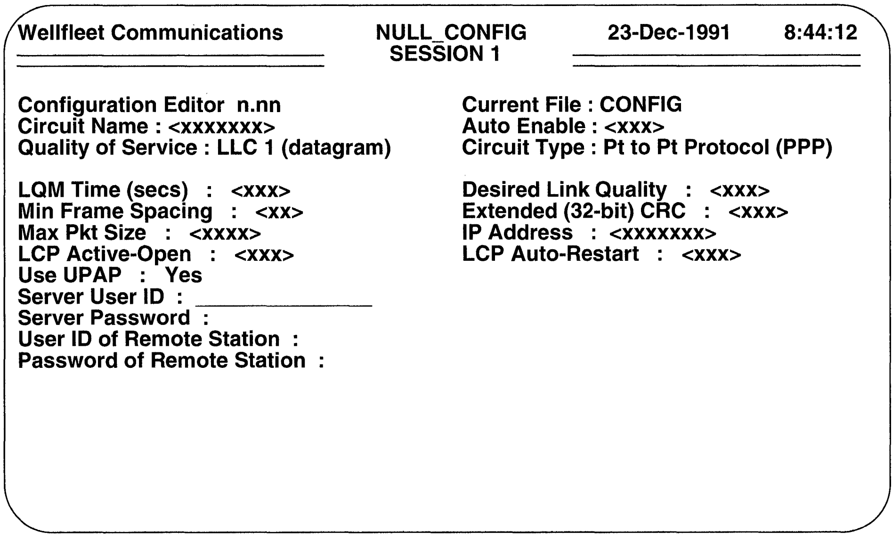
- **LCP Auto Restart** specifies whether PPP attempts to re-establish a LCP connection after the link has been declared down.

  Failure to receive Link-Quality-Report packets for the period defined by the **LQM Time (secs)** parameter, causes the link to go down. With **LCP Auto-Restart** set to **Yes**, PPP attempts to re-establish the LCP connection. With the parameter set to **No**, PPP does not attempt to re-establish the connection.

- **Use UPAP** enables the User Password Authentication Protocol (UPAP).

  PPP implementations may require a remote peer to authenticate itself before engaging in NCP negotiation. This initial configuration option is described in RFC 1172. If you do not want to enable UPAP, press `[RETURN]` to accept the default response, **No**.

  If you do want to enable UPAP, press the `[RIGHTARROW]` to display **Yes** and then press `[RETURN]`. The screen prompts for additional data.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Circuit Name : <xxxxxxxx>                     Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)         Circuit Type : Pt to Pt Protocol (PPP)

LQM Time (secs)  :  <xxx>                     Desired Link Quality  :  <xxx>
Min Frame Spacing  :  <xx>                    Extended (32-bit) CRC  :  <xxx>
Max Pkt Size  :  <xxxx>                       IP Address  :  <xxxxxxxx>
LCP Active-Open  :  <xxx>                     LCP Auto-Restart  :  <xxx>
Use UPAP  :  Yes
Server User ID  :  ______________
Server Password  :
User ID of Remote Station  :
Password of Remote Station  :
```

Figure 5-13 UPAP Parameters Screen

- **Server User ID** specifies the name (user ID) used by the router when it logs in to the remote PPP peer.

  Enter the name as an ASCII string of less than 16 characters.

- **Server Password** specifies the password used by the router when it logs in to the remote PPP peer.

  Enter the password as an ASCII string of less than 16 characters.

- ❒ **User ID of Remote Station** specifies the name (user ID) used by the remote PPP peer when its logs in to the local router.

  Enter the name as an ASCII string of less than 16 characters.

- ❒ **Password of Remote Station** specifies the password used by the remote PPP peer when its logs in to the local router.

  Enter the password as an ASCII string of less than 16 characters.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Configuration Menu.

You configure additional PPP circuits from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Circuits Summary Screen. Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Circuit Parameters Screen. Now follow the previously described procedures configure an additional PPP circuit; repeat this procedure until you have configured all PPP circuits.

5.5 Configuring SMDS Circuits

Switched Multi-megabit Data Service (SMDS) is a high-speed, connectionless, packet service offered by several local exchange carriers. SMDS extends LAN-like performance beyond the subscriber' premises across a metropolitan or wide area.

The SMDS implementation uses an HDLC-like protocol called SMDS Data Exchange Interface (DXI) protocol to manage communications between the multiprotocol router and a DSU/CSU. DXI, a proposed standard, defines an open interface between a router and a DSU and specifies how SMDS Level 3 Protocol Data Units (L3PDU) are encapsulated in HDLC and transmitted between the router and the DSU. The current SMDS implementation complies with Version 2.1 of the DXI protocol.

NOTE

The SMDS implementation supports the establishment of connections over V.35 synchronous media. It provides support for all protocol suites (AppleTalk, Bridge, DECnet Phase IV, IPX, TCP/IP, and XNS) over SMDS circuits.

The SMDS circuit parameters are listed in Table 5-8.

Before configuring an SMDS circuit, refer to the *Synchronous Line Summary Chart*. Any circuit listed on this chart as providing SMDS service must be configured as an SMDS circuit. You may also wish to use the *SMDS Circuit Summary Chart* (also in Appendix C) to maintain a record of SMDS circuit parameters.

You configure an SMDS circuit from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured circuits, the screen displays the following:

Table 5-8: SMDS Circuit Parameters

Parameter	Function
Circuit Name	identifies the SMDS circuit
Auto Enable	specifies the initialization state
Quality of Service	assigns LLC1 service level
Circuit Type	specifies an SMDS circuit
Min Frame Spacing	specifies frame spacing
Individual Address	specifies the SMDS local address
Group Address	specifies the SMDS broadcast address
ARP Group Address	specifies the ARP broadcast address
Use Extended (32-bit) CRC	selects an error-detection method
Max Pkt Size	specifies the maximum size of the SMDS packet
Use SNAP	specifies 802.6 version

No Circuits record(s) found
Do you wish to add Circuits record(s)?

Press `[RETURN]` to display the Circuit Parameters Screen.

If you have previously configured circuits, the screen displays the Circuits Summary Screen. To move to the Circuit Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

❒ **Circuit Name** identifies the SMDS circuit.

Enter the circuit name (taken from the *Synchronous Line Summary Chart*).

❒ **Auto Enable** specifies the initial state of the SMDS circuit.

This circuit-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the SMDS circuit when the multiprotocol router boots.

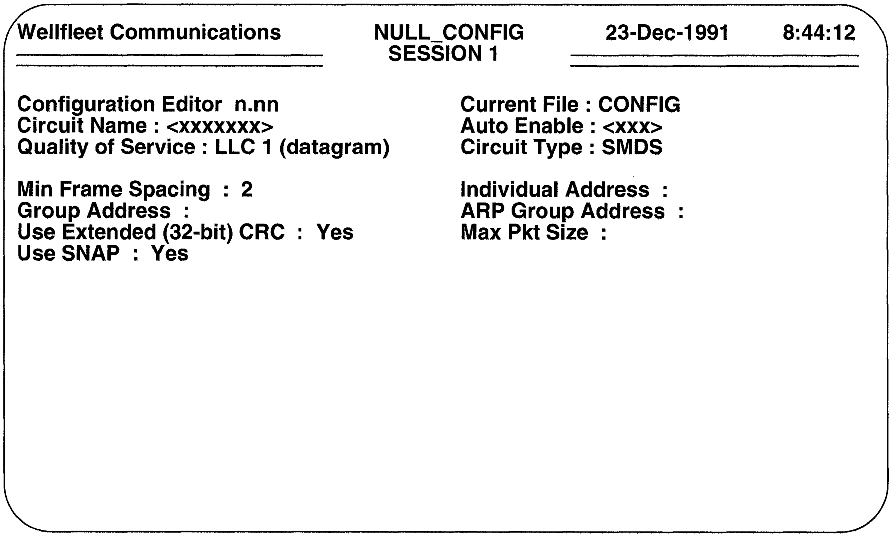
When global auto enable is **No**, the SMDS circuit is unconditionally disabled. You will later need to enable the circuit with NCL commands after the router boots.

When global auto enable is **Yes**, the circuit is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable) or **No** (disable), then press `[RETURN]`. If you select **No**, you will later need to enable the circuit with NCL commands after the router boots.

❒ **Quality of Service** is always **LLC1** for SMDS circuits.

❒ **Circuit Type** is **SMDS** for SMDS circuits.

After you specify an SMDS circuit, the screen displays the SMDS Circuit Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                         Current File : CONFIG
Circuit Name : <xxxxxxx>                           Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)              Circuit Type : SMDS

Min Frame Spacing  :  2                            Individual Address  :
Group Address  :                                   ARP Group Address  :
Use Extended (32-bit) CRC  :  Yes                  Max Pkt Size  :
Use SNAP  :  Yes
```

Figure 5-14 SMDS Circuit Parameters Screen

❒ **Min Frame Spacing** specifies the minimum number of flag sequences prefixed to the HDLC packet transmitted by SMDS.

As previously shown in Figure 5-5 an HDLC packet is prefixed by a variable number of 8-bit flag sequences, and is terminated by a single instance of the same flag. The number of flags transmitted between sequential packets is the sum of the constant 1 (the trailing flag) and the variable number of leading flags.

After determining the minimum number of flags to transmit between each packet, reduce this number by one (to account for the terminating flag), press the [RIGHTARROW] to display this or the closest available value, then press [RETURN].

❐ **Individual Address** specifies the 10-digit SMDS address.

SMDS addresses mirror the North American Numbering Plan (NANP). Enter the 10-digit decimal address.

❐ **Group Address** specifies an SMDS broadcast address.

SMDS service providers offer a multicast facility which associates a broadcast address with a set of individual SMDS addresses specified by the subscription agreement.

If your SMDS subscription provides broadcast service, enter the 10-digit decimal broadcast address, else press [RETURN].

❐ **ARP Group Address** specifies an IP address resolution multicast address.

Enter the 10-digit decimal address to be used for IP address resolution broadcasts. If the SMDS circuit will not carry IP traffic, simply press [RETURN].

❐ **Use Extended (32-bit) CRC** specifies an error detection scheme.

SMDS implementations may use either a 32-bit or 16-bit frame check sequence to detect errors.

Select **Yes** to use the a 32-bit CRC, or **No** to use a 16-bit CRC.

❐ **Max Pkt Size** specifies the maximum size of an SMDS packet transmitted by the router.

Enter the maximum size of the SMDS packet transmitted by the router.

❐ **Use SNAP** identifies the version of IEEE 802.6 to be used.

Yes specifies the approved version of IEEE 802.6 (D15). With 802.6 (D15), encapsulation is as specified by Internet RFC 1209, *IP Over SMDS*.

No specifies IEEE version(s) D9 and D11. With IEEE 802.6 (D9/D11), an AT&T proprietary encapsulation is used.

When the screen prompts **Hit Return to Continue**, press [RETURN] to go back to the Configuration Menu.

You configure additional SMDS circuits from the Configuration Menu. Enter <4> at **Enter Selection (0 for Previous Menu)**. The screen displays the Circuits Summary Screen. Press the [RIGHTARROW] to display **Add**, then press [RETURN] to display the Circuit Parameters Screen. Now follow the previously described procedure to configure an additional SMDS circuit; repeat this procedure until you have configured all SMDS circuits.

5.6 Configuring Frame Relay Circuits

Frame Relay is a newly-introduced, circuit-switched, high-speed packet service. Unlike the older X.25, which requires both network layer and data-link layer processing, Frame Relay operates exclusively at the data-link layer. At the data-link layer Frame Relay provides a small set of "core aspects" which provide checking for error-free packets and various network congestion avoidance techniques.

NOTE

The Frame Relay implementation supports the establishment of connections over synchronous media (V.35, T1, or E1 lines). It provides support for all protocol suites (AppleTalk, Bridge, DECnet Phase IV, IPX, TCP/IP, and XNS) over Frame Relay circuits.

The Frame Relay parameters are listed in Table 5-9.

Table 5-9: Frame Relay Circuit Parameters

Parameter	Function
Circuit Name	identifies the Frame Relay circuit
Auto Enable	specifies the initialization state
Quality of Service	assigns LLC1 service level
Circuit Type	specifies a Frame Relay circuit
DLCI Encoding Type	specifies the format of the Frame Relay Data Link Connection Identifier (DLCI)
DLCI Encoding Length	specifies the number of bytes in the Frame Relay address field
Maximum Packet Size	specifies the maximum size of the Frame Relay packet
Provide InARP	specifies whether the Frame Relay circuit implements the Inverse Address Resolution Protocol (InARP).
Management Type	specifies the management interface between the multiprotocol router and the Frame Relay network

Before configuring a Frame Relay circuit, refer to the *Synchronous Line Summary Chart*, the *T1 Line Summary Chart*, and the *E1 Line Summary Chart* . Any circuit listed on these charts as providing Frame Relay service must be configured as a Frame Relay circuit. You may also wish to use the *Frame Relay Circuit Summary Chart* (also in Appendix C) to maintain a record of Frame Relay circuit parameters.

You configure a Frame Relay circuit from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured circuits, the screen displays the following:

No Circuits record(s) found
Do you wish to add Circuits record(s)?

Press `[RETURN]` to display the Circuit Parameters Screen.

If you have previously configured circuits, the screen displays the Circuits Summary Screen. To move to the Circuit Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

❒ **Circuit Name** identifies the Frame Relay circuit.

Enter the circuit name (taken from the *Synchronous Line Summary Chart*, the *T1 Line Summary Chart*, or the *E1 Line Summary Chart*.

❒ **Auto Enable** specifies the initial state of the Frame Relay circuit.

This circuit-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the Frame Relay circuit when the router boots.

When global auto enable is **No**, the Frame Relay circuit is unconditionally disabled. You will later need to enable the circuit with NCL commands after the multiprotocol router boots.

When global auto enable is **Yes**, the circuit is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable) or **No** (disable), then press `[RETURN]`. If you select **No**, you will later need to enable the circuit with NCL commands after the router boots.

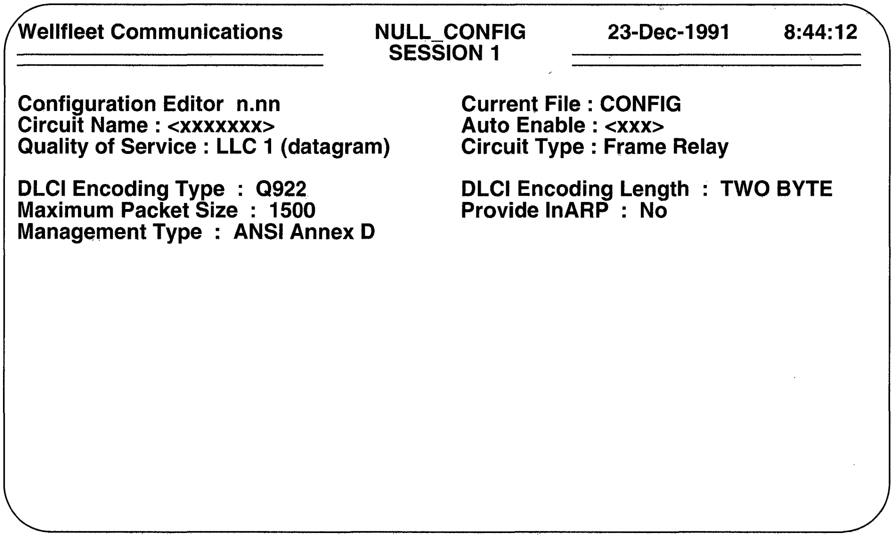
❒ **Quality of Service** is always **LLC1** for Frame Relay circuits.

❒ **Circuit Type** is **Frame Relay** for Frame Relay circuits.

After you specify a Frame Relay circuit, the screen displays the Frame Relay Circuit Parameters Screen (Figure 5-15).

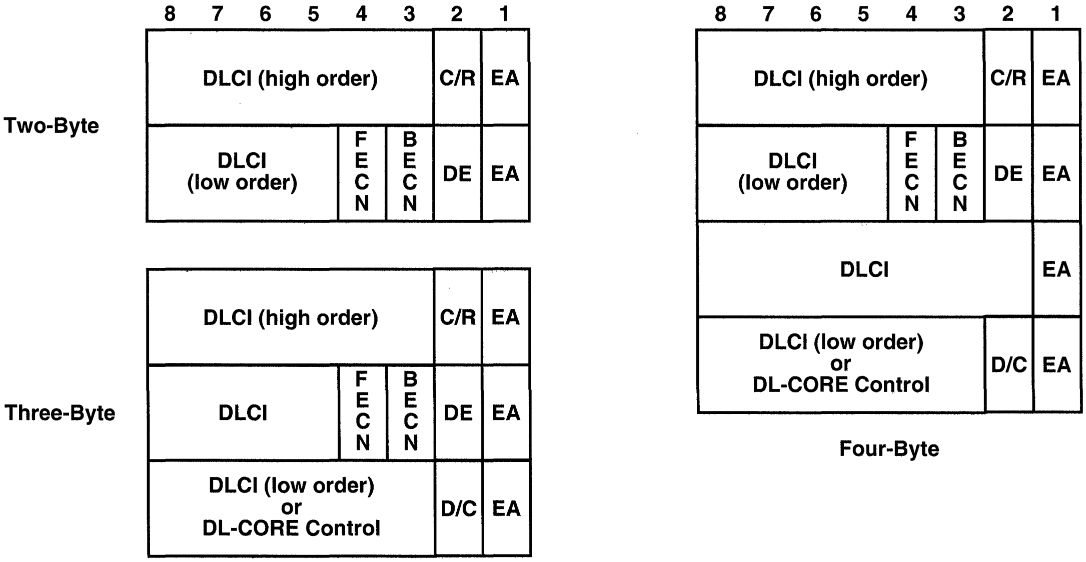
❒ **DLCI Encoding Type** selects the format of the DLCI.

The multiprotocol router supports four types of DLCI encoding. The default, **Q922**, selects DLCI encoding as described in CCITT draft standard Q.922. This standard specifies a 10-bit DLCI. While the DLCI is most often contained within a two-byte address field, the Q.922 standard allows for three-byte and four-byte address fields as shown in Figure 5-16. Regardless



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG
Circuit Name : <xxxxxxx>                        Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)           Circuit Type : Frame Relay

DLCI Encoding Type  :  Q922                     DLCI Encoding Length  :  TWO BYTE
Maximum Packet Size  :  1500                    Provide InARP  :  No
Management Type  :  ANSI Annex D
```

Figure 5-15 Frame Relay Circuit Parameters Screen



Two-Byte

<table>
<tr><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td colspan="6">DLCI (high order)</td><td>C/R</td><td>EA</td></tr>
<tr><td colspan="4">DLCI (low order)</td><td>FECN</td><td>BECN</td><td>DE</td><td>EA</td></tr>
</table>

Three-Byte

<table>
<tr><td colspan="6">DLCI (high order)</td><td>C/R</td><td>EA</td></tr>
<tr><td colspan="4">DLCI</td><td>FECN</td><td>BECN</td><td>DE</td><td>EA</td></tr>
<tr><td colspan="6">DLCI (low order)
or
DL-CORE Control</td><td>D/C</td><td>EA</td></tr>
</table>

<table>
<tr><th>8</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th></tr>
<tr><td colspan="6">DLCI (high order)</td><td>C/R</td><td>EA</td></tr>
<tr><td colspan="4">DLCI (low order)</td><td>FECN</td><td>BECN</td><td>DE</td><td>EA</td></tr>
<tr><td colspan="7">DLCI</td><td>EA</td></tr>
<tr><td colspan="6">DLCI (low order)
or
DL-CORE Control</td><td>D/C</td><td>EA</td></tr>
</table>

Four-Byte

Figure 5-16 DLCI Encoding Within Various Address Fields

of the address field length, Q.922 encoding provides for forward explicit congestion notification (FECN), backward explicit congestion notification (BECN), discard eligibility (DE), and address field extension (EA) within the second byte of the address field.

Q922 November encoding is identical to Q922 encoding save in the "extended forms" (three-byte and four-byte address fields). The only difference is that **Q922 November** encoding lacks a control indicator (D/C) bit in the least significant byte.

Q922 March defines an 11-bit DLCI and drops the DE bit from the second byte of the address field.

Q921 encoding (virtually obsolete) specifies a 13-bit DLCI within a two-byte address field. It drops the FECN, BECN, and DE bits from the second byte of the address field.

Select DLCI encoding on the basis of the encoding format used by the attached Frame Relay DCE device, and then press `[RETURN]`.

❒ **Desired Encoding Length** specifies the length of the Frame Relay address field.

In most cases, you will select the default, **TWO BYTE**. Should your Frame Relay service provide for extended (three-byte or four-byte) address fields, select the **THREE BYTE** or **FOUR BYTE** option.

NOTE

Two additional selections **TWO + CONTROL** and **THREE + CONTROL** are specific to Q922 encoding, but have not as yet been completely standardized. While these values can be selected with Q922 encoding type, the control field is undefined.

❒ **Maximum Packet Size** specifies the largest packet which can be handled by the Frame Relay network.

Enter the packet length (in bytes, up to a maximum of 1600), then press `[RETURN]`.

❒ **Provide InARP** enables or disables the Inverse Address Resolution Protocol (InARP).

InARP, an extension to the Address Resolution Protocol, enables the router to resolve a given DLCI to a specific protocol address. Within the Frame Relay environment, new PVCs may be announced through the exchange of signalling messages between the Frame Relay DCE and the multiprotocol router. These signalling exchanges provide an indication of the DLCI assigned to the PVC, but provide no information regarding protocol addressing (thus severely limiting the immediate utility of the PVC). InARP enables the multiprotocol router to discover the protocol address of the remote station associated with the newly-announced DLCI.

Select **Yes** (enable InARP) or **No** (disable InARP), and then press `[RETURN]`.

❒ **Management Type** chooses between interface management modes.

The interface between the multiprotocol router and the Frame Relay network is generally defined by one of two commonly-implemented standards. Both standards generally specify notification procedures for the addition or deletion of PVCs, indications of the availability or unavailability of PVCs, and verification of link integrity.

ANSI Annex D specifies interface management procedures defined in Annex D to ANSI Standard T1617-1991.

LMI (Local Management Interface) specifies a set of vender-generated enhancement to the original Annex D procedures.

UNSUPPORTED specifies no management interface between the multiprotocol router and the Frame Relay network. In this instance all PVCs must be manually configured.

NOTE

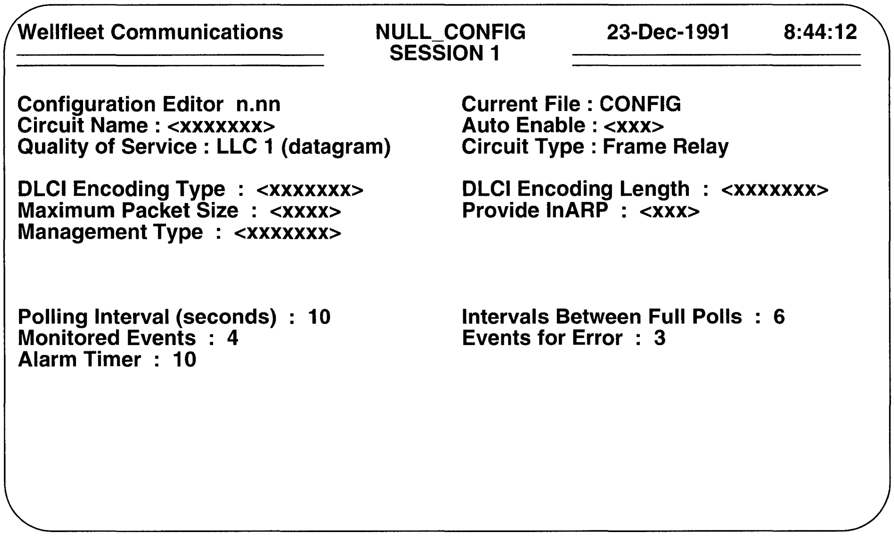
Two other options **LMI Switch** and **Annex D Switch** are intended to support test/debug environments where two Wellfleet multiprotocol routers are directly connected. In the event of such a configuration, one router should be configured as a DTE (with **ANSI Annex D** or **LMI** specified as the **Management Type**), and the other router as a DCE (with **Annex D Switch** or **LMI Switch** specified as the **Management Type**).

If you specify either **ANSI Annex D** or **LMI** for the **Management Type**, the screen prompts for additional parameters as shown in Figure 5-17.

❒ **Polling Interval (seconds)** specifies the interval between *Status Enquiry* messages transmitted by the router to the Frame Relay network.

The *Status Enquiry* message requests the Frame Relay network to respond with a *Link Integrity Verification* to verify the status of the DCE/DTE link.

Enter the interval (within the range 5 to 30 seconds) between *Status Enquiry* messages, and then press `[RETURN]`.



```
Wellfleet Communications           NULL_CONFIG        23-Dec-1991     8:44:12
                                    SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Circuit Name : <xxxxxxx>                       Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)          Circuit Type : Frame Relay

DLCI Encoding Type  :  <xxxxxxx>               DLCI Encoding Length  :  <xxxxxxx>
Maximum Packet Size  :  <xxxxx>                Provide InARP  :  <xxx>
Management Type  :  <xxxxxxx>


Polling Interval (seconds)  :  10              Intervals Between Full Polls  :  6
Monitored Events  :  4                         Events for Error  :  3
Alarm Timer  :  10
```

Figure 5-17 Frame Relay Management Interface Parameters Screen

❒ **Intervals Between Full Polls** specifies the interval between *Full Status Enquiry* messages transmitted by the router to the Frame Relay network.

The *Full Status Enquiry* message requests the Frame Relay network to respond with a *Full Status Report* which lists all PVCs, the PVC state (active or inactive), and whether the PVC is new or previously established.

The default response, **6**, indicates that the multiprotocol router sends a *Full Status Enquiry* message every 6 polling intervals; that is, if the polling interval is 10, the router sends a *Full Status Enquiry* every 60 seconds.

Enter a value within the range 1 to 255, and then press `[RETURN]`.

❒ **Monitored Events** (in conjunction with **Events for Error**) specifies a quality of service metric for the Frame Relay DCE/DTE connection

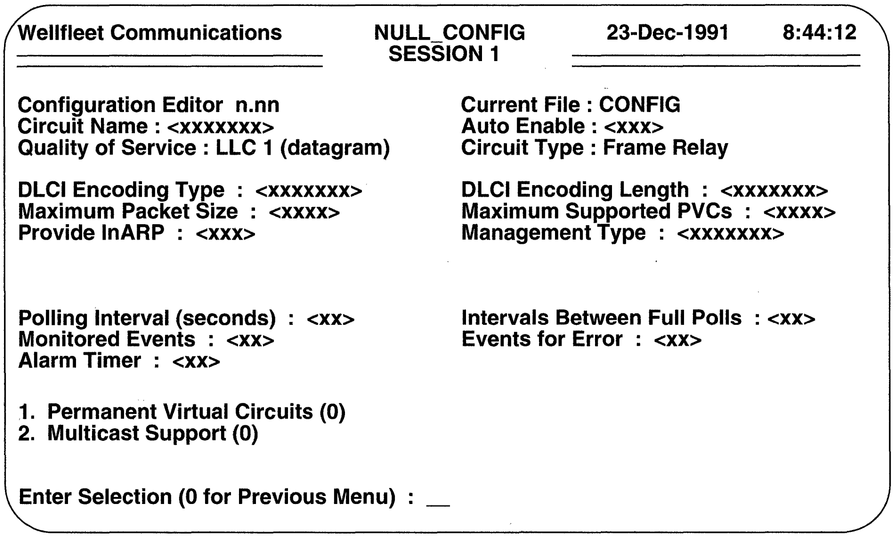
These two parameters specify a *j* out of *k* relationship used to measure circuit reliability as follows. If the number of faulty status exchanges (*Status Enquiry*, *Link Integrity Verification*, *Full Status Enquiry*, and/or *Full Status Report* messages) in a continuous sequence of *k* (**Monitored Events**) such events, equals or exceeds *j* (**Events for Error**), the interface is declared down. While the connection is down, status exchanges continue. Once *j* consecutive status exchanges are transferred without error, the connection is restored to the active state.

Toggle the `[RIGHTARROW]` and then press `[RETURN]` to specify first the number of events that are monitored for error conditions (**Monitored Events**), and second the number of error events that will cause the connection to go down (**Events for Error**).

- **Alarm Timer** specifies the interval between the issuance of a *Status Enquiry* or *Full Status Enquiry* message and the receipt of a *Link Integrity Verification* or *Full Status Report* from the Frame Relay DCE.

  Select a value (less than or equal to **Polling Interval**), and then press `[RETURN]`.

After you press `[RETURN]`, the screen prompts for additional information as shown in Figure 5-18. If you do not need to configure Frame Relay multicast service or to manually configure PVCs, enter `0` at **Enter Selection (0 for Previous Menu)** to return to the Main Menu.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                       Current File : CONFIG
Circuit Name : <xxxxxxxx>                        Auto Enable : <xxx>
Quality of Service : LLC 1 (datagram)            Circuit Type : Frame Relay

DLCI Encoding Type  :  <xxxxxxx>                 DLCI Encoding Length  :  <xxxxxxx>
Maximum Packet Size  :  <xxxxx>                  Maximum Supported PVCs  :  <xxxx>
Provide InARP  :  <xxx>                          Management Type  :  <xxxxxxx>


Polling Interval (seconds)  :  <xx>              Intervals Between Full Polls  : <xx>
Monitored Events  :  <xx>                        Events for Error  :  <xx>
Alarm Timer  :  <xx>

1.  Permanent Virtual Circuits (0)
2.  Multicast Support (0)

Enter Selection (0 for Previous Menu)  :  __
```

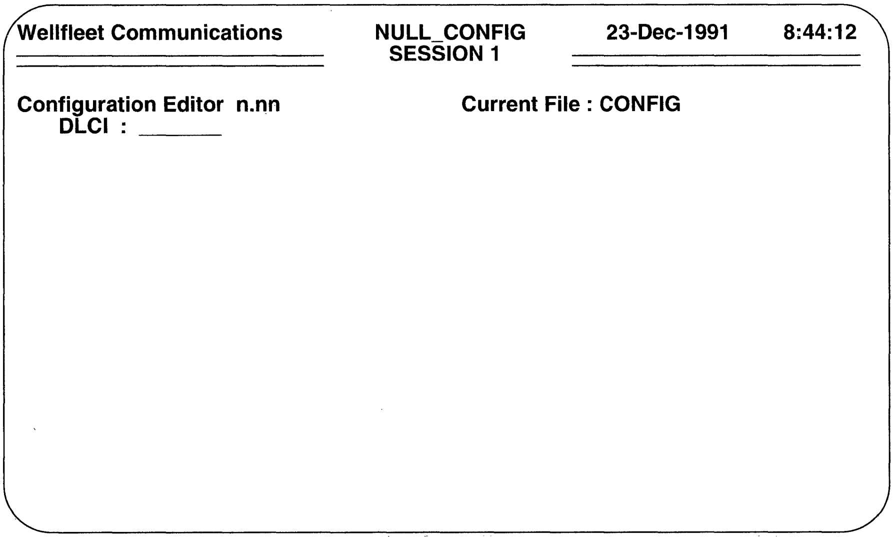
Figure 5-18 Frame Relay Supplemental Support Access Screen

5.6.1 Frame Relay PVCs

In the unlikely absence of Annex D or LMI network management services (when the **Management Type** parameter is set to **UNSUPPORTED**), you must manually configure all Frame Relay PVCs. You configure PVCs from the Frame Relay Supplemental Support Access Screen. To begin, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. After the screen displays

No Permanent Virtual Circuits Record(s) found
Do you wish to add Permanent Virtual Circuits Record(s)

press [RETURN] to display the Frame Relay PVC Configuration Screen (Figure 5-19).



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
    DLCI  : ______
```

Figure 5-19 Frame Relay PVC Configuration Screen

At **DLCI** enter the network-assigned DLCI (in decimal format) and then press [RETURN]. When the console screen prompts **Hit Return to Continue**, press [RETURN] to go back to the Frame Relay Supplemental Support Access Screen.

To configure additional PVCs, enter <1> at the **Enter Selection (0 for Previous Menu)** prompt. In response, the screen displays a list of previously configured PVCs; now press the [RIGHTARROW] to display **Add**, and then press [RETURN] to access the Fame Relay PVC Configuration Screen. Now use the procedure previously described in this section to configure additional PVCs.

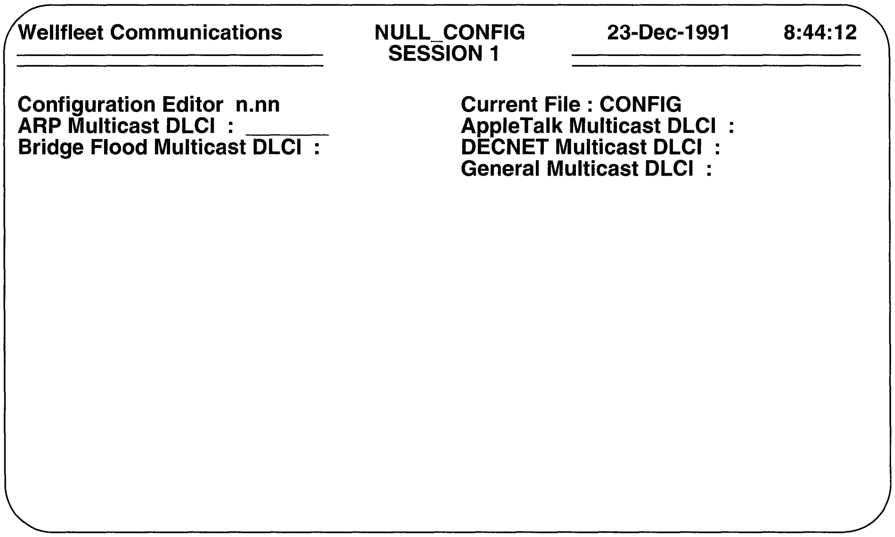
5.6.2 Frame Relay Multicast Support

Frame Relay multicast support enables the multiprotocol router to take advantage of multicast functionality offered (or anticipated to be offered) by some Frame Relay service providers. Frame Relay multicasting reserves certain network-assigned DLCIs as multicast addresses. The Frame Relay network maps multiple recipients (an address group) to this single DLCI and delivers copies of a single Frame Relay packet to each member of the address group. As the packet passes through the Frame Relay network, the DLCI is manipulated so that the packet recipient receives a DLCI indicating the actual packet source (not the multicast DLCI). Multicasting is generally used in certain address resolution techniques and for applications that require the delivery of identical information to multiple recipients.

You implement multicast support from the Frame Relay Supplemental Support Access Screen. Enter <2> at the **Enter Selection (0 for Previous Menu)** prompt. After the screen displays

No Multicast Support Record(s) found
Do you wish to add Multicast Support Record(s)

press [RETURN] to display the Frame Relay Multicast Screen.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
ARP Multicast DLCI  : _______                 AppleTalk Multicast DLCI  :
Bridge Flood Multicast DLCI  :                DECNET Multicast DLCI  :
                                              General Multicast DLCI  :
```

Figure 5-20 Frame Relay Multicast Screen

At each field (**ARP Multicast DLCI**, **AppleTalk Multicast DLCI**, **Bridge Flood Multicast DLCI**, **DECNET Multicast DLCI**, and **General Multicast DLCI**) enter the network-assigned DLCI appropriate for each type of protocol traffic. To skip a field, simply press `[RETURN]`.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Frame Relay Supplemental Support Access Screen.

5.6.3 Adding Frame Relay Circuits

You configure additional Frame Relay circuits from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Circuits Summary Screen. Next, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the Circuit Parameters Screen. Now follow the previously described procedures to configure an additional Frame Relay circuit; repeat these procedures until you have configured all Frame Relay circuits.

6 Configuring X.25 Service

This chapter tells you how to configure X.25 packet-switched service. The multiprotocol router provides three levels of X.25 service, as follows:

X.25 DDN

X.25 DDN (Defense Data Network) service provides end-to-end connectivity between the router and a remote host or gateway equipped to support DDN "Standard Service". DDN service is used only by TCP/IP to transmit IP datagrams over the DDN.

X.25 PDN

X.25 PDN (Public Data Network) service provides end-to-end connectivity between the router and a remote host or device equipped to support Internet RFC 877 X.25 service. (RFC 877 specifies a standard for the transmission of IP datagrams over public data networks). PDN service is used only by TCP/IP to transmit IP datagrams over public data networks.

X.25 Pt to Pt

X.25 Pt to Pt service provides end-to-end connectivity via an intervening X.25 network between local and remote peer routers. Pt to Pt service can be used by any protocol suite (AppleTalk, Bridge, DECnet Phase IV, IPX, TCP/IP, and/or XNS).

Establishing X.25 service is a two-step process: you begin the process by configuring a LAPB circuit, and complete it by configuring network-level services. The following sections provide a series of instructions for configuring LAPB circuits and the three X.25 service levels. Depending on your network requirements, you may need to refer to all sections, or to only some of the sections.

6.1 Configuring LAPB Circuits

A LABP (Link Access Protocol/Balanced) circuit provides access to X.25 packet-switched networks. Each LABP circuit supports concurrent operation of X.25 service levels with the caveat that *X.25 DDN and X.25 PDN (which are identical in packet and frame format, and thus indistinguishable) service cannot be concurrently supported by the same LAPB circuit.*

NOTE

The router's LAPB implementation supports the establishment of LAPB connections over synchronous media (V.35, T1, or E1 lines). Depending on the type of X.25 network service (DDN, PDN, or Pt to Pt), it provides support for all protocol suites (AppleTalk, Bridge, DECnet Phase IV, IPX, TCP/IP, and XNS).

The LAPB parameters are listed in Table 6-1.

Table 6-1: LAPB Circuit Parameters

Parameter	Function
Circuit Name	identifies the LAPB circuit
Auto Enable	specifies the initialization state
Quality of Service	assigns X.25 service level
Circuit Type	specifies a LAPB circuit
PDN	specifies the service provider
T1	specifies a T1 timer value
N2	specifies retransmission attempts
Min Frame Spacing	specifies frame spacing
Flow Ctrl	enables Flow Control Parameter Negotiation
Pkt Window	specifies the number of outstanding (unacknowledged) packets
Pkt Size	specifies the maximum size of the X.25 packet
SVCs	enables the establishment of switched virtual circuits

Before configuring a LAPB circuit, refer to the *Synchronous Line Summary Chart*, the *T1 Line Summary Chart*, and the *E1 Line Summary Chart*. Any circuit listed on these charts as providing X.25 service must be configured as a LAPB circuit. You may also wish to use the *LAPB Circuit Summary Chart* (also in Appendix C) to maintain a record of LAPB circuit parameters.

You configure a LAPB circuit from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. If you have not previously configured any circuits, the screen displays the following:

No Circuits record(s) found
Do you wish to add Circuits record(s)?

Press `[RETURN]` to display the Circuit Parameters Screen (Figure 5-1).

However, if you have previously configured circuits, the screen displays the Circuits Summary Screen (Figure 5-3). To move to the Circuit Parameters Screen, at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`.

❒ **Circuit Name** identifies the LAPB circuit.

Enter the circuit name.

❒ **Auto Enable** specifies the initial state of the LAPB circuit.

This circuit-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the LAPB circuit when the multiprotocol router boots.

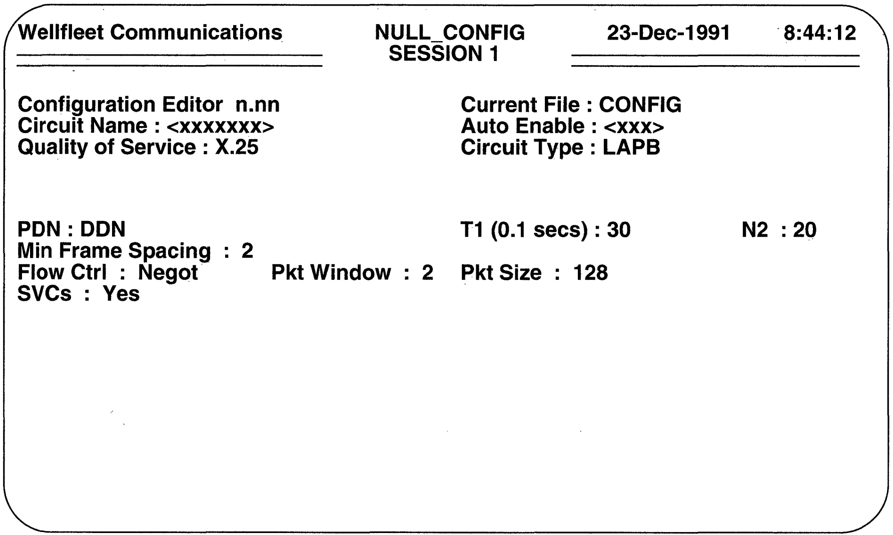
When global auto enable is **No**, the LAPB circuit identified by **Circuit Name** is unconditionally disabled. You will subsequently need to enable **Circuit Name** with NCL commands after the router boots.

When global auto enable is **Yes**, the LAPB circuit is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable **Circuit Name**) or **No** (disable **Circuit Name**), then press `[RETURN]`. If you select **No**, you will subsequently need to enable the circuit with NCL commands after the router boots.

❒ **Quality of Service** is always **X.25** for LAPB circuits.

❒ **Circuit Type** is **LAPB** for LAPB circuits.

After you specify a LAPB circuit, the screen displays the LAPB Circuit Parameters Screen (Figure 6-1).



```
Wellfleet Communications           NULL_CONFIG       23-Dec-1991     8:44:12
                                    SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Circuit Name : <xxxxxxx>                       Auto Enable : <xxx>
Quality of Service : X.25                      Circuit Type : LAPB


PDN : DDN                                      T1 (0.1 secs) : 30       N2  : 20
Min Frame Spacing  :  2
Flow Ctrl  :  Negot        Pkt Window  :  2    Pkt Size  :  128
SVCs  :  Yes
```

Figure 6-1 LAPB Circuit Parameters Screen

❐ **PDN** identifies the supplier of X.25 services.

Four of the available responses (**DDN**, **TELENET**, **UK-PSS**, and **NET2**) identify specific providers of X.25 services. If your X.25 provider is one of these, press the `[RIGHTARROW]` to display the name of the provider, then press `[RETURN]`.

If your X.25 provider is not listed, press the `[RIGHTARROW]` to display **Other** (thus configuring the router to interface with a non-specific packet-switched network), then press `[RETURN]`.

If you wish, you can explicitly configure certain low-level attributes that specify the interface between the router and a packet-switched network. To specify these attributes, press the `[RIGHTARROW]` to display **Use Bitmap**, then press `[RETURN]`.

If you select **Use Bitmap**, the cursor moves downward and to the right to a newly displayed field, **Bitmap (hex)**.

❐ **Bitmap (hex)** constructs a 32-bit status word that specifies certain low-level attributes of the interface between the router and the X.25 service provider.

Refer to Table 6-2 to construct the status word. Enter the status word in 8-digit hexadecimal format and press `[RETURN]`.

Table 6-2: X.25 Bitmap Values

Bit	Function	ON (1)	OFF (0)
0	FORCE FRMR	If X.25 sends a FRMR on the line, the reception of any frame other than an SABM, DISC, or FRMR causes another FRMR to be sent.	If X.25 sends a FRMR on the line, the reception of any frame other than an SABM, DISC, or FRMR is ignored.
1	FRMR ON RR	If X.25 sends a FRMR on the line, the reception of an RR frame causes another FRMR to be sent; all other frames (except SABM, DISC, or FRMR) are ignored.	If X.25 sends a FRMR on the line, the reception of any frame other than an SABM, DISC, or FRMR (to clear the condition) is ignored.
2	CLEAR P/F	Receiving an unknown frame causes a FRMR frame to be sent with its P/F bit set to zero (0) regardless of the P/F setting in the received frame.	Receiving an unknown frame causes a FRMR frame to be sent with its P/F bit set to the same value as the P/F bit in the received frame.
3	DISC ANSWER	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it responds with a UA.	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it responds with a DM.
4	DISC ACTION	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it sends an SABM immediately upon responding to the previous flag.	If X.25 sends an SABM (or is waiting for one), and receives a DISC, it disconnects the link after responding to the previous flag.

Table 6-2: X.25 Bitmap Values

Bit	Function	ON (1)	OFF (0)
5	INFO COUNT	IF X.25 (1) enters the T1 time-out state, (2) sends an RR, (3) obtains an RR response, and (4) transmits the unacknowledged INFOR frame -- the retry counter is not cleared until the retransmitted INFO frame is acknowledged. This procedure avoids an endless loop the would occur if the DCE were processing RR frames, but not INFO frames.	IF X.25 (1) enters the T1 time-out state, (2) sends an RR, (3) obtains an RR response, and (4) transmits the unacknowledged INFOR frame -- the retry counter is cleared immediately per the CCCIT definition. This procedure leaves open the possibility of an endless loop if the DCE were processing RR frames, but not INFO frames.
6	N2 ACTION	If X.25 is waiting for an UA, and receives either a T1 time-out or a DM, it retries the SABM up to N2 (40) times. If (after N2 retries) it has still not received a UA, it goes to disconnect mode and ceases to transmit SABMs.	If X.25 is waiting for an UA, and receives either a T1 time-out or a DM, it retries the SABM up to N2 (40) times. If (after N2 retries) it has still not received a UA, it goes to disconnect mode and continues sending SABMs at intervals of T3 (20) seconds.
7	ACTIVE CONNECTION	X.25 begins sending SABMs as soon as the physical connection is established	X.25 waits for an SABM from the remote end to initiate establishment at the Frame level.
8	CALL DATA	X.25 will accept a CALL ACCEPT packet containing a User Data Field, even if Fast Select was not specified in the call request.	X.25 will not accept a CALL ACCEPT packet containing a User Data Field, unless Fast Select was specified in the call request.

Table 6-2: X.25 Bitmap Values

Bit	Function	ON (1)	OFF (0)
9	D BIT CONFIRMATION	X.25 disables the D bit in CALL CONFIRM packets.	X.25 enables the D bit in CALL CONFIRM packets.
10	COLLISION REJECT	If a Clear Collision occurs, and the received CLEAR packet has a bad length, X.25 sends a new CLEAR packet with a diagnostic code.	If a Clear Collision occurs, and the received CLEAR packet has a bad length, X.25 drops the CLEAR packet.
11	TIMER DIAG	If a T20 (3 minutes) time-out occurs, X.25 retransmits a RESTART packet with the original diagnostic code.	If a T20 (3 minutes) time-out occurs, X.25 retransmits a RESTART packet with a "T20 Expired" diagnostic code.
12	CLEAR LENGTH	X.25 rejects CLEAR INDICATION and CLEAR CONFIRMATION packets if they contain facilities or user data.	X.25 accepts CLEAR INDICATION and CLEAR CONFIRMATION packets even if they contain facilities or user data.
13	UNASSIGNED LCN	X.25 clears calls received on an invalid LCN.	X.25 ignores calls received on an invalid LCN.
14	DATAPAC FACILITIES	X.25 enables special DATAPAC facilities checking.	X.25 disables special DATAPAC facilities checking.
15	LINE RESTART	X.25 transmits a RESTART packet whenever Frame Level is established.	X.25 does not transmit a RESTART packet whenever Frame Level is established.
16	ADDRESS SUPPRESSION	X.25 includes the local X.121 address in any CALL packet sent from the device.	X.25 does not include the local X.121 address in any CALL packet sent from the device.

Table 6-2: X.25 Bitmap Values

Bit	Function	ON (1)	OFF (0)
17	X.25 VERSION	X.25 (1984)	X.25 (1980)
18	FRAME LEVEL KEEP ALIVE	X.25 generates an RR (with the Poll bit set) when the link has been idle for two seconds. In the absence of DCE response, X.25 initiates normal retry and link recovery procedures.	X.25 does not poll the link when it is idle.
19	LINE_MODE	X.25 functions as DCE at Frame and Packet levels.	X.25 functions as DTE at Frame and Packet levels.
20 to 31	Reserved	N/A	Set to 0

- ❐ **T1** (the T1 timer value) specifies the time interval a frame can remain unacknowledged.

  Typically a T1 value in excess of 3 seconds is required only if your network connection has a substantial path delay (for instance, if the connection is accomplished with a satellite link). Under these conditions, T1 must have a value greater than the round-trip frame-transmission time, plus the time required to process the frame at the receiving end.

NOTE

If the **T1** value is too small, throughput is reduced because of needless retransmittal of frames; if **T1** is too large, X.25 takes an excessive length of time to detect lost frames.

Enter the T1 timer value, taking note that the timer is expressed in tenths of seconds (for example, a value of 30 sets the timer to 3 seconds). Note also that the value of **T1** must be the same for both ends of the link.

- ❐ **N2** specifies the number of times a frame is retransmitted before the circuit is reset.

  If a frame remains unacknowledged at the expiration of the T1 timer, X.25 retransmits the outstanding frame up to N2 times, with each retransmittal requesting an immediate acknowledgment. If the frame remains unacknowledged after N2 retries, the router resets the X.25 service. Valid **N2** values are in the range 1 to 255.

- ❐ **Min Frame Spacing** specifies the minimum number of flag sequences prefixed to an X.25 packet.

  As is the HDLC packet previously shown in Figure 5-5, an X.25 frame is prefixed by a variable number of 8-bit flag sequences, and is terminated by a single instance of the same flag. Therefore, the number of flags transmitted between sequential frames is equal to the constant 1 (the trailing flag) plus the (variable) number of leading flags.

  After determining the minimum number of flags to prefix to each frame, reduce this number by 1 (to account for the terminating flag), press the `[RIGHTARROW]` to display this or the closest available value, then press `[RETURN]`.

- ❐ **Flow Ctrl** enables or disables Flow Control Parameter Negotiation.

  Flow Control Parameter Negotiation is available as a subscription option from most X.25 service providers. **Deflt**, disables negotiation in *call request* packets across the LAPB circuit. With negotiation disabled, the configured values for **Pkt Window** and **Pkt Size** serve as the defaults across the circuit. If you disable flow control, you must ensure that the X.25 DCE has also disabled flow control. Additionally, you must ensure that the values you select for **Pkt Window** and **Pkt Size** match those of the DCE.

  Negot enables negotiation. With flow control enabled, the window and packet size are negotiated on a virtual circuit basis.

  Use the `[RIGHTARROW]` to enable (**Negot**) or disable (**Deflt**) Flow Control Parameter Negotiation, and then press `[RETURN]`.

NOTE

If you disable Flow Control Parameter Negotiation (**Flow Ctrl** equals **Deflt**), you should ensure that the remote DTE has also disabled negotiation and that its assigned values for **Pkt Window** and **Pkt Size** match those of the local DTE.

- ❐ **Pkt Window** specifies the maximum number of outstanding (unacknowledged) packets.

  Use the `[RIGHTARROW]` to select a value from **1** through **7**, then press `[RETURN]`.

- ❐ **Pkt Size** specifies the maximum number of bytes in the information field of an X.25 level-3 packet.

  Use the `[RIGHTARROW]` to select a value from **16** through **2048**, then press `[RETURN]`.

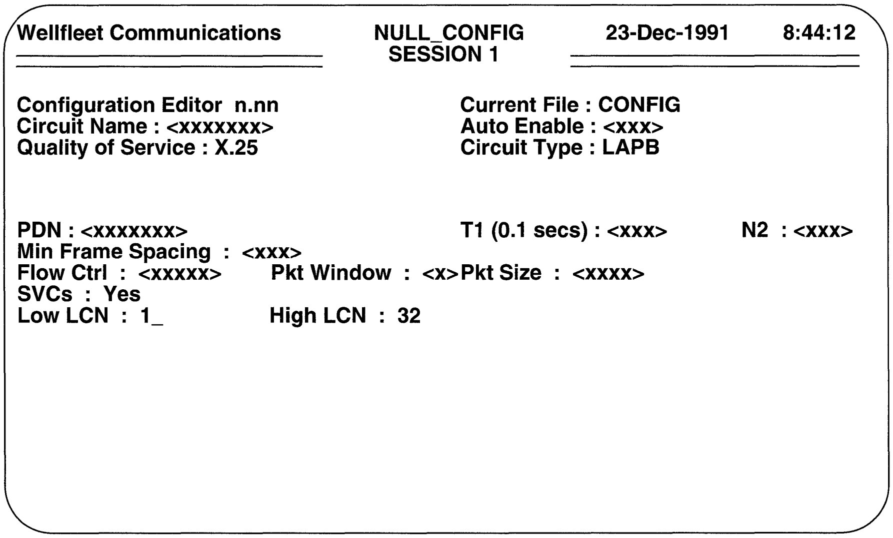
NOTE

Current buffer size limitations prevent upper level redirecting protocols from presenting packets larger than 1600 bytes to X.25. Consequently, the actual maximum size of the information field that will actually be transmitted by X.25 (even if **Pkt Size** is set to 2048) is 1600 bytes.

□ **SVCs** enables the establishment of switched virtual circuits.

Press `[RETURN]` to enable the establishment of switched virtual circuits.

After you press `[RETURN]` the screen prompts for additional information as shown in Figure 6-2.



```
Wellfleet Communications        NULL_CONFIG          23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Circuit Name : <xxxxxxxx>                     Auto Enable : <xxx>
Quality of Service : X.25                     Circuit Type : LAPB


PDN : <xxxxxxxx>                              T1 (0.1 secs) : <xxx>       N2  : <xxx>
Min Frame Spacing  :  <xxx>
Flow Ctrl  :  <xxxxxx>       Pkt Window  :  <x>Pkt Size  :  <xxxx>
SVCs  :  Yes
Low LCN  :  1_               High LCN  :  32
```

Figure 6-2 X.25 LCN Parameters Screen

□ **Low LCN** (logical channel number) sets the minimum logical channel number.

The logical channel number, also called the logical channel identifier, is a decimal number that identifies the switched virtual circuit.

Press the `[RIGHTARROW]` to select **1** (the default) or enter a numeric value within the range 0 to 999, then press `[RETURN]`.

❐ **High LCN** sets the maximum logical channel number.

The router supports up to 32 dedicated switched virtual circuits (used for X.25 Pt to Pt service) for each LAPB connection and up to 254 switched virtual circuits per slot. Upon initialization, the router first allocates dedicated switched virtual circuits to X.25 Pt to Pt service; it then makes the remaining logical channels available (on an equal basis) to X.25 PDN, X.25 DDN, or X.25 Switch services.

If the LAPB circuit supports only X.25 Pt to Pt service, add the number of dedicated switched two-way virtual circuits provided for by your X.25 subscription agreement to the value assigned to **Low LCN** and then decrease the result by 1.

If you are configuring only X.25 DDN, X.25 PDN, and/or X.25 Switch service on the current slot, use the following formula to calculate **High LCN**:

High LCN = [254 / N] + Low_LCN - 1

where:

N	is the number of LAPB circuits on the slot.
[254 / N]	is the integer quotient of 254 divided by N.
Low_LCN	is the value assigned to the **Low LCN** parameter.

If you are configuring a combination of X.25 DDN, X.25 PDN or X.25 Switch service in conjunction with X.25 Pt to Pt service, use the following formula to calculate **High LCN**:

High LCN = [(254 - V) / N] + Low_LCN - 1

where:

V	is the number of dedicated Pt to Pt service virtual circuits on the slot.
N	is the number of LAPB B circuits on the slot.
[254 / N]	is the integer quotient of 254 divided by N.
Low_LCN	is the value assigned to the **Low LCN** parameter.

Enter the value of **High LCN** (within the range 0 to 999) as calculated above, then press `[RETURN]`.

NOTE

Because the logical channel number range for the physical link determines the number of virtual connections that can be established, the values assigned to **Low LCN** and **High LCN** must be identical on both sides of the X.25 physical link.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Configuration Menu.

You configure additional LAPB circuits from the Configuration Menu. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. Because you have already configured a LAPB circuit, the screen displays the Circuits Summary Screen (Figure 5-3). This screen lists each previously configured circuit along with its circuit type.

Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Circuit Parameters Screen (Figure 5-1). Now follow the previously described procedure to configure an additional LAPB circuit. Repeat this procedure until you have configured all LAPB circuits.

6.2 Configuring X.25 Network-Level Service

After configuring circuits, you configure X.25 network-level services. Depending on your requirements, use some or all of the following sections to configure network-level services.

6.2.1 X.25 PDN Service

X.25 PDN service provides service as specified in Internet RFC 877. Such access enables TCP/IP to use the 877-conforming network's packet-switching facilities to transfer IP datagrams to a remote host or gateway (note that the remote host or gateway need not be a peer router).

You configure X.25 PDN service from the Configuration Menu. Enter the number that appears to the left of **X.25 Network Service** at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

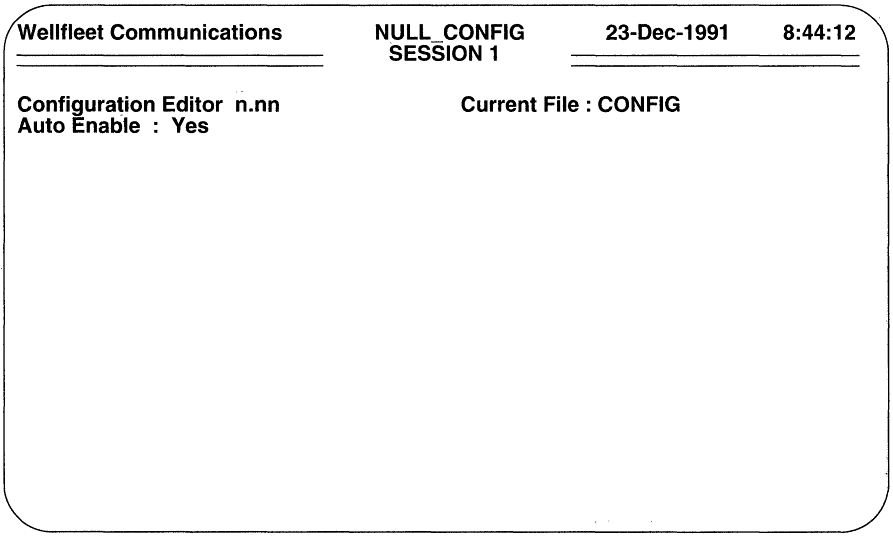
No X.25 Network Service record(s) found
Do you wish to add X.25 Network Service record(s)?

Press `[RETURN]` to display the X.25 Auto Enable Screen (Figure 6-3).

❐ **Auto Enable** specifies the initial state of X.25 services.

This X.25-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable X.25 services when the router boots.

When global auto enable is **No**, X.25 services are unconditionally disabled. You will later need to enable X.25 services with NCL commands after the router boots.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Auto Enable  :  Yes
```

Figure 6-3 X.25 Auto Enable Screen

When global auto enable is **Yes**, X.25 services are conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable X.25 services) or **No** (disable X.25 services), then press `[RETURN]`. If you select **No**, you will later need to enable X.25 services with NCL commands after the router boots.

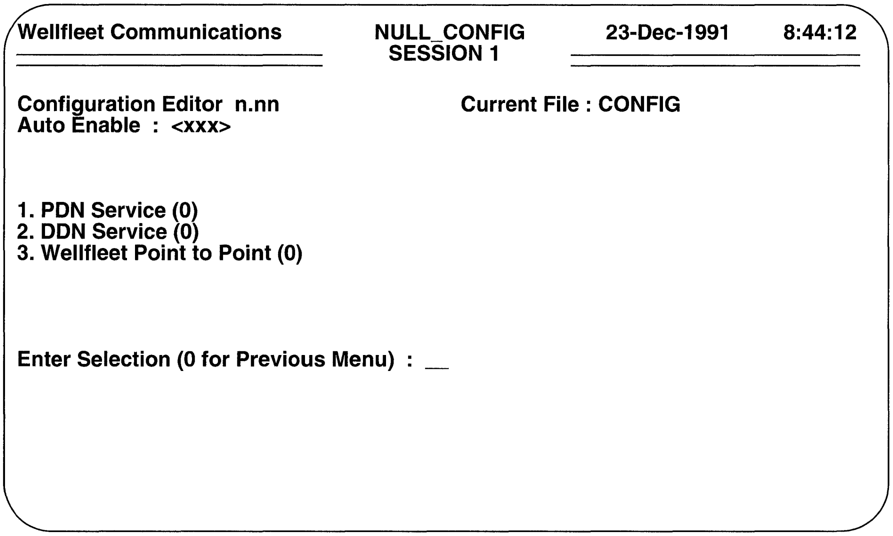
After you specify the initialization state, the screen displays the X.25 Service Selection Screen (Figure 6-4). With the cursor at **Enter Selection (0 for Previous Display)**, enter `<1>` to configure X.25 PDN service. After you do so, the screen displays the X.25 PDN Service Parameters Screen (Figure 6-5).

- ❐ **Lower Circuit Name** identifies the LAPB circuit that provides the network interface.

  Enter the name of the previously configured LAPB circuit.

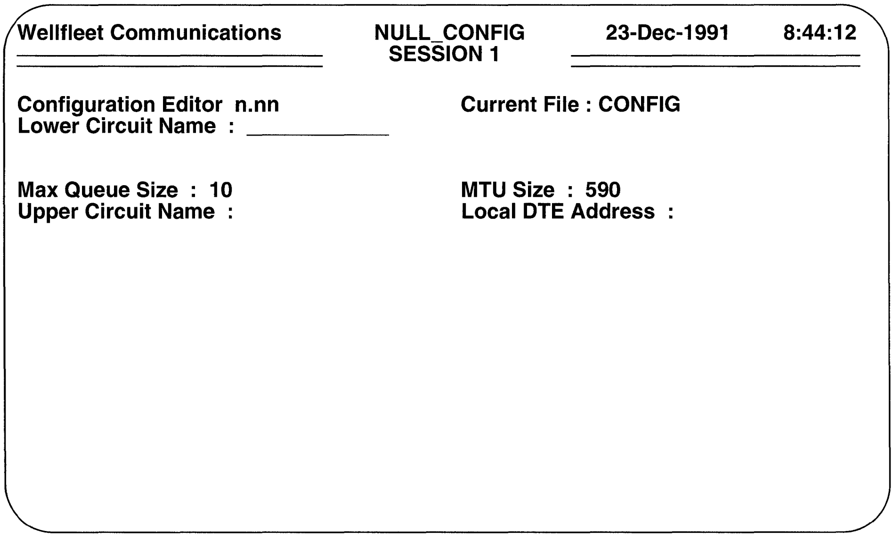
- ❐ **Max Queue Size** specifies the maximum size (in packets) of the transmit queue of each individual X.25 PDN switched virtual circuit. If the value specified by **Max Queue Size** is exceeded, the router "clips" (discards) the oldest packet(s) in the transmit queue.

  Enter a decimal value from `1` to `99`, then press `[RETURN]`. To avoid queue "clipping", enter a value of 0, and then press `[RETURN]`.



```
Wellfleet Communications         NULL_CONFIG        23-Dec-1991     8:44:12
                                  SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Auto Enable  :  <xxx>


1. PDN Service (0)
2. DDN Service (0)
3. Wellfleet Point to Point (0)


Enter Selection (0 for Previous Menu)  :  __
```

Figure 6-4 X.25 Service Selection Screen



```
Wellfleet Communications         NULL_CONFIG        23-Dec-1991     8:44:12
                                  SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Lower Circuit Name  :  ____________

Max Queue Size  :  10                          MTU Size  :  590
Upper Circuit Name  :                          Local DTE Address  :
```

Figure 6-5 X.25 PDN Service Parameters Screen

- ❒ **MTU Size** specifies the maximum number of bytes in the information field of an X.25 PDN level-3 packet.

  This PDN-specific parameter allows you to tailor the packet length set by LAPB circuit **Pkt Size** parameter. It facilitates X.25 PDN service if the remote end of the virtual circuit requires a specific information field length.

  Allowable values are in the range up to 1600 bytes (the largest packet sent by an upper level redirecting protocol to X.25 PDN). Should you enter a value greater the 1600, X.25 enforces the upper boundary limit.

  Press `[RETURN]` to accept the default of 590 bytes (providing for a 14 byte Ethernet header and 576 bytes of data), or enter another value (up to a maximum of 1600) and then press `[RETURN]`.

NOTE

Ensure that the value you enter at **MTU Size** is equal to or less than the value specified at **Pkt Size**.

- ❒ **Upper Circuit Name** identifies a "software circuit" or "pipe" that provides the interface between a protocol suite (in this case, TCP/IP) and X.25 packet-level services.

  Conceptually, X.25 PDN service can be illustrated as shown in Figure 6-6.

  The upper circuit provides an interface between the IP routing protocol and X.25 network services. The lower (LAPB) circuit, in contrast, provides an interface (via a device driver) between X.25 network services and the X.25 service provider.

  Enter the unique upper circuit name, then press `[RETURN]`.

  You will use **Upper Circuit Name** when you build circuit groups and when you configure the IP Router for X.25 PDN service.

- ❒ **Local DTE Address** is a network-supplied decimal number (X.121 Address) that identifies the interface between the router and the X.25 network.

  Enter this address and press `[RETURN]`.

After you specify the local DTE address, the screen prompts for X.25 address map data (Figure 6-7).

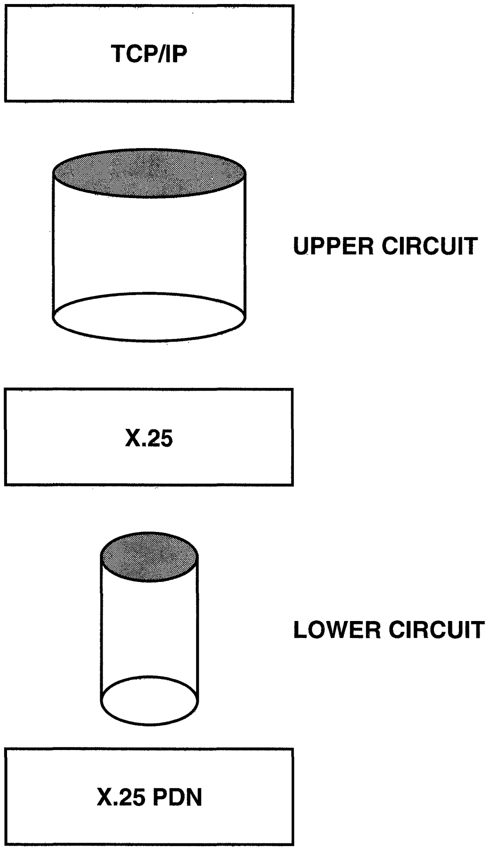
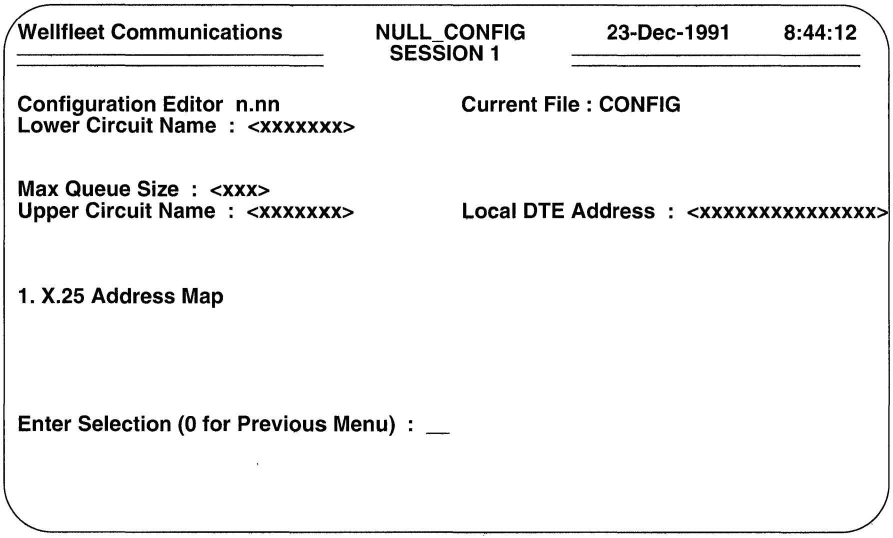


Figure 6-6 X.25 PDN Service Block Diagram



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Lower Circuit Name  :  <xxxxxxx>

Max Queue Size  :  <xxx>
Upper Circuit Name  :  <xxxxxxx>              Local DTE Address  :  <xxxxxxxxxxxxxxx>

1. X.25 Address Map

Enter Selection (0 for Previous Menu)  :  __
```

Figure 6-7 X.25 PDN Address Map Access Screen

6.2.1.1 X.25 PDN Address Map

The X.25 PDN Address Map consists of a series of address pairs. Each pair associates a destination X.121 address with a 32-bit TCP/IP address. The address map can contain up to 256 address pairs.

You begin address mapping from the X.25 PDN Address Map Access Screen. Enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen prompts:

No X.25 Address Map record(s) found
Do you wish to add X.25 Address Map record(s)?

Press `[RETURN]` to display the X.25 Address Map Data Screen (Figure 6-8).

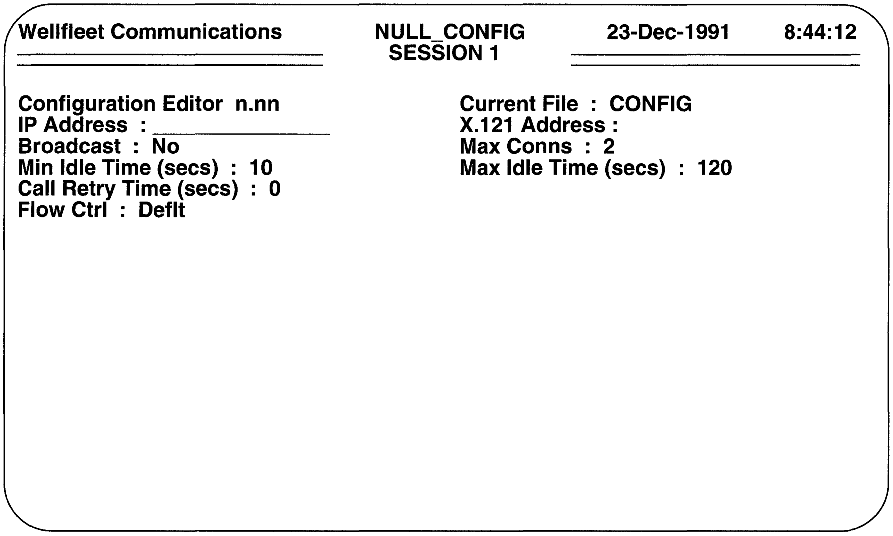
❒ **IP Address** identifies a recipient of IP datagrams transmitted by the X.25 PDN service.

Enter the 32-bit IP address in dotted decimal notation.

❒ **X.121 Address** is the X.121 address that corresponds to **IP Address**.

Enter the X.121 address.

❒ **Broadcast** identifies **IP Address** as a possible recipient of broadcast messages.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File  :  CONFIG
IP Address  : ______________                    X.121 Address :
Broadcast  :  No                                Max Conns  :  2
Min Idle Time (secs)  :  10                     Max Idle Time (secs)  :  120
Call Retry Time (secs)  :  0
Flow Ctrl  :  Deflt
```

Figure 6-8 X.25 PDN Address Map Data Screen

With **Broadcast** set to **Yes**, X.25 sends broadcast messages to **IP Address**. With **Broadcast** set to **No**, theX.25 makes no effort to send broadcast messages to **IP Address**.

□ **Max Conns** specifies the maximum number of connections that can be simultaneously established with **IP Address**.

The X.25 PDN service clears any incoming calls that would exceed this limit. Similarly, the X.25 PDN service makes no attempt to place outgoing calls that would exceed this limit. The establishment of multiple connections with a single destination may improve throughput by increasing the window size.

Use the `[RIGHTARROW]` to select from the available options (**1**, **2**, **3**, or **4**), then press `[RETURN]`.

□ **Min Idle Time (secs)** specifies the minimum period of circuit inactivity (no IP datagrams sent to or received from **IP Address**) before a circuit can be cleared and reused for a call to another destination.

A value of 0 (implying an infinite idle time) prevents a connection to IP Address from ever being cleared once such a connection is established. Enter the minimum idle time value and then press `[RETURN]`, or simply press `[RETURN]` to accept the default value of **10** seconds.

- ❒ **Max Idle Time (secs)** specifies the maximum period that a circuit can remain idle.

  After the expiration of max idle timer, the router clears the circuit. This parameter is intended to minimize CPU and network overhead during periods of low datagram traffic. If **Min Idle Time (secs)** is set to 0, this parameter is ignored.

  Enter the maximum idle time value and then press `[RETURN]`.

NOTE

If the IP router uses the Routing Information Protocol (RIP), you should set the **Max Idle Time** parameter to a value greater than 30 seconds (the RIP update period) to prevent call/clear thrashing.

- ❒ **Call Retry Timer (secs)** specifies the interval between *Call Request* packets to a specific destination. In the event of an unsuccessful call attempt (for example, the *call request* is cleared), the router waits **Call Retry Timer (secs)** before sending another call request to the destination. Any IP datagrams received for the destination during this period are dropped by the router.

  This timer is activated in the event of an failed call attempt and prevents a potential "thrashing" situation that may occur when the IP router directs a stream of datagrams to a busy or unreachable destination. With the timer enabled (set at a non-zero value), the X.25 PDN service drops received datagrams and transmits another *Call Request* at the expiration of the timer. With the timer disabled (set to 0), the X.25 PDN service sends *Call Request* packets for every datagram received from the IP router.

- ❒ **Flow Ctrl** enables or disables Flow Control Parameter Negotiation on a per destination (switched virtual circuit) basis.

  Deflt uses the previously configured LAPB values for **Pkt Window** and **Pkt Size** for all transfers across the switched virtual circuit.

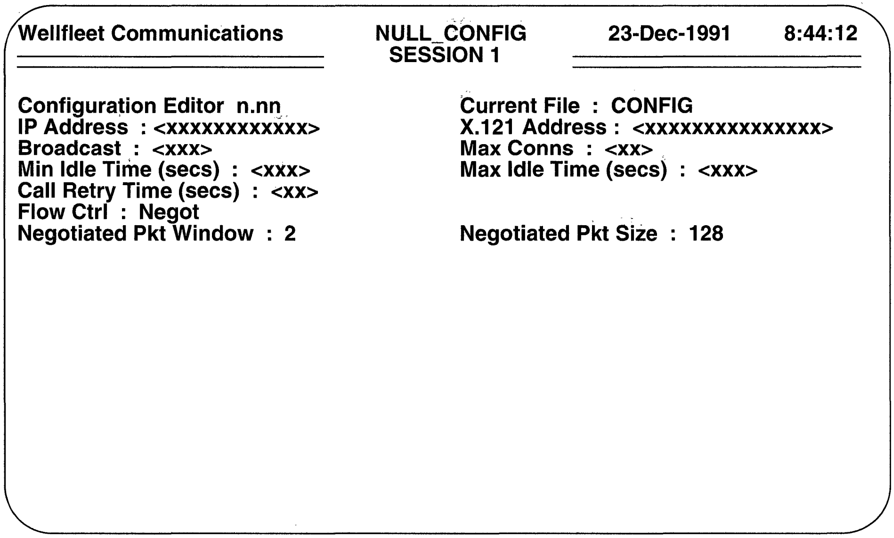
NOTE

If you disable SVC-specific flow control, you must ensure that (1) the X.25 switching device (DCE) to which this circuit connects has also disabled flow control, and (2) the values you select for **Pkt Window** and **Pkt Size** match those of the DCE. Additionally, you must also ensure that the remote DTE has also disabled negotiation and that its assigned values for **Pkt Window** and **Pkt Size** match those of the router.

Negot enables negotiation. With flow control enabled, the window and packet size are negotiated on a per destination (switched virtual circuit) basis.

If you disable flow control the screen prompts **Hit Return to Continue**. Press [**RETURN**] to go back to the X.25 PDN Address Map Access Screen. Now proceed to Section 6.3.1.2.

If you enable flow control, the screen displays the X.25 PDN Flow Control Parameter Negotiation Screen.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                 Current File  :  CONFIG
IP Address  : <xxxxxxxxxxxx>               X.121 Address : <xxxxxxxxxxxxxxx>
Broadcast  :  <xxx>                        Max Conns  :  <xx>
Min Idle Time (secs)  :  <xxx>             Max Idle Time (secs)  :  <xxx>
Call Retry Time (secs)  :  <xx>
Flow Ctrl  :  Negot
Negotiated Pkt Window  :  2                Negotiated Pkt Size  :  128
```

Figure 6-9 X.25 PDN Flow Control Parameter Negotiation Screen

NOTE

If you enable Flow Control Parameter Negotiation (**Flow Ctrl** equals **Negot**), you can maximize virtual circuit efficiency by ensuring that the remote DTE has also enabled negotiation and that its assigned values for **Negotiated Pkt Window** and **Negotiated Pkt Size** match those of the local DTE. In such an instance the negotiation proceeds as follows: (1) the calling system issues a *Call Request* packet that specifies Flow Control Parameter Negotiation and includes the values for **Negotiated Pkt Window** and **Negotiated Pkt Size** in the facilities field of the packet; (2) the called system performs simple boundary checking to verify that the negotiated parameters are within acceptable ranges and issues a *Call Confirm* packet.

❐ **Negotiated Pkt Window** specifies the window size that appears in the facilities field of *Call Request* packets originated on the PDN **Circuit Name**.

Select a value from **1** through **7**.

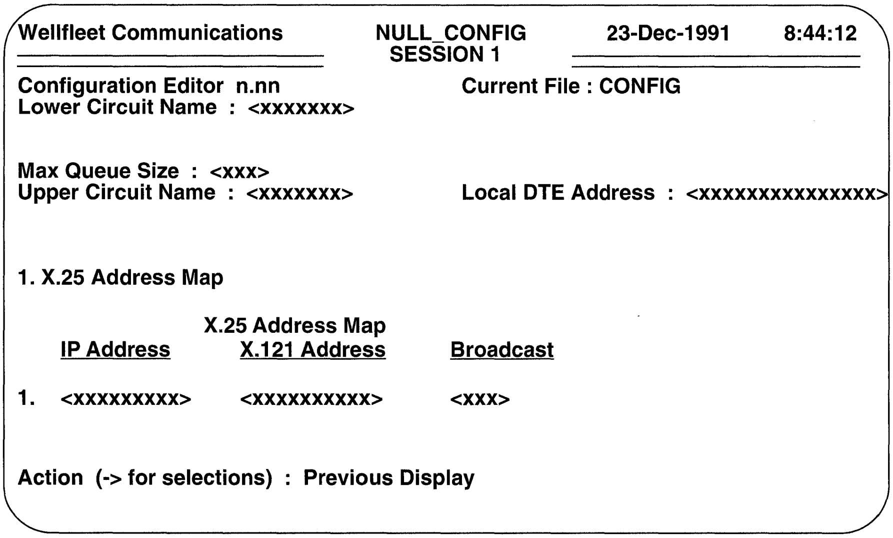
- ❒ **Negotiated Pkt Size** specifies the packet size that appears in the facilities field of *Call Request* packets originated on PDN **Circuit Name**.

  Select a value from `16` through **2048**, keeping in mind that while the X.25 service will negotiate a packet size of 2048 octets the actual maximum packet size is 1600 octets.

NOTE

X.25 PDN service supports *Throughput Negotiation* (with an initial value of 48,000 bits per second) on incoming calls. *Throughput Negotiation* is not initiated on outgoing calls.

The screen prompts **Hit Return to Continue**. After you do so, the screen displays the X.25 PDN Address Map Access Screen. You use this screen to add additional entries to the X.25 PDN Address Map. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the X.25 Address Map Summary Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Lower Circuit Name  :  <xxxxxxx>


Max Queue Size  :  <xxx>
Upper Circuit Name  :  <xxxxxxx>              Local DTE Address  :  <xxxxxxxxxxxxxxx>


1. X.25 Address Map

                   X.25 Address Map
   IP Address        X.121 Address        Broadcast

1. <xxxxxxxxx>      <xxxxxxxxxx>          <xxx>


Action  (-> for selections)  :  Previous Display
```

Figure 6-10 X.25 Address Map Summary Screen

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the X.25 Address Map Data Screen. Now follow the same procedure as you did before to add another entry to the address map. Continue this procedure, until you have completed the address map.

6.2.1.2 X.25 PDN Virtual Circuits

It is not necessary to explicitly configure X.25 PDN virtual circuits. The X.25 PDN service dynamically establishes such circuits on an as-needed basis. Circuit establishment is triggered by the receipt of a datagram from the IP Router. After the X.25 PDN service receives a datagram, it first determines if there is an established switched virtual-circuit connection(s) with the next-hop IP destination. If a single established connection is found and if the circuit's transmit queue is empty, the datagram is queued on the virtual circuit for subsequent transmission. In the event of multiple established virtual-circuit connections (none of which possess an empty transmit queue), the datagram is directed to the circuit with the shortest transmit queue.

In the absence of currently established switched virtual circuit connections to the next-hop destination, X.25 establishes a call to the next-hop destination, and then queues the datagram on the newly-established call. If resource limitations (for example, all switched virtual circuits are busy) prevent call establishment, X.25 drops the datagram.

All incoming calls are accepted (resources permitting). All received datagrams are forwarded to the IP Router.

6.2.1.3 IP Router Configuration

Establishing X.25 PDN service requires that you define an IP network interface for each X.25 PDN circuit group. When configuring the IP network interface, use Table 6-3 to supply required parameter values. Other parameter values are unrestricted.

Table 6-3: TCP/IP Parameters (X.25 PDN Service)

Network Interface Parameter	Required Value
Circuit Group	Upper Circuit Name
Address Resolution	PDN
Normal ARP	No
Proxy ARP	No
Address Mask Reply	No
MTU Discovery Option	No

6.2.2 Configuring X.25 DDN Service

X.25 DDN service provides access to the Defense Data Network. Such access enables the IP Router to use the DDN's packet switching facilities, specifically "DDN Standard Service" to transfer IP datagrams to a remote host or gateway (note that the remote host or gateway need not be a peer router).

You configure X.25 DDN service from the Configuration Menu. Enter the number that appears to the left of **X.25 Network Service** at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No X.25 Network Service record(s) found
Do you wish to add X.25 Network Service record(s)?

Press `[RETURN]` to display the X.25 Auto Enable Screen.

❒ **Auto Enable** specifies the initial state of X.25 services.

This X.25-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable X.25 services when the router boots.

When global auto is **No**, X.25 services are unconditionally disabled. You will later need to enable X.25 services with NCL commands after the router boots.

When global auto enable is **Yes**, X.25 services are conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable X.25 services) or **No** (disable X.25 services), then press `[RETURN]`. If you select **No**, you will later need to enable X.25 services with NCL commands after the router boots.

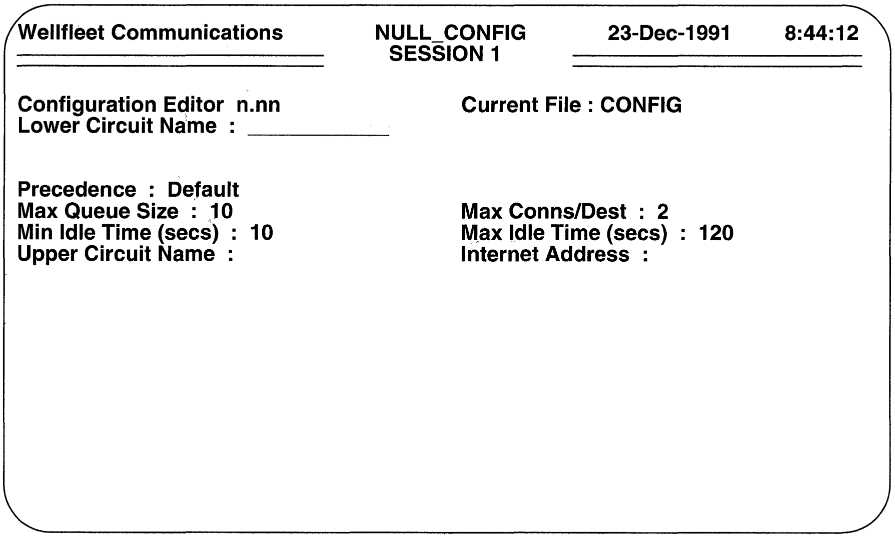
After you specify the initialization state, the screen displays the X.25 Service Selection Screen. With the cursor at **Enter Selection (0 for Previous Display)**, enter `<2>` to configure X.25 DDN service. After you do so, the screen displays the X.25 DDN Service Parameters Screen (Figure 6-11).

❒ **Lower Circuit Name** identifies the LAPB circuit that provides the network interface.

Enter the name of the previously configured LAPB circuit.

❒ **Precedence** enables or disables a request for "Level 0" precedence.

The default response, **Deflt**, disables precedence requests. **Negot** enables a request for "Level 0" precedence in all outgoing calls. Use the `[RIGHTARROW]` to enable or disable precedence requests, then press `[RETURN]`.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Lower Circuit Name  :  ____________

Precedence  :  Default
Max Queue Size  :  10                        Max Conns/Dest  :  2
Min Idle Time (secs)  :  10                  Max Idle Time (secs)  :  120
Upper Circuit Name  :                        Internet Address  :
```

Figure 6-11 X.25 PDN Service Parameters Screen

- ❐ **Max Queue Size** specifies the maximum size (in packets) of the transmit queue of each individual X.25 DDN virtual circuit.

  If the value specified by **Max Queue Size** is exceeded, X.25 "clips" (discards) the oldest packet(s) in the transmit queue.

  To specify the queue size, enter a decimal value from 1 to 999, then press `[RETURN]`. To avoid queue "clipping", enter a value of 0, and then press `[RETURN]`.

- ❐ **Max Conns/Dest** specifies the maximum number of connections that can be simultaneously established with a single destination host or gateway.

  The X.25 DDN service clears any incoming calls that would exceed this limit. Similarly, the X.25 DDN service makes no attempt to place outgoing calls that would exceed this limit. The establishment of multiple connections with a single destination may improve throughput by increasing the window size.

  Use the `[RIGHTARROW]` to select from the available options (**1**, **2**, **3**, or **4**), then press `[RETURN]`.

- ❐ **Min Idle Time (secs)** specifies the minimum period of circuit inactivity (no IP datagrams sent or received) before a circuit can be cleared and reused for a call to another destination.

A value of 0 (implying an infinite idle time) prevents logical connections from ever being cleared once such a connection is established. Enter the minimum idle time value and then press `[RETURN]`, or simply press `[RETURN]` to accept the default value of **10** seconds.

- ❐ **Max Idle Time (secs)** specifies the maximum period that a circuit can remain idle.

  After the expiration of max idle timer, X.25 clears the circuit. This parameter is intended to minimize CPU and network overhead during periods of low datagram traffic. If **Min Idle Time (secs)** is set to 0, this parameter is ignored.

  Enter the maximum idle time value and then press `[RETURN]`, or simply press `[RETURN]` to accept the default value of **120** seconds.

- ❐ **Upper Circuit Name** identifies a "software circuit" or "pipe" that provides the interface between a protocol suite (in this case, TCP/IP) and X.25 packet-level services.

  Conceptually, X.25 DDN service can be illustrated as shown in Figure 6-12.

  The upper circuit provides an interface between the IP routing protocol and X.25 network services. The lower (LAPB) circuit, in contrast, provides an interface (via a device driver) between X.25 network services and the X.25 service provider (the DDN).

  Enter the unique upper circuit name, then press `[RETURN]`.

  You will use **Upper Circuit Name** when you build circuit groups and when you configure the IP Router for X.25 PDN service.

- ❐ **Internet Address** specifies the 32-bit IP address of **Upper Circuit Name**.

  Enter this address in dotted decimal notation, then press `[RETURN]`. The DDN algorithm will map this IP address to a X.121 address.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Configuration Menu.

6.2.2.1 X.25 DDN Virtual Circuits

It is not necessary to explicitly configure X.25 DDN virtual circuits. The X.25 DDN software dynamically establishes such circuits on an as-needed basis. Virtual circuit establishment is triggered by the receipt of a DDN-destined datagram from the IP Router software. After X.25 receives a datagram, it first determines if there is an established virtual-circuit connection(s) with the next-hop IP destination. If a single established connection is found and if the circuit's transmit queue is empty, the datagram is queued on the virtual circuit for subsequent transmission. In the event of multiple established virtual-circuit connections (none of which possess an empty transmit queue), the datagram is directed to the circuit with the shortest transmit queue.

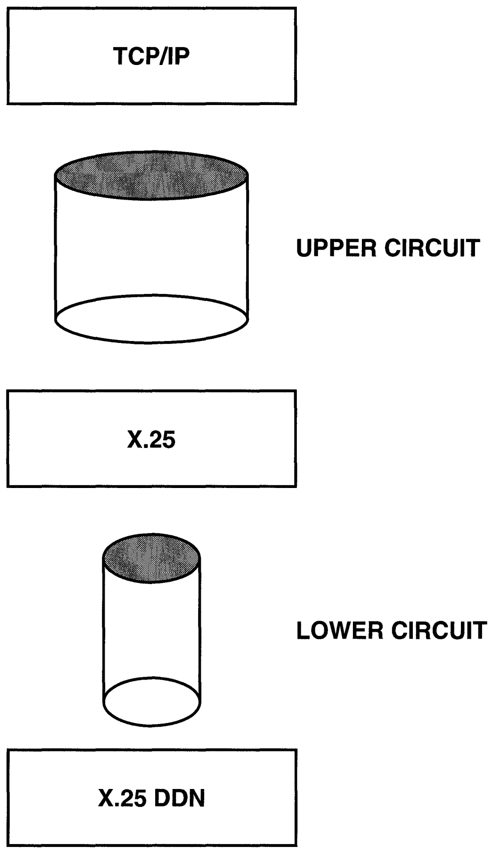


Figure 6-12 X.25 DDN Service Block Diagram

In the absence of currently established virtual-circuit connections to the next-hop destination, X.25 establishes a call to the next-hop destination, and then queues the datagram on the newly-established call. If resource limitations (e.g., all switched virtual circuits are busy) prevent call establishment, X.25 drops the datagram.

All incoming calls are accepted (resources permitting). All received datagrams are forwarded to the IP Router.

6.2.2.2 IP Router Configuration

Establishing X.25 DDN service requires that you define an IP network interface for each circuit group that contains an X.25 DDN circuit. When configuring the network interface, use Table 6-4 to supply required parameter values. Other parameter values are unrestricted. You must also either: (1) configure the Exterior Gateway Protocol, or (2) specify a default route for the X.25 DDN interface.

Table 6-4: TCP/IP Configuration (X.25 DDN Service)

Network Interface Parameter	Required Value
Internet Address	Internet Address
Circuit Group	Upper Circuit Name
Address Resolution	DDN
Normal ARP	No
Proxy ARP	No
RIP Supply	No
RIP Listen	No
Default Route Supply	No
Default Route Listen	No
Address Mask Reply	No
MTU Discovery Option	No

6.2.3 Configuring X.25 Point-to-Point Service

X.25 Point-to-Point service provides end-to-end connectivity between a local multiprotocol router and a remote peer through an intervening public data network. Such connectivity is provided by "dedicated" switched virtual circuits. Table 6-5 distinguishes between virtual circuit types.

You configure X.25 Point-to-Point service from the Configuration Menu. Enter the number that appears to the left of **X.25 Network Service** at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

```
No X.25 Network Service record(s) found
Do you wish to add X.25 Network Service record(s)?
```

Press `[RETURN]` to display the X.25 Auto Enable Screen.

Table 6-5: Virtual Circuit Types

Virtual Circuit Type	Description
Switched Virtual Circuit (SVC) (used by PDN and DDN service)	An SVC is a temporary association between two DTEs established by the transmission of a call request packet. The calling DTE receives a response indicating whether or not the called DTE wishes to accept the call. After SVC establishment either DTE can clear the call, after which the SVC no longer exists.
Permanent Virtual Circuits (PVC) (not used)	A PVC is a permanent association between two DTEs established when subscribing to the X.25 service. The X.25 provider allocates resources to this circuit for the subscription duration. A PVC requires no call set-up or call clearing by the user.
Dedicated Virtual Circuits (DVC) (used by Wellfleet point-to-point service only)	A DVC is established during the router initialization process and remain permanently available unless taken out of service with the NCLDISABLE command.Calls are established by the exchange of a call request packet (issued by the router with the higher X.121 address) and a call confirm packet (issued by the router with the lower X.121 address).

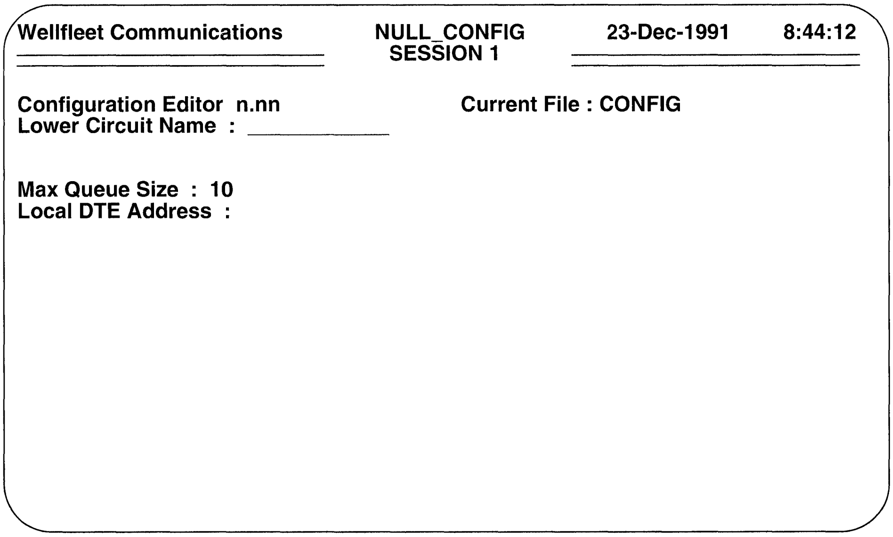
❒ **Auto Enable** specifies the initial state of X.25 services.

This X.25-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable X.25 services when the router boots.

When global auto enable is **No**, X.25 services are unconditionally disabled. You will later need to enable X.25 services with NCL commands after the router boots.

When global auto enable is **Yes**, X.25 services are conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable X.25 services) or **No** (disable X.25 services), then press `[RETURN]`. If you select **No**, you will later need to enable X.25 services with NCL commands after the router boots.

After you specify the initialization state, the screen displays the X.25 Service Selection Screen. Enter **<3>** to configure X.25 Point-to-Point service. After you do so, the screen displays the X.25 Point-to-Point Service Parameters Screen (Figure 6-13).



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Lower Circuit Name  : ___________


Max Queue Size  :  10
Local DTE Address  :
```

Figure 6-13 X.25 PDN Service Parameters Screen

- **Lower Circuit Name** identifies the LAPB circuit that provides the network interface.

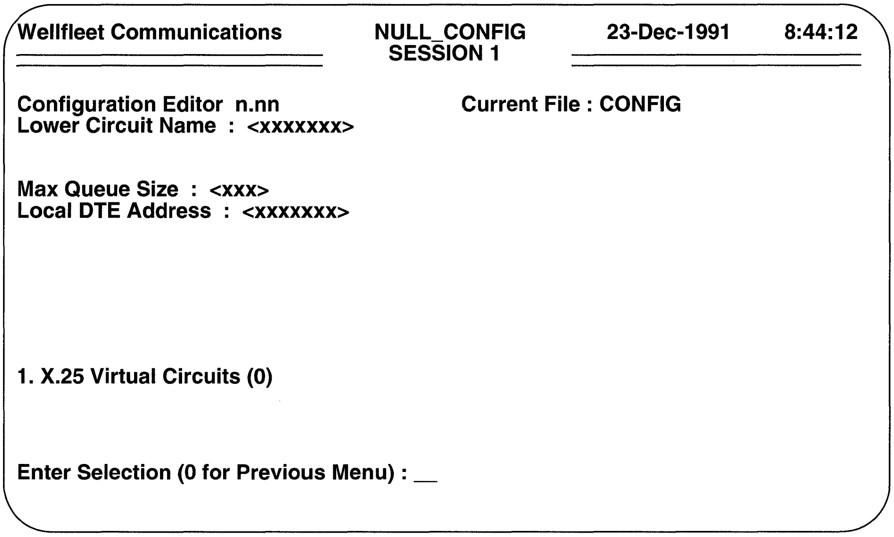
  Enter the name of the previously configured LAPB circuit.

- **Max Queue Size** specifies the maximum size (in packets) of the transmit queue of each individual X.25 Point-to-Point switched virtual circuit. If the value specified by **Max Queue Size** is exceeded, the router “clips” (discards) the oldest packet(s) in the transmit queue.

  Enter a decimal value from `1` to `99`, then press `[RETURN]`. To avoid queue “clipping”, enter a value of 0, and then press `[RETURN]`.

- **Local DTE Address** is a network-supplied decimal number (X.121 Address) that identifies the interface between the router and the X.25 network.

  Enter this number and press `[RETURN]`. The screen displays the X.25 Virtual Circuit Access Screen (Figure 6-14) to prompt for dedicated virtual circuit information.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Lower Circuit Name  :  <xxxxxxx>


Max Queue Size  :  <xxx>
Local DTE Address  :  <xxxxxxx>






1. X.25 Virtual Circuits (0)



Enter Selection (0 for Previous Menu) : __
```

Figure 6-14 X.25 Virtual Circuits Access Screen

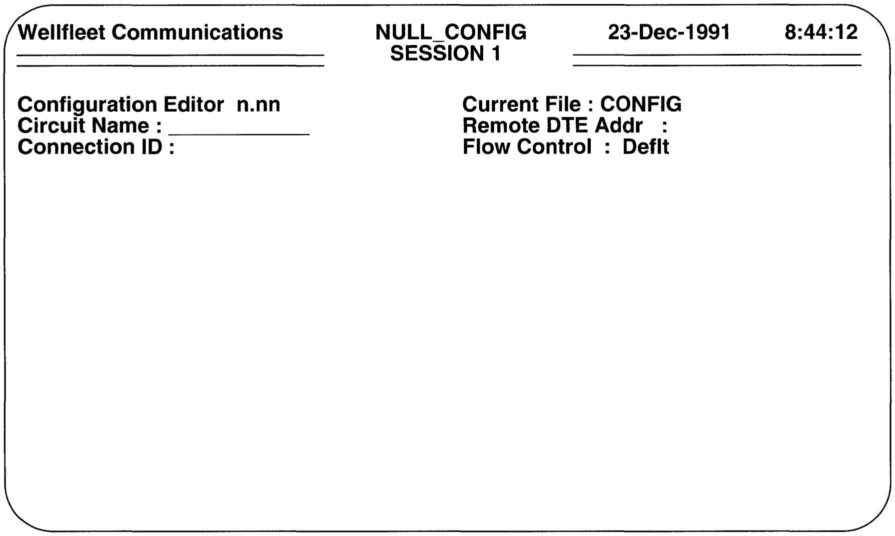
X.25 point-to-point service operates by establishing dedicated switched virtual circuits between the local Wellfleet router and a remote peer. These circuits are established during the router initialization process and remain permanently available unless taken out of service with the NCL DISABLE command. Calls are established by the exchange of a *call request* packet (issued by the router with the higher X.121 address) and a *call confirm* packet (issued by the router with the lower X.121 address).

Each LAPB circuit supports up to 32 dedicated virtual circuits.You may wish to use the *X.25 Virtual Circuit Summary Chart* (contained in Appendix C) to maintain a record of X.25 dedicated virtual-circuit parameters.

You configure a dedicated virtual circuit from the X.25 Virtual Circuits Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

```
No X.25 Virtual Circuits record(s) found
Do you wish to add X.25 Virtual Circuits record(s)?
```

Press `[RETURN]` to display the X.25 Virtual Circuit Parameters Screen (Figure 6-15).



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Circuit Name : ___________                     Remote DTE Addr   :
Connection ID :                                Flow Control  :  Deflt
```

Figure 6-15 X.25 Virtual Circuit Parameters Screen

□ **Circuit Name** identifies the dedicated virtual circuit.

Virtual circuits are named under the same conventions as are all other circuit types. Because you use virtual circuit names to configure application software modules, it is very important that you maintain an accurate record of virtual circuit names.

Enter the name of the dedicated virtual circuit, then press `[RETURN]`.

□ **Remote DTE Address** specifies the network-supplied decimal number (X.121 Address) that identifies the interface between the remote Wellfleet peer and the X.25 network.

Enter the X.121 address and press `[RETURN]`.

□ **Connection ID** enables the establishment of multiple, parallel dedicated virtual circuits between two routers. Such parallel circuits may result in higher throughput, because of the increased window size afforded by multiple virtual circuits.

If you are establishing only one dedicated virtual circuit between the local router and the remote peer designated by **Remote DTE Address**, enter `<1>`, and then press `[RETURN]`. When configuring the remote peer, you must ensure that you also assign a **Connection ID** of 1.

If you are establishing multiple dedicated virtual circuits between the local and remote peers, you must assign a unique **Connection ID** to each virtual circuit. When configuring the remote peer, you must ensure that you assign identical **Connection ID** values. Enter a decimal value in the range `1` through `99`, then press `[RETURN]`.

❒ **Flow Ctrl** enables or disables Flow Control Parameter Negotiation for the dedicated virtual circuit.

Flow Control Parameter Negotiation is available as a subscription option from most X.25 service providers. The default response, **Deflt**, disables negotiation in *call request* packets. With negotiation disabled, the configured LAPB values for **Pkt Window** and **Pkt Size** serve as the defaults across the dedicated virtual circuit. If you disable flow control, you must ensure that the X.25 switching device (DCE) to which this circuit connects has also disabled flow control. Additionally, you must ensure that the values you select for **Pkt Window** and **Pkt Size** match those of the DCE.

Negot enables negotiation. With flow control enabled, the window and packet size are negotiated on a dedicated virtual circuit basis.

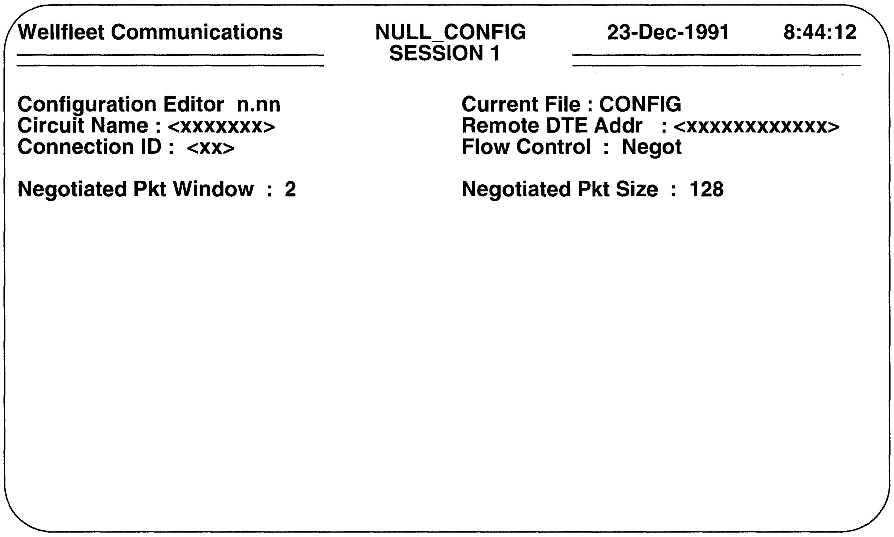
Use the `[RIGHTARROW]` to enable (**Negot**) or disable (**Deflt**) Flow Control Parameter Negotiation, and then press `[RETURN]`.

NOTE

If you disable Flow Control Parameter Negotiation (**Flow Ctrl** equals **Deflt**), you should ensure that the remote DTE has also disabled negotiation and that its assigned values for **Pkt Window** and **Pkt Size** match those of the local DTE.

If you disable Flow Control Parameter Negotiation, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the X.25 Virtual Circuit Access Screen .

If you enable Flow Control Parameter Negotiation, the screen displays the X.25 Point-to-Point Flow Control Parameter Negotiation Screen (Figure 6-16).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Circuit Name : <xxxxxxx>                      Remote DTE Addr  : <xxxxxxxxxxxx>
Connection ID :  <xx>                         Flow Control  :  Negot

Negotiated Pkt Window  :  2                   Negotiated Pkt Size  :  128
```

Figure 6-16 X.25 Point-to-Point Flow Control Parameter Negotiation Screen

NOTE

If you enable Flow Control Parameter Negotiation (**Flow Ctrl** equals **Negot**), you can maximize virtual circuit efficiency by ensuring that the remote DTE has also enabled negotiation and that its assigned values for **Negotiated Pkt Window** and **Negotiated Pkt Size** match those of the local DTE. In such an instance the negotiation proceeds as follows: (1) the peer with the higher X.121 address issues a *call request* packet that specifies Flow Control Parameter Negotiation and includes the values for **Negotiated Pkt Window** and **Negotiated Pkt Size** in the facilities field of the packet; (2) the called peer (the one with the lower X.121 address) performs simple boundary checking to verify that the negotiated parameters are within acceptable ranges and issues a *call confirm* packet.

❒ **Negotiated Pkt Window** specifies the window size that appears in the facilities field of *Call Request* packets originated on **Circuit Name**.

Use the `[RIGHTARROW]` to select a value from **1** through **7**, then press `[RETURN]`.

❒ **Negotiated Pkt Size** specifies the packet size that appears in the facilities field of *Call Request* packets originated on **Circuit Name**.

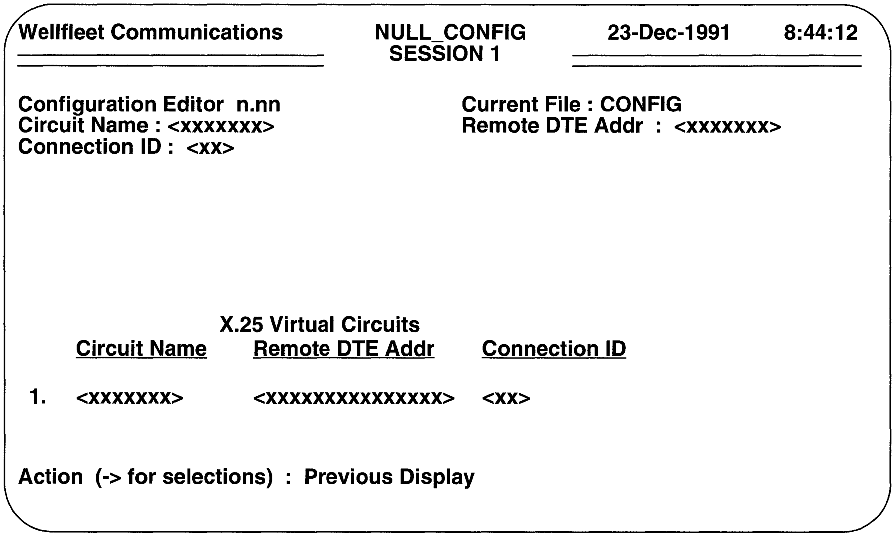
Use the `[RIGHTARROW]` to select a value from `128` through **2048**, then press `[RETURN]`.

NOTE

X.25 point-to-point service supports *Throughput Negotiation* (with an initial value of 48,000 bits per second) on incoming calls. *Throughput Negotiation* is not initiated on outgoing calls.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the X.25 Virtual Circuit Access Screen.

You configure additional dedicated virtual circuits from the X.25 Virtual Circuits Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the X.25 Virtual Circuits Summary Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Name : <xxxxxxx>                    Remote DTE Addr  :  <xxxxxxx>
Connection ID :  <xx>



                        X.25 Virtual Circuits
      Circuit Name       Remote DTE Addr        Connection ID

  1.  <xxxxxxx>          <xxxxxxxxxxxxxxx>      <xx>

Action  (-> for selections)  :  Previous Display
```

Figure 6-17 X.25 Virtual Circuits Summary Screen

With the cursor at **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the X.25 Virtual Circuit Parameters Screen . Now follow the same procedure as before to configure an additional X.25 dedicated virtual circuit; repeat this procedure until you have configured all virtual circuits.

7 Building Circuit Groups

This chapter tells you how to build circuit groups.

After you have established lines and defined individual circuits, you complete communications channels between the multiprotocol router and network devices by building *circuit groups*. Circuit groups are collections of circuits used by the application modules to bridge and route packets. A circuit group comprises circuits of the same type (LAN, synchronous, T1, E1, PPP, SMDS, or Frame Relay) that originate at a common point and terminate at another common point.

Application modules either bridge or route traffic across circuit groups. Therefore, each individual circuit must be assigned to a circuit group (even if the circuit group consists of only a single circuit). Individual circuits, however, can be assigned to more than one circuit group.

Figure 7-1 illustrates the assignment of individual circuits to multiple circuit groups. Circuits A, B, C, and D belong to Circuit Group 1; circuits C and D also belong to Circuit Group 2; and circuits A and B belong to Circuit Group 3. The router balances the traffic flow across all circuits within a circuit group. Such balancing prevents one circuit from becoming overloaded (and possibly dropping packets) while other similar circuits providing unused bandwidth are available.

For specific information on building circuit groups for X.25 service, refer to Section 7.3.

7.1 Establishing a Circuit Group

Before building circuit groups, refer to the summary circuit charts in Appendix C. *Every LAN, synchronous, T1, E1, PPP, SMDS, or Frame Relay circuit listed on these charts must be assigned to a circuit group.*

You establish circuit groups from the Configuration Menu. Enter `<5>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Circuit Groups record(s) found
Do you wish to add Circuit Groups record(s)?

Press `[RETURN]` to display the Circuit Group Screen (Figure 7-2). At **Circuit Group Name**, enter the circuit-group name (using a maximum of 12 alphanumeric characters) and press `[RETURN]` to display the Circuit Assignment Screen (Figure 7-3).

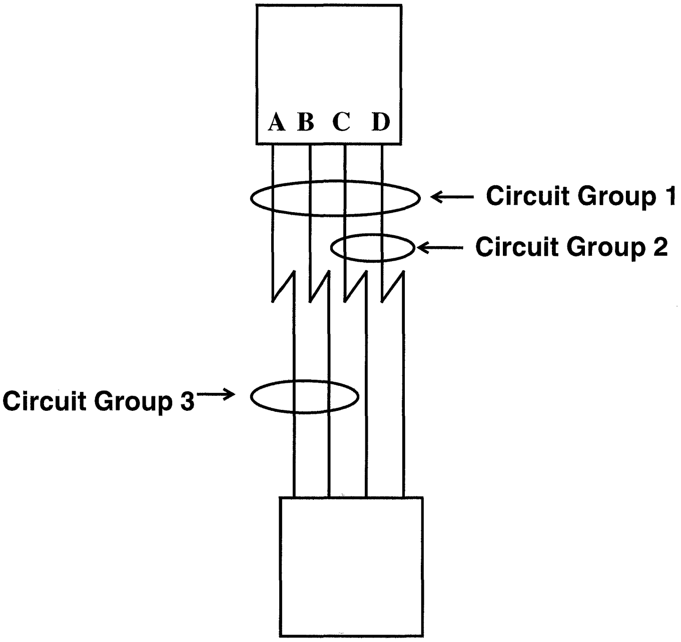


Figure 7-1 Multiple Circuit Group Assignment

7.2 Assigning Circuit Group Members

You assign circuit-group members from the Circuit Assignment Screen. Enter <1> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

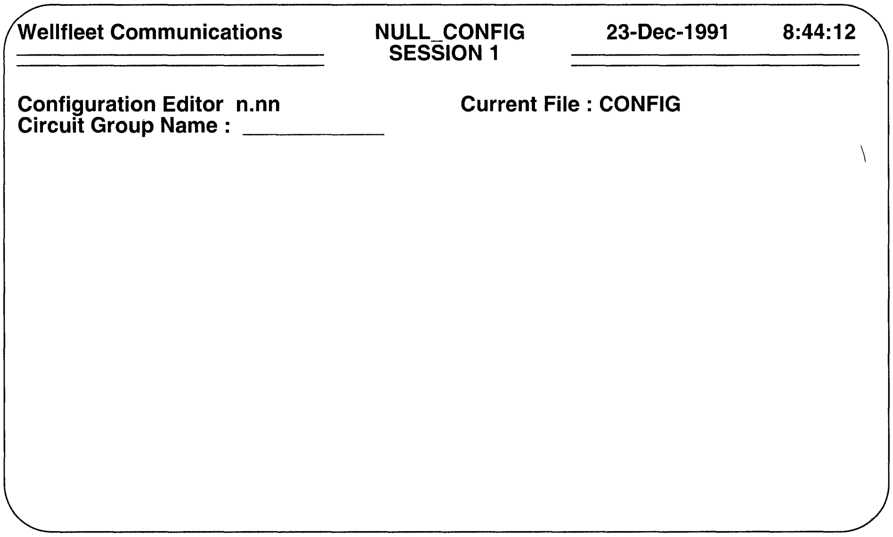
No Circuit Group Members record(s) found
Do you wish to add Circuit Group Members record(s)?

Press [RETURN]. The screen prompts for a **Circuit Name**.

At **Circuit Name** enter the name of the circuit that you wish to assign to this circuit group; then press [RETURN].

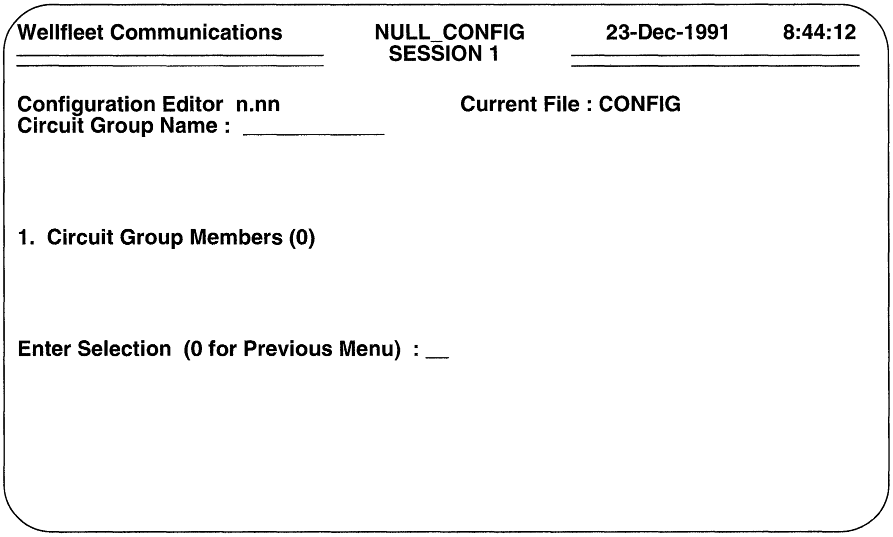
After the system prompts **Hit Return to Continue**, press [RETURN] to go back to the Circuit Assignment Screen.

To obtain a listing of circuit-group members, enter <1> at **Enter Selection (0 for Previous Menu)**. The screen displays the Circuit Group Members Screen (Figure 7-4). This screen lists the circuit-group name and each circuit assigned to the circuit group.



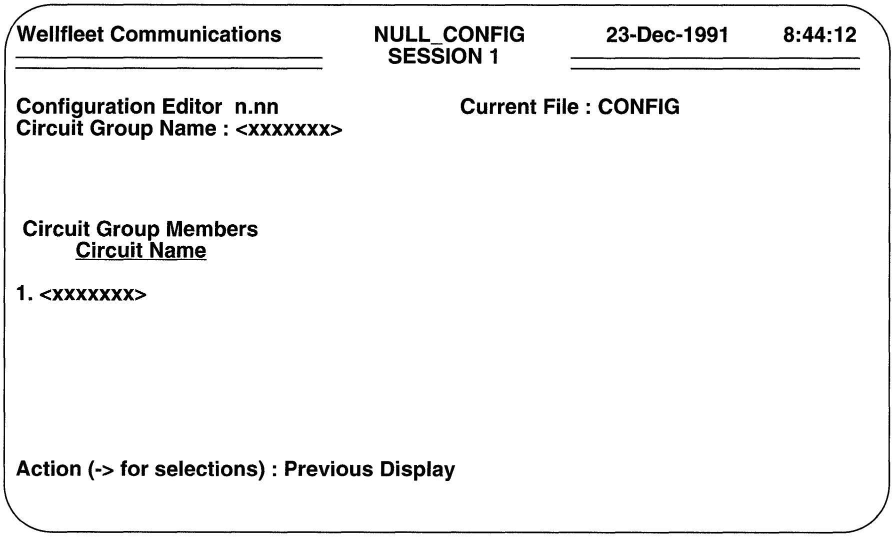
```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                    SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Circuit Group Name : ____________
```

Figure 7-2 Circuit Group Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                    SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Circuit Group Name : ____________



1.  Circuit Group Members (0)



Enter Selection  (0 for Previous Menu)  : __
```

Figure 7-3 Circuit Assignment Screen



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Circuit Group Name : <xxxxxxx>


 Circuit Group Members
      Circuit Name

1. <xxxxxxx>




Action (-> for selections) : Previous Display
```

Figure 7-4 Circuit Group Members Screen

You add members to a circuit group from the Circuit Group Members Screen. At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. When the screen prompts for **Circuit Name**, enter the name of another circuit (of the same type) that you wish to assign to this circuit group, then press `[RETURN]`. After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Circuit Assignment Screen. Follow this procedure until you have assigned all members to the circuit group.

7.3 Establishing an X.25 Circuit Group

While X.25 circuit groups are constructed in the same manner as other groups, the ability of a single LABP circuit to provide concurrent support for multiple X.25 service types, and the distinction between LAPB circuits, lower circuits, and upper circuits can be a source of confusion when building X.25 circuit groups. To clarify the establishment of X.25 circuit groups, refer to Figure 7-5 which shows a single LABP circuit providing simultaneous support for PDN and Wellfleet Point-to-Point service.

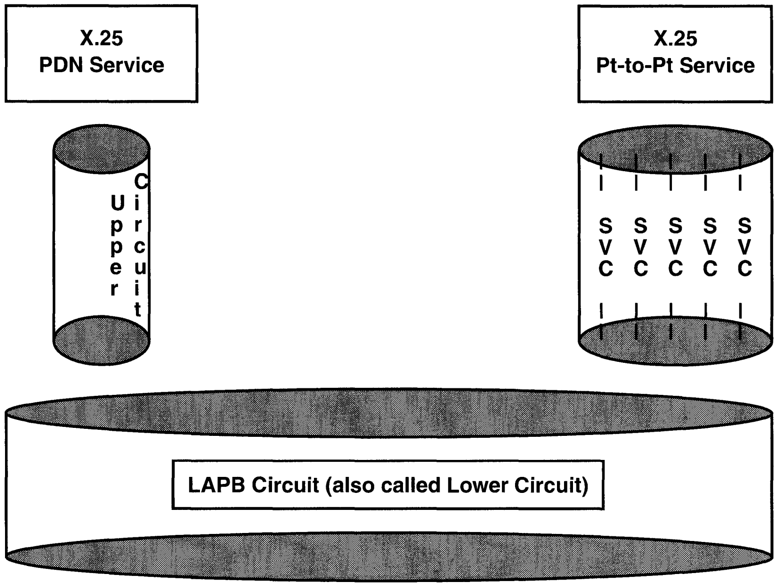
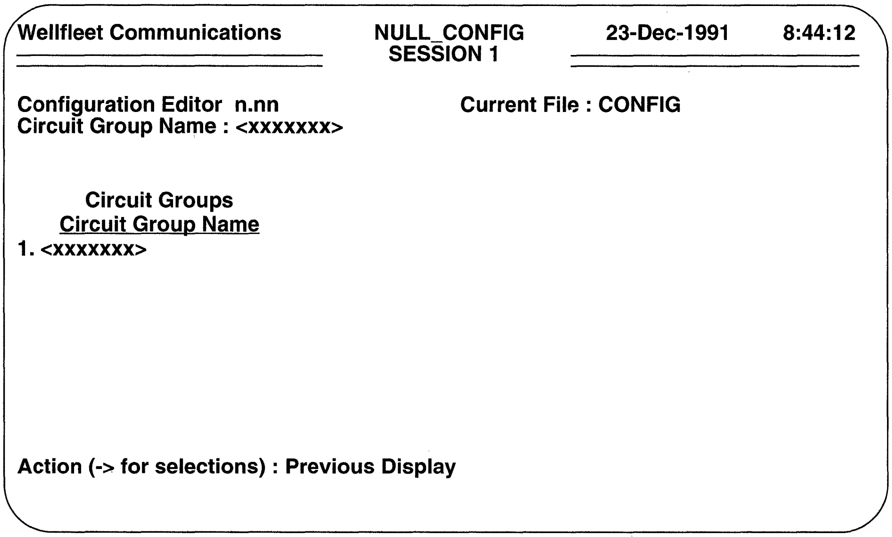


Figure 7-5 X.25 Circuit Groups

As shown in Figure 7-5, X.25 PDN service (as does X.25 DDN service) interfaces with the LABP circuit (which provides a network connection) through an upper circuit. X.25 Wellfleet Point-to-Point service interfaces with the LAPB connection through a series (up to 32) of switched virtual circuits. *X.25 circuit groups are established at the upper circuit and svc level.* Thus, with regard to the above figure, concurrent support for X.25 PDN and Point-to-Point service requires the establishment of two circuit groups, the first of which consists of the single upper circuit that provides a pipe between X.25 PDN and the LAPB network connection, and the second of which consists of the multiple switched virtual circuits that provide a pipe between X.25 Point-to-Point and the LAPB network connection.

7.4 Adding Circuit Groups

After building the initial circuit group, you add circuit groups from the Configuration Menu. Enter <5> at **Enter Selection (0 for Previous Menu)**. The screen displays the Circuit Groups Summary Screen.



```
Wellfleet Communications          NULL_CONFIG      23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Group Name : <xxxxxxx>


      Circuit Groups
    Circuit Group Name
1. <xxxxxxx>







Action (-> for selections) : Previous Display
```

Figure 7-6 Circuit Groups Summary Screen

To build an additional circuit group, press the `[RIGHTARROW]` at **Action (-> for selections)** to display **Add**, then press `[RETURN]`. The screen displays the Circuit Group Screen. Now follow the previously described proceduresto build an additional circuit group; repeat these procedures until you have built all circuit groups.

8 Configuring the Bridge

This chapter tells you how to configure the Source Routing/Transparent Bridge.

Bridges are data-link layer relay devices that use Media Access Control (MAC) source and destination addresses to relay frames between network and/or point-to-point connections. Bridges generally provide two types of service: t*ransparent bridging* and *source routing*.

8.1 Transparent Bridges

Transparent bridges provide network interconnection and/or extension services for LANs that employ identical protocols at the data-link and physical layers. Transparent bridges place no burden on end-stations. From the point of view of a LAN end-station, it appears that all end-stations are resident on a single extended network with each end-station identified by a unique MAC-level address.

Transparent bridges provide three primary services: they learn the addresses of end-stations on connected networks; they relay frames on the basis of acquired knowledge of end-station addresses; and they (in conjunction with the spanning tree algorithm) ensure a loop-free topology throughout the extended network.

Transparent bridges learn end-station addresses by observing the source address of each received frame. As bridges receive frames, they build and update a database (called the forwarding table) that lists each source address. Each source address table entry is accompanied by the circuit group on which the address was observed and by a timer value that indicates the age of the observation.

Transparent bridges relay frames on the basis of forwarding table entries. When they receive a frame, they compare the frame's destination address with addresses found in the forwarding table. In the absence of a match, they relay the frame on all circuit groups (except the circuit group on which the frame was received). This action of multicasting a frame is called flooding.

If a match is found between the destination address and a forwarding-table entry, transparent bridges compare the circuit group on which the frame was received with the circuit group associated with the table entry. Identical circuit groups indicate that the source and destination end-stations are located on the same network. In this instance, because relay is not necessary, the frame is dropped. Different circuit groups indicate that the source and destination are not located on the same network. In this instance, bridges relay the frame on the circuit group found in the forwarding table.

With the spanning tree algorithm enabled, transparent bridges ensure a loop-free network topology. The algorithm provides a single path (composed of bridges and intervening LANs) between any two end-stations.

8.2 Source Routing Bridges

The term source routing was coined by IBM to describe a method of bridging frames across token ring networks. Source routing differs from transparent bridging in two critical ways:

- ❐ Source routing bridges tolerate a multiplicity of paths between any two end-stations in the extended network; transparent bridges, in contrast, require a loop-free topology with a single path between source and destination.
- ❐ Source routing bridges require end-stations to supply the information needed to deliver a frame to its intended recipient. Consequently, within a source-routing network, bridges need not maintain forwarding tables. Rather they make the decision to forward or to drop a frame solely on the basis of routing information contained within the frame itself. To implement such a scheme each source end-station determines the route to a destination end-station through a process labeled route discovery. The route discovery process is enabled by four types of routing directives:

All paths broadcast routing:

Generates multiple frames that traverse all paths between source and destination end-stations. Such frames are called all-paths explorer (APE) frames. Upon receiving an APE frame, a bridge within the source routing network appends a routing designator which takes the following form:

[LAN$_i$] [Bridge_ID] [LAN$_j$]

where

LAN$_i$
is a unique number that identifies the LAN upon which the APE frame arrived

Bridge_ID
is a number that identifies the bridge

LAN$_j$
is a unique number that identifies the LAN upon which the APE frame is relayed by the bridge

After adding a routing designator, each bridge floods the frame. As a consequence, multiple copies of the same APE frame can appear on a LAN, and the frame recipient can receive multiple copies of the frame (one copy for each possible path through the extended network). Each APE frame received by the recipient contains a unique sequenced list of routing designators tracing the frame's path through the source routing network.

Spanning Tree broadcast routing:

Generates a single frame that follows a loop-free path from source to destination. Such frames are called transparent spanning frames (TSF). Upon receiving a TSF, each bridge on the spanning tree forwards the frame onto all active (non-blocked) ports save the port on which the frame was received. With Spanning Tree broadcast routing, one copy of the TSF appears on each LAN, and the frame recipient receives only a single copy of the frame.

Specific routing:

Generates a single frame that traverses a specific path designated by the source end-station. Such a frame is called a specifically routed frame (SRF). SRFs contain a list of routing designators that maps a path through the extended network from source to destination. Upon receiving an SRF, each bridge examines the list of routing designators. It forwards the SRF only if it is on the specified path, otherwise it ignores the frame.

Null routing:

Indicates that the source does not desire any routing services from network bridges. As a result null-routed frames are restricted to the resident LAN of the originating end-station.

Source routing networks consist of LAN segments interconnected by source routing bridges. Each LAN segment has a unique network-wide identification number. Each source routing bridge has an identification number. Additionally, each source routing bridge has a unique network-wide internal or virtual LAN identification number.

This internal LAN id is required because source routing relies on features of the token ring chipset to capture source routed packets from the LAN. These chipset-specific features limit source routing functions to so-called "1:1 source routing" meaning that standard source routing bridges can link only two networks (either two LANs or a LAN and a WAN). The implementation of an internal "virtual LAN" enables "1:N source routing" at the expense of an additional hop through the bridge.

A proprietary hop-count reduction algorithm eliminates the hop count overhead associated with the internal LAN and enables an expansion of network diameter while remaining within the specifications of the source routing protocol. In order to reduce the hop count between source and destinations on a token ring network, the bridge maintains a unique routing table and uses the information in this table to direct frames to their destinations. For example, when the bridge receives a source routed explorer frame, it examines the routing designators and stores the path from the source to itself in its internal routing table. Later, when the bridge receives an SRF response frame from the destination, it stores the rest of the path between the source-destination pair into the same table.

The bridge refers to this table when it receives a data frame. It first removes all the route designators from the frame's MAC header. It then retrieves only the route descriptors needed to get the frame from the bridge to the destination from its internal routing table and inserts only this information back into the frame's routing designator field. The bridge then relays the frame.

NOTE

In order to maintain sequentiality between a particular pair of source-destination addresses, the bridge always routes frames along the same path once the specific route has been determined.

8.3 Source Routing/Transparent Bridges

Source routing/transparent (SRT) bridge provide concurrent transparent and source routing services. Figure 8-1 shows a sample multi-ring, multi-Ethernet extended network linked by four SRT bridges. Bridge T provides only transparent bridging services. The three other bridges (all labelled S) provide both source routing and transparent services.

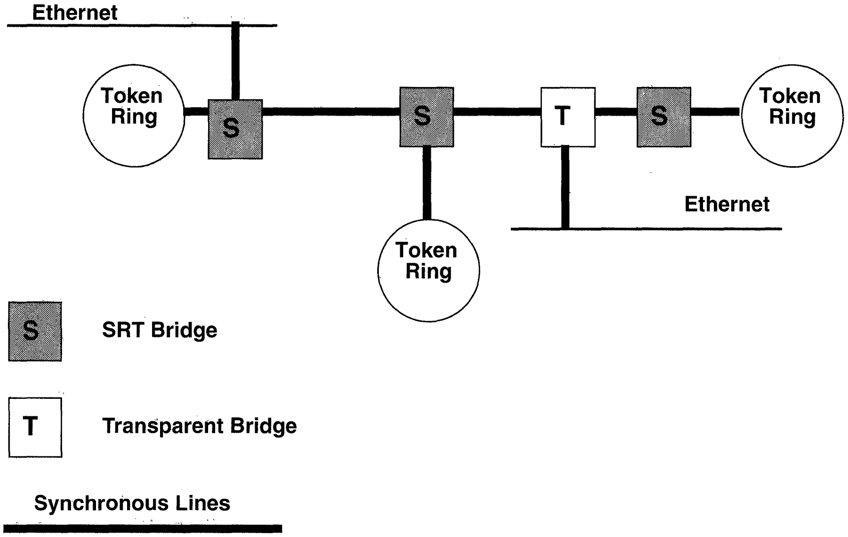


Figure 8-1 Sample SRT Topology

The transparent bridge treats all frames as if they are transparent-bridging frames. In order to effect route discovery, however, the SRT bridge needs to separate frames which require source-routing service from those frames which require transparent-bridging service.

In order to identify source-routing frames, the SRT Bridge inspects the value of the most significant bit of the frame's source address (referred to as the routing information indicator or RII). An RII value of 1 specifies source routing; an RII value of 0 specifies transparent bridging.

NOTE

With source routing enabled, the bridge provides both source routing and transparent bridging.

8.4 Spanning Tree Algorithm

The IEEE 802.1 committee has issued a standard applicable to all MAC-level bridges. Much of this standard is concerned with the operation of bridges in topologically complex environments which may contain redundant or parallel bridge connections between multiple LANs. Such parallel connections cannot be tolerated within a transparent bridging environment.

For example, in Figure 8-2 the Red and White LANs are connected by two parallel bridges, Bridge_1 and Bridge_2. Consider the chain of events when End-station_J on the Red LAN first sends a frame to End-station_K on the White LAN. The frame originated by End-station_J and addressed to End-station_K is read by both Bridge_1 and Bridge_2. As this is the first frame between J and K, the forwarding table of neither bridge contains an entry for End-station_J or End-station_K.

Each bridge updates its forwarding table to indicate that End-station_J is in the direction of the Red LAN. After updating its forwarding table, each bridge floods the frame: Bridge_1 relays the frame over interface 1 and Bridge_2 relays the frame over interface 2. Bridge_2 also relays the frame over interface 3; to simplify the example, however, this frame will not be traced.

Next, End-station_K receives two copies of the frame originated by End-station_J. While the reception of duplicate frames by an end-station is not generally fatal, at best such duplication represents an inefficient use of available bandwidth. Of graver consequence is the effect of duplicate frames on Bridge_1 and Bridge_2. The frame flooded by Bridge_1 onto interface 1 is ultimately read by Bridge_2 on interface 2. When Bridge_2 reads this frame, it updates its forwarding table to indicate End-station_J is in the direction of the White LAN. In a similar fashion Bridge_1 reads the frame flooded by Bridge_2, and it updates its forwarding table to show End-station_J in the direction of the White LAN. Consequently, the forwarding tables of both bridges are corrupted and neither bridge is now able to properly forward a frame to End-station_J.

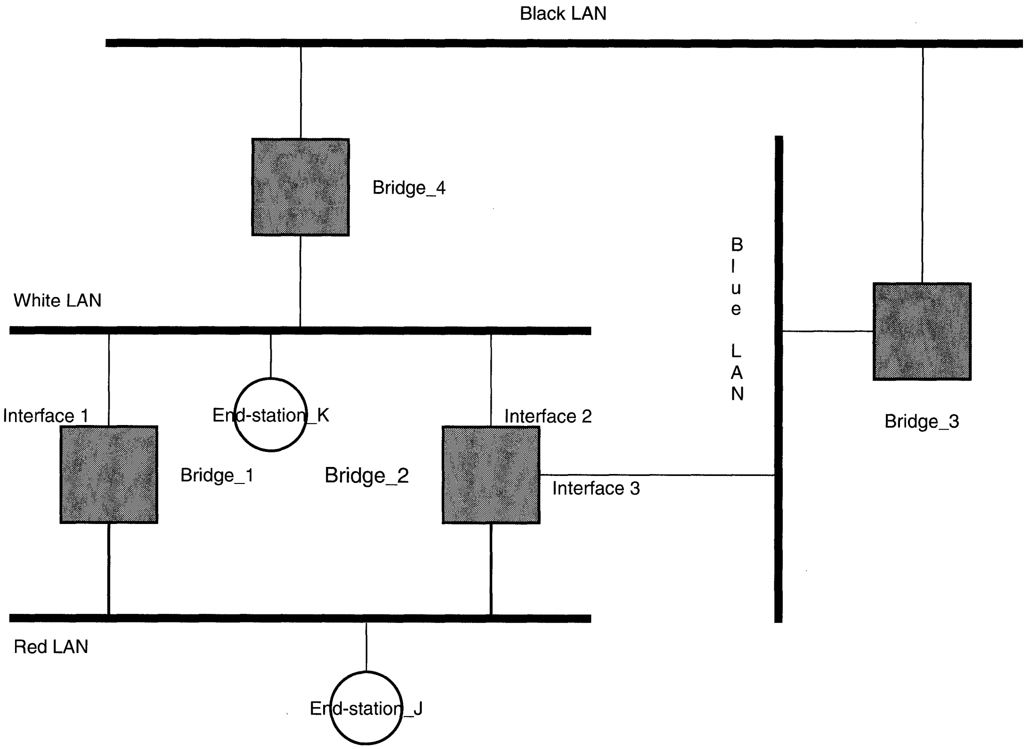


Figure 8-2 Parallel Bridge Topology

This corruption is caused by the existence of alternate routes between hosts. Such alternate routes are generally referred to as loops. The *Spanning Tree Algorithm* (fully described in IEEE 802.1 *MAC Bridges*) ensures the existence of a loop-free topology in networks that contain parallel bridges. The algorithm provides a single path (composed of bridges and intervening LANs) between any two end-stations in such an extended network. It also provides a high degree of fault tolerance by allowing for the automatic reconfiguration of the spanning tree topology in the face of bridge or data-path failure. Five management-assigned values are required for derivation of the spanning tree topology:

- a *multicast address* specifying all bridges within the extended network
- a *network-unique identifier for each bridge* within the extended network
- a *unique identifier for each bridge/LAN interface* (called a port)
- a *priority* specifying the relative priority of each port
- a *cost* for each port

With these values assigned, bridges broadcast and process formatted frames (called Bridge Protocol Data Units or BPDUs) to derive a single loop-free topology throughout the extended network. BPDU frame exchange is accomplished quickly, thus minimizing the time during which service is unavailable between hosts.

In constructing a loop-free topology, the bridges within the extended network first determine the root bridge, the bridge with the best (that is, lowest) priority value. This bridge serves as the root of the loop-free topology.

After determining the identity of the root bridge, all other bridges calculate path costs, that is the cost of the path to the root bridge offered by each bridge port. Each bridge designates the port that offers the lowest-cost path to the root bridge as the root port. In the event of equal path costs, the bridge designates the port with the best (that is, lowest) priority value as the root port.

On each LAN within the extended network one bridge (the one whose root port offers the lowest cost path to the root bridge) is selected as the designated bridge. The port that connects the LAN to the designated bridge is selected as the designated port. This port carries all extended network traffic to and from the LAN, and is said to be in the forwarding state.

This process ensures that all redundant ports (those providing parallel connections) are removed from service (placed in the blocking state). In the event of a topological change, or in the event of bridge or data-path failure, however, the algorithm derives a new spanning tree that may move some such ports from the blocking to the forwarding state.

Using Figure 8-2 as an example, the implementation of the Spanning Tree Algorithm could remove Bridge_1 from service and block Bridge_2/Interface 3. Figure 8-3 shows the resulting logical topology which provides a loop-free topology with only a single path between any two hosts.

8.5 Filtering

Filters enable the bridge to either selectively relay or drop a particular frame on the basis of header fields within each of the four encapsulation methods supported by the bridge. These encapsulation methods are as follows:

- Ethernet
- IEEE 802.2 logical link control
- IEEE 802.2 LLC with SNAP header
- Novell proprietary

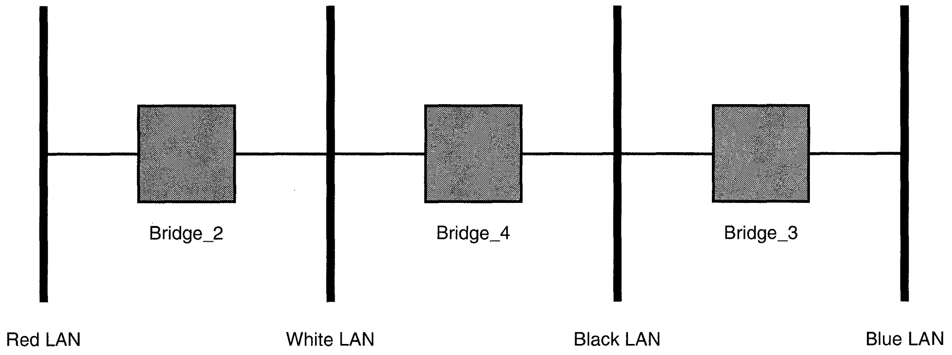


Figure 8-3 Spanning Tree (Loop-Free) Logical Topology

Figures 8-4 through 8-7 illustrate each method of encapsulation.

Preamble 8 octets	Destination 6 octets	Source 6 octets	Type 2 octets	Data 46 - 1500 octets

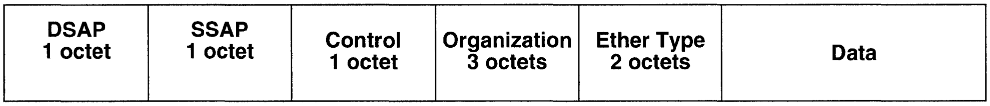
Figure 8-4 Ethernet Encapsulation

Ethernet encapsulation prefixes an eight-octet preamble, six octets of destination-address information, six octets of source-address information, and two octets of protocol type information to the frame. It appends a four-octet frame check sequence to the frame.

DSAP 1 octet	SSAP 1 octet	Control 1 octet	Data 46 - 1500 octets

Figure 8-5 802.2 Encapsulation

802.2 encapsulation prefixes one octet of destination service access point identification, one octet of source service access point identification, and one octet of control information to the frame. The 802.2 frame, in turn, is encapsulated within a MAC-level media-specific frame.



DSAP 1 octet	SSAP 1 octet	Control 1 octet	Organization 3 octets	Ether Type 2 octets	Data

Figure 8-6 SNAP Encapsulation

SNAP encapsulation is an extension of 802.2 encapsulation. It prefixes one octet of DSAP information, one octet of SSAP information, one octet of control information, three octets of organizational information, and two octets of Ethernet Type information to the frame. The SNAP structure is further encapsulated within a MAC-level medium-specific 802.x frame.

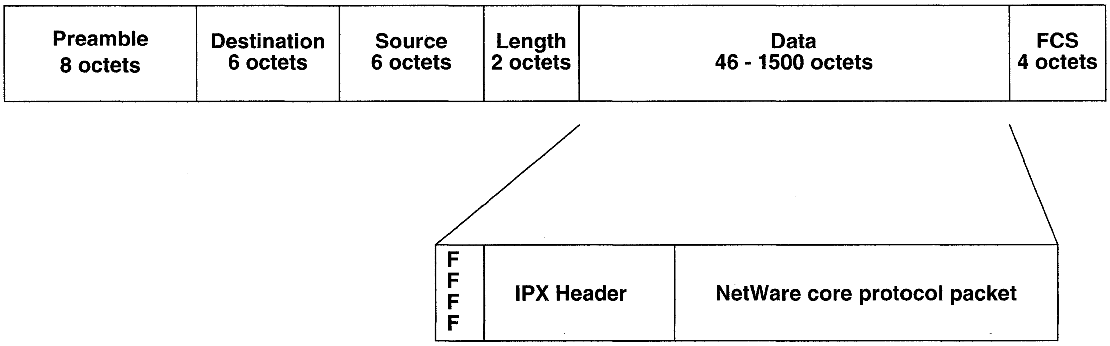


Figure 8-7 Novell Proprietary Encapsulation

Novell proprietary encapsulation prefixes an eight-octet preamble, six octets of destination-address information, six octets of source-address information, and two octets of frame-length information to the unchecksummed IPX frame (indicated by a value of FFFF). It appends a four-octet frame check sequence to the frame.

Table 8-1 shows encapsulation support for each physical access medium.

Table 8-1: Encapsulation/Media Matrix

	Encapsulation Method			
	Ethernet	**802.3**	**SNAP**	**Novell**
Ethernet/802.3	Yes	Yes	Yes	Yes
Token Ring	No	Yes	Yes	No
FDDI	No	Yes	Yes	No
Point-to-Point	Yes	Yes	Yes	Yes

The bridge provides a set of pre-defined filter fields. Table 8-2 lists encapsulation methods along with associated pre-defined fields.

Table 8-2: Pre-Defined Filter Fields

Encapsulation Method	**Pre-Defined Fields**
All	MAC source address MAC destination address
Ethernet	Type
802.2	SSAP DSAP
SNAP	Organization EtherType

The bridge supplements basic filtering functionality by providing the ability to specify user-defined fields within each of the supported encapsulation formats. It also provides the ability to specify lists which contain a collection of value ranges to be filtered.

8.6 Setting Bridge Global Parameters

To begin the bridge configuration process, you assign values to global parameters as listed in Table 8-3.

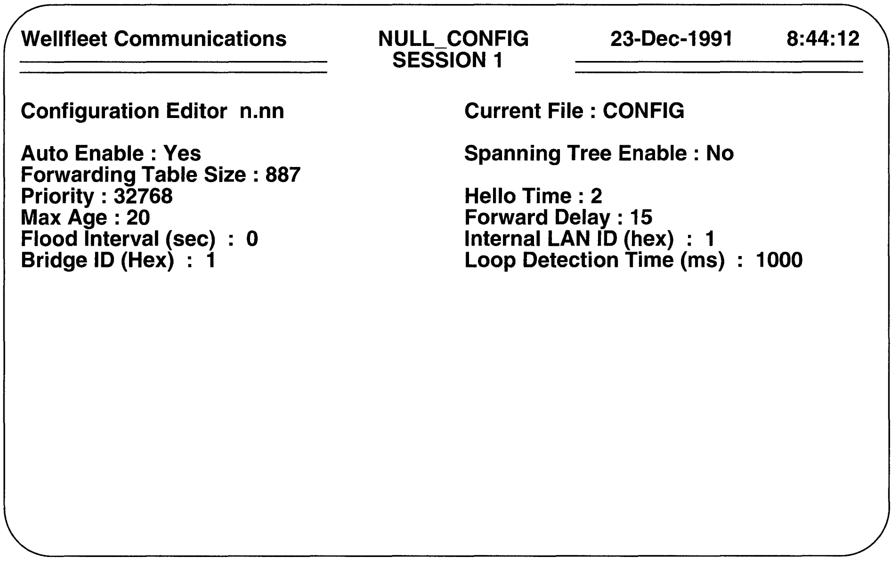
Table 8-3: Bridge Global Parameters

Parameter	Function
Auto Enable	specifies the initialization state
Spanning Tree Enable	enables the spanning tree algorithm
Forwarding Table Size	allocates memory for the forwarding table

You set global bridge parameters from the Configuration Menu. Enter the number that appears to the left of **Bridge** at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Bridge record(s) found
Do you wish to add Bridge record(s)?

Press `[RETURN]` to display the Bridge Parameters Screen (Figure 8-8).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Auto Enable : Yes                            Spanning Tree Enable : No
Forwarding Table Size : 887
Priority : 32768                             Hello Time : 2
Max Age : 20                                 Forward Delay : 15
Flood Interval (sec)  :  0                   Internal LAN ID (hex)  :  1
Bridge ID (Hex)  :  1                        Loop Detection Time (ms)  :  1000
```

Figure 8-8 Bridge Parameters Screen

❒ **Auto Enable** specifies the initial state of the bridge.

This bridge-specific **Auto Enable** works in conjunction with the global auto enable parameter (see Section 2.1) to enable or disable the bridge when the router boots.

When global auto enable is **No**, the bridge is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable the bridge with NCL commands after the router boots.

When global auto enable is **Yes**, the bridge is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either Y**es** (enable the bridge) or **No** (disable the bridge), then press `[RETURN]`. If you choose **No**, you will later need to enable the bridge with NCL commands after the router boots.

❒ **Spanning Tree Enable** enables or disables the spanning tree algorithm.

If your network topology contains redundant bridge/LAN connections, press the `[RIGHTARROW]` to display **Yes** (enabling the spanning tree algorithm), then press `[RETURN]`. If your network topology contains a single bridge or multiple, non-redundant bridges, press `[RETURN]` to disable the algorithm.

NOTE

If you enable source routing, the spanning tree algorithm is always enabled regardless of the value assigned to the **Spanning Tree Enable** parameter.

❒ **Forwarding Table Size** specifies the maximum size of the forwarding table.

The forwarding table contains the list of end-station addresses learned by the bridge, plus all source-address filters and destination-address filters. The value that you enter at **Forwarding Table Size** sets the maximum size of this table. To specify forwarding table size, refer to your network topology drawing and estimate the number of end-stations serviced by the bridge. Double this figure. Finally, select the next highest value from the available responses, and press `[RETURN]`.

8.7 Setting Spanning Tree Parameters

After you set global bridge parameters, you assign values to spanning tree parameters as listed in Table 8-4.

Table 8-4: Bridge Spanning Tree Parameters

Parameter	Function
Priority	assigns a spanning tree priority
Hello Time	specifies the interval between BPDUs
Max Age	specifies the time that routing information is stored
Forward Delay	specifies the time spent in spanning tree Listening and Learning states

❐ **Priority** sets the bridge priority within the spanning tree algorithm.

If you have not enabled the spanning tree algorithm, press `[RETURN]`.

If you have enabled the algorithm, **Priority** supplies the most-significant 16-bits of the unique 64-bit bridge identifier used by the algorithm to identify the root bridge (the bridge with the best priority). The smaller this value, the more likely it is that the bridge will be the root.

Press the `[RIGHTARROW]` to select a value (keeping in mind that the smaller the value, the more likely the bridge will be the root), then press `[RETURN]`.

NOTE

When assigning values to the following three spanning tree parameters (**Hello Time**, **Max Age**, and **Forward Delay**), you may wish to use the recommended values listed in Table 8-5.

❐ **Hello Time** specifies the interval in seconds between BPDUs transmitted by the bridge.

If you have not enabled the spanning tree algorithm, press `[RETURN]`.

If you have enabled the algorithm, **Hello Time** specifies the interval between BPDUs, the periodic transmissions exchanged between bridges in the network to convey configuration and topology change data. Press `[RETURN]` to accept the default value of **2** (seconds), or press the `[RIGHTARROW]` to select another value, then press `[RETURN]`.

Table 8-5: Suggested Spanning Tree Parameter Values

Hello Time	Max Age	Forward Delay
1	>= 6	>= 3
2	>= 6	>= 4
3	>= 8	>= 5
4	>= 10	>= 6
5	>= 12	>= 7
6	>= 14	>= 8
7	>= 16	>= 9
8	>= 18	>= 10
9	>= 20	>= 11
10	>= 22	>= 12

- **Max Age** specifies the maximum length of time the bridge stores configuration information. The bridge declares a line down if it does not receive a BPDU for **Max Age** seconds. After declaring the line down, the bridge sets the port state to *Listen.*

  If you have not enabled the spanning tree algorithm, press `[RETURN]`.

  If you have enabled the spanning tree algorithm, consult Table 8-5 to determine an appropriate value for **Max Age**. Press the `[RIGHTARROW]` to select the value (in the range `6` through `40`), then press `[RETURN]`.

- **Forward Delay** specifies the time that a circuit group spends in the *Listening* and *Learning* states.

  If you have not enabled the spanning tree algorithm, press `[RETURN]`.

  If you have enabled the algorithm, you use **Forward Delay** to provide a timer that clocks a circuit group as it moves from state to state. Setting **Forward Delay** to the minimum value causes the spanning tree to converge at its fastest rate.

  As the algorithm operates, it eventually places all circuit groups in either a *Forwarding* (enabled) or *Blocking* (disabled) state. Later, in response to network topology changes, the algorithm may change the state of specific circuit groups. In order to prevent network looping caused by sudden state changes, the algorithm does not transition circuit groups directly from *Blocking* to *Forwarding*. Rather, it places them in two intermediate states, *Listening* and *Learning*.

While in the *Listening* (stand-by) state, the circuit group receives network-generated BPDUs, but does not receive end-station-generated message traffic. When the Forward Delay Timer expires, the circuit group is placed in the *Learning* state. While in *Learning* state, the circuit group receives network-generated BPDUs, and also receives end-station-generated traffic which is subjected to the learning process but not relayed. When the Forward Delay Timer expires, the circuit group is placed in the *Forwarding* state.

Consult Table 8-5 to determine an appropriate value for **Forward Delay**. Press the `[RIGHTARROW]` to select the value (in the range `4` through `30`), then press `[RETURN]`.

8.8 Flood Limiting

Each frame to an unlearned MAC address (with the exception of multicast or broadcast addresses which are always flooded) is flooded based on a user configurable timer.

❐ **Flood Interval (sec)** specifies the interval during which (at most) a single frame will be flooded to an unlearned address.

If you wish to disable flood limiting, press `[RETURN]` to accept the default value, **0**. If you wish to enable flood limiting, enter a value and then press `[RETURN]`.

8.9 Setting Source Routing Parameters

Internal LAN ID (hex), **Bridge ID (Hex)**, and **Loop Detection Time (ms)** specify source routing services.

❐ **Internal LAN ID (hex)** assigns a numeric identifier to the internal virtual LAN.

If you do not want to enable source routing, press `[RETURN]`. If you do want to enable source routing, enter a hexadecimal value from 0 to FFF and then press `[RETURN]`.

❐ **Bridge ID (Hex)** identifies a specific source route bridge.

If you do not want to enable source routing, press `[RETURN]`.

To facilitate source routing, enter a hexadecimal value between 1 and F and press `[RETURN]`.

NOTE

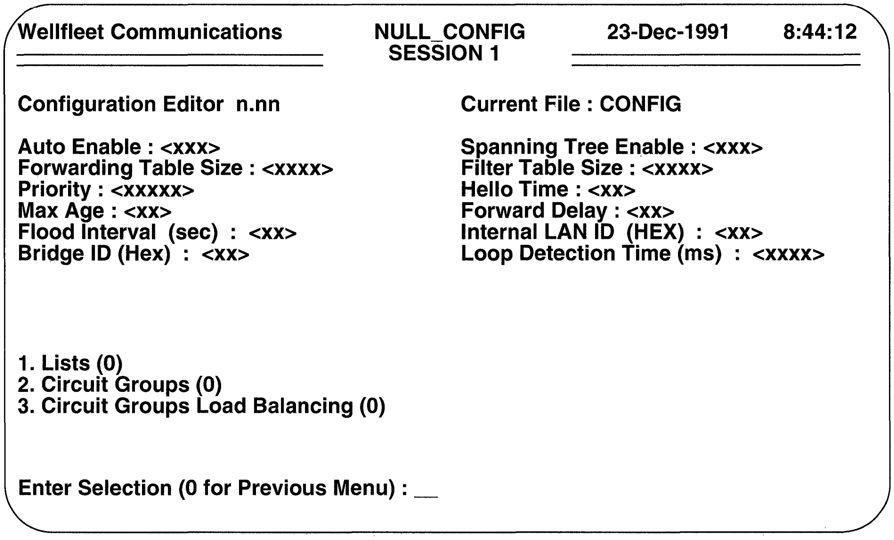
Parallel source routing bridges require unique network-wide **Bridge ID (Hex)** values. Non-parallel bridges need not have unique identifiers.

- ❐ **Loop Detection Time (ms)** detects a loop in the network.

  When the bridge receives an All-Routes Explorer Packet (ARE) for a particular source-destination pair, a time stamp is stored in the appropriate entry in the Source Routing Intermediate Station Table. If the bridge receives another ARE for that same source destination pair before the loop timer has expired, a loop exists in the network and the bridge will drop the packet.

  Accept the default loop detection time of 1000 ms by pressing `[RETURN]` or enter an alternate value and then press `[RETURN]`.

After you press `[RETURN]`, the screen displays the Bridge Configuration Menu.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Auto Enable : <xxx>                          Spanning Tree Enable : <xxx>
Forwarding Table Size : <xxxx>               Filter Table Size : <xxxxx>
Priority : <xxxxxx>                          Hello Time : <xx>
Max Age : <xx>                               Forward Delay : <xx>
Flood Interval  (sec)  :  <xx>               Internal LAN ID  (HEX)  :  <xx>
Bridge ID (Hex)  :  <xx>                     Loop Detection Time (ms)  :  <xxxx>




1. Lists (0)
2. Circuit Groups (0)
3. Circuit Groups Load Balancing (0)


Enter Selection (0 for Previous Menu) : __
```

Figure 8-9 Bridge Configuration Menu

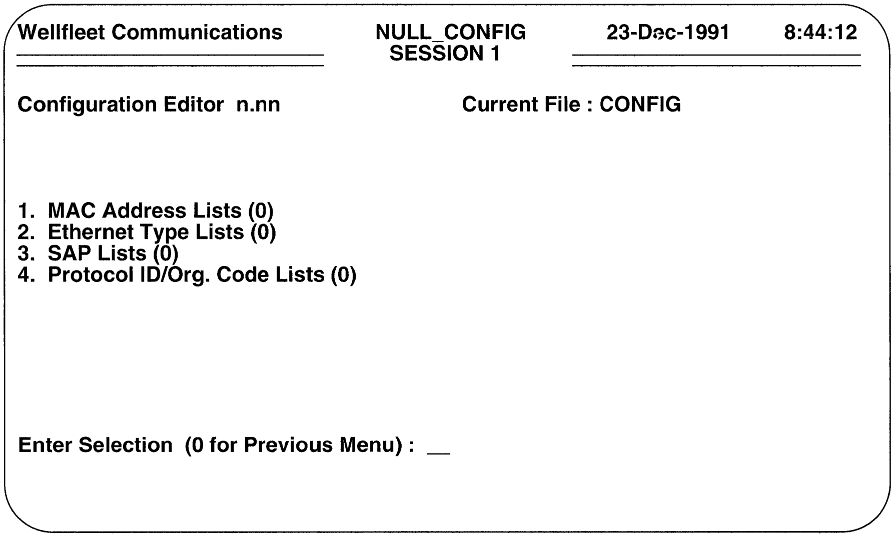
8.10 Compiling Filter Lists

A list contains a range of values that can be used in conjunction with the filtering of pre-defined fields. A list consists of a symbolic name and a collection of ranges. When a bridge filter specifies a list name, frames are checked against the range of values specified by the list.

You compile lists from the Bridge Configuration Menu. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Lists record(s) found
Do you wish to add Lists record(s)?

Press [RETURN] to display the List Access Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG



1. MAC Address Lists (0)
2. Ethernet Type Lists (0)
3. SAP Lists (0)
4. Protocol ID/Org. Code Lists (0)





Enter Selection  (0 for Previous Menu) : __
```

Figure 8-10 List Access Screen

You use the List Access Screen to construct field-specific lists, as follows.

8.10.1 MAC Address Lists

MAC address lists specify ranges of media-access-control addresses.

You compile a MAC address list from the List Access Screen. Enter <1> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

> **No MAC Address Lists record(s) found**
> **Do you wish to add MAC Address Lists record(s)?**

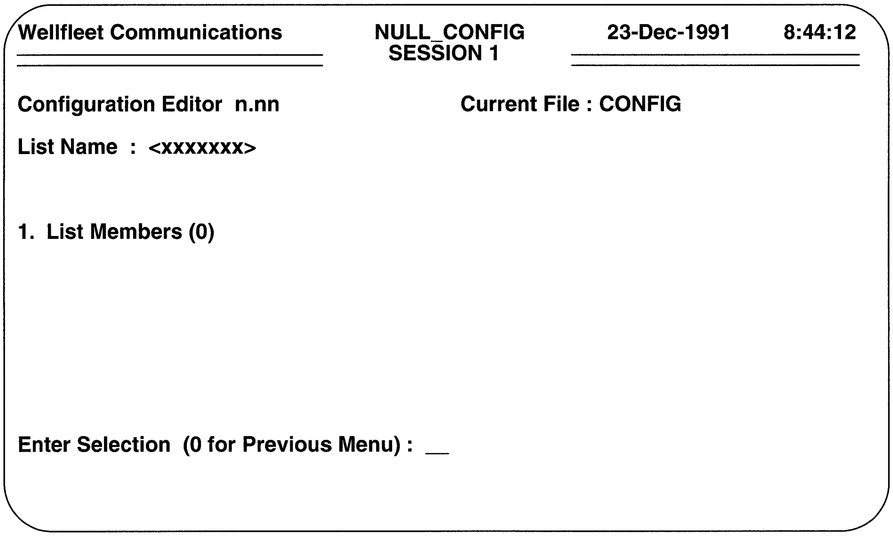
Press [RETURN]. The screen prompts for a **List Name**.

❒ **List Name** identifies the MAC address list.

Enter a list name.

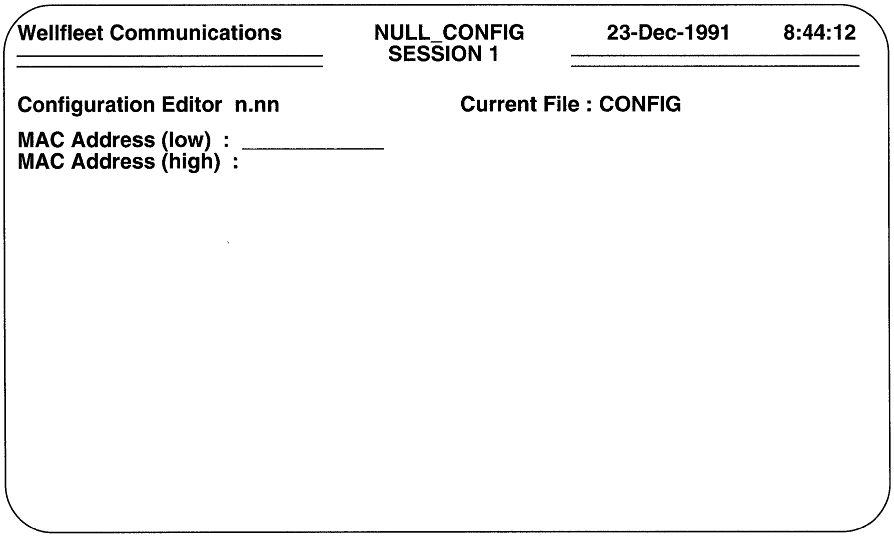
The screen prompts for list members (Figure 8-11).

To assign a range of MAC-level addresses to the list, enter <1> at **Enter Selection (0 for Previous Menu)**. The screen prompts:



```
Wellfleet Communications          NULL_CONFIG       23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG

List Name  :  <xxxxxxx>


1.  List Members (0)






Enter Selection  (0 for Previous Menu) :  __
```

Figure 8-11 List Member Access Screen



```
Wellfleet Communications          NULL_CONFIG       23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG

MAC Address (low)  :  ____________
MAC Address (high)  :
```

Figure 8-12 MAC Address Range Screen

No List Members record(s) found
Do you wish to add List Members record(s)?

Press `[RETURN]` to display the MAC Address Range Screen (Figure 8-12).

- ❐ **MAC Address (low)** specifies the lower boundary of the filtered MAC address range.

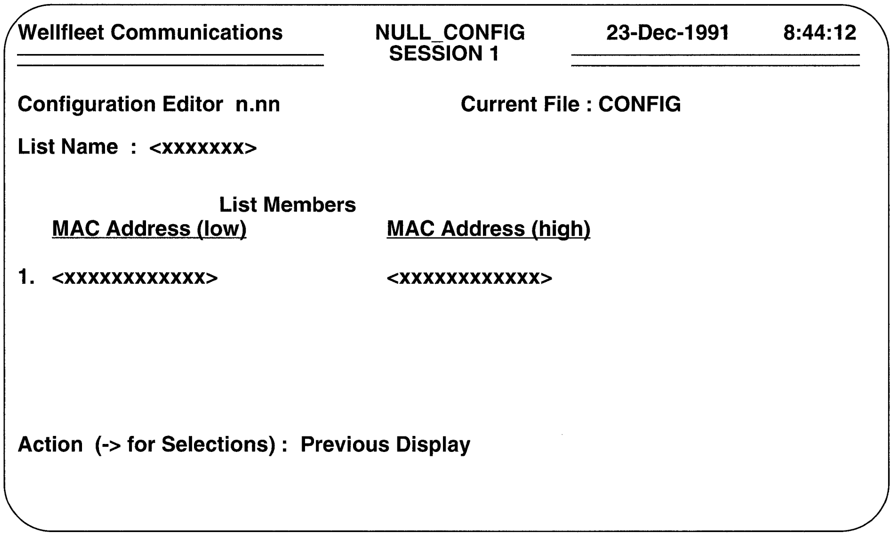
  Enter the MAC address.

- ❐ **MAC Address (high)** specifies the upper boundary of the filtered MAC address range.

  Enter the MAC address. If you want the list range to consist of a single value, entered in response to **MAC Address (low)**, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the List Member Access Screen.

If you want, you can add other MAC address ranges to the MAC address list. To add an address range, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the MAC Address List Members Screen.

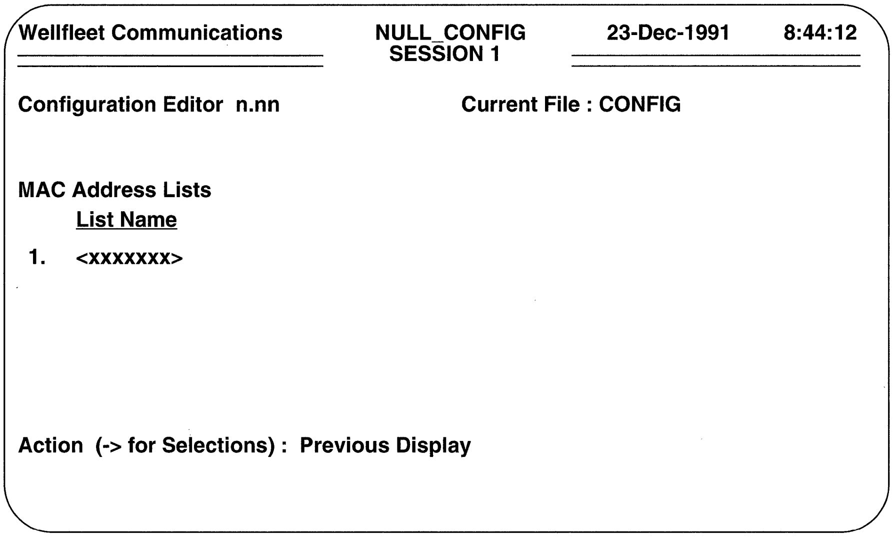


```
Wellfleet Communications         NULL_CONFIG       23-Dec-1991      8:44:12
                                  SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG

List Name  :  <xxxxxxx>

                           List Members
   MAC Address (low)                 MAC Address (high)

1.  <xxxxxxxxxxxx>                   <xxxxxxxxxxxx>




Action  (-> for Selections) :  Previous Display
```

Figure 8-13 MAC Address List Members Screen

To add another range of MAC addresses, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the MAC Address Range Screen. Now follow the same procedure as before to add another MAC address range; continue in this fashion until you have added all desired ranges to the list.

You construct additional MAC address lists from the List Access Screen. To begin, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the MAC Address List Summary Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG


MAC Address Lists
     List Name
 1.  <xxxxxxx>






Action  (-> for Selections) :  Previous Display
```

Figure 8-14 MAC Address List Summary Screen

To construct another MAC address list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the same procedure as before to construct an additional MAC address list; continue until you have constructed all MAC address lists.

8.10.2 Ethernet Type Lists

Ethernet type lists specify ranges of Ethernet type values. Table 8-6 provides a partial list of such values.

You construct an Ethernet type list from the List Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Ethernet Type Lists record(s) found
Do you wish to add Ethernet Type Lists record(s)?

Press `[RETURN]`. The screen prompts for a **List Name**.

❒ **List Name** identifies the Ethernet type list.

Enter a list name, and then press `[RETURN]`.

Table 8-6: Public Ethernet Type Field Values

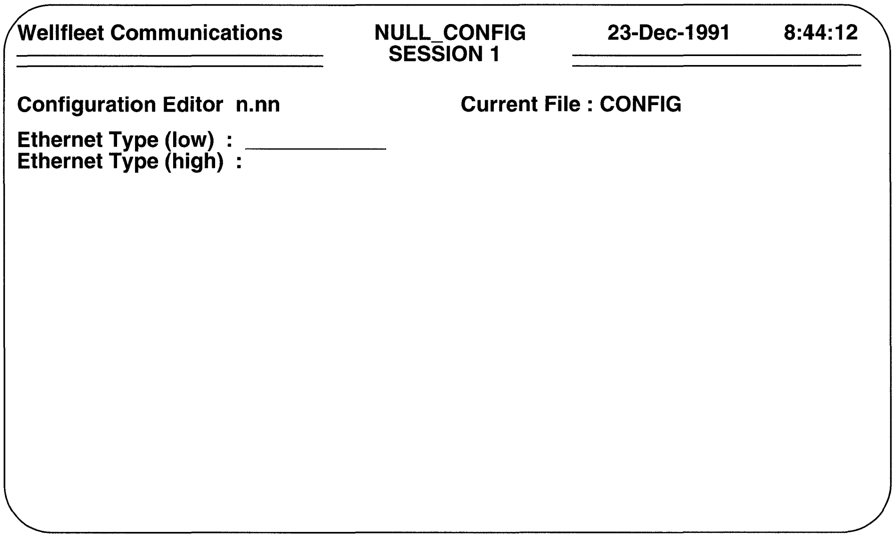
Type Field	Assigned to:	Type Field	Assigned to:
0600	XNS Internet	807A	Matra
0800	DoD Internet	807C	Univ of Michigan
0801	X.75 Internet	807D to 8080	Vitalink Communications
0802	NBS Internet	8081 to 8083	Counterpoint Communications
0803	ECMA Internet	809B	Kinetics
0804	CHAOSnet	809C to 809E	Datability
0805	X.25 Level 3	809F	Spider Systems
0806	Ethernet ARP	80A3	Nixdorf Computer
0888 to 088A	Xyplex	80A4 to 80B3	Siemens Gammasonics
6010 to 6014	3COM Corporation	80C0 to 80C3	Digital Communications
7020 to 7029	LRT	80C6	Pacer Software
8006	Nestar	80C7	Applitek Corporation
8008	AT&T	80C8 to 80CC	Intergraph Corporation
8013 to 8016	Silicon Graphics	80CD to 80CE	Harris Corporation
8019	Apollo Computer	80CF to 80D2	Taylor Instrument
802E	Tymshare	80D3 to 80D4	Rosemount Corporation
802F	Tigan	80DD	Varian Associates
8035	Stanford University	80DE to 80DF	Integrated Solutions
8036	Aeonic Systems	80E0 to 80E3	Allen-Bradley
8044	Planning Research Corp.	80E4 to 80F0	Datability
8046 to 8047	AT&T	80F2	Retix
8049	ExperData	80F3 to 80F5	Kinetics
805B to 805C	Stanford University	80F7	Apollo Computer
805D	Evans & Sutherland	80FF to 8103	Wellfleet Communications
8060	Little Machines	8069	AT&T
8062	Counterpoint Computers	807B	Dansk Data Elektronic
8065 to 8066	U of Mass/Amhearst	8130	Waterloo Microsystems
8067	Veeco Integrated	8131	VG Laboratory Systems
8068	General Dynamics	8137 to 8138	Novell, Inc.
806A	Autophon	8139 to 813D	KTI
806C	ComDesign	0101 to 01FF	Experimental
806D	Compugraphic	9000	Loopback
806E to 8077	Landmark Graphic		

After you name the Ethernet type list, the screen prompts for list members.

To assign a range of Ethernet types to the list, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen prompts:

> **No List Members record(s) found**
> **Do you wish to add List Members record(s)?**

Press `[RETURN]` to display the Ethernet Type Range Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG

Ethernet Type (low)  : ___________
Ethernet Type (high)  :
```

Figure 8-15 Ethernet Type Range Screen

- ❒ **Ethernet Type (low)** specifies the lower boundary of the filtered Ethernet type range.

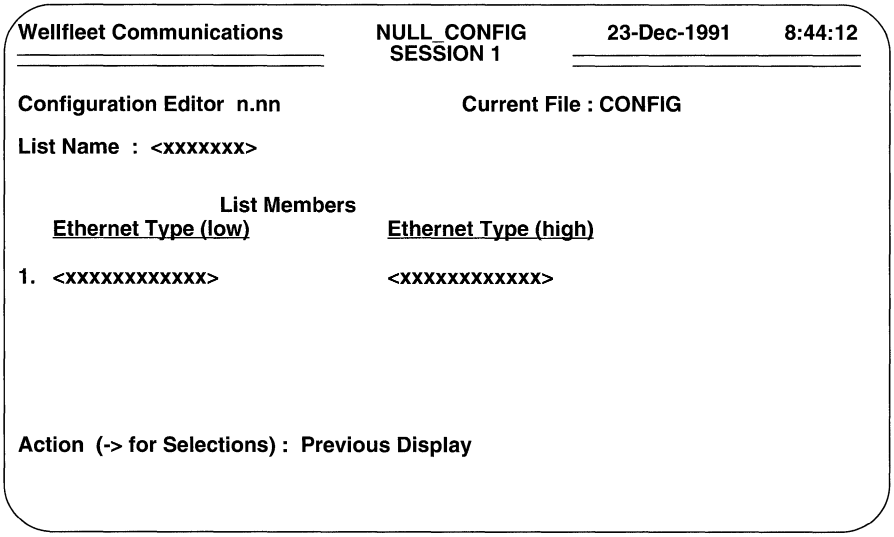
  Enter the Ethernet type.

- ❒ **Ethernet Type (high)** specifies the upper boundary of the filtered Ethernet type range.

  Enter the Ethernet type, and then press `[RETURN]`. If you want the list range to consist of a single value, entered in response to **Ethernet Type (low)**, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the List Member Access Screen.

If you want, you can add other Ethernet type ranges to the Ethernet type list. To add a type range, enter <1> at **Enter Selection (0 for Previous Menu)** to display the Ethernet Type List Members Screen.



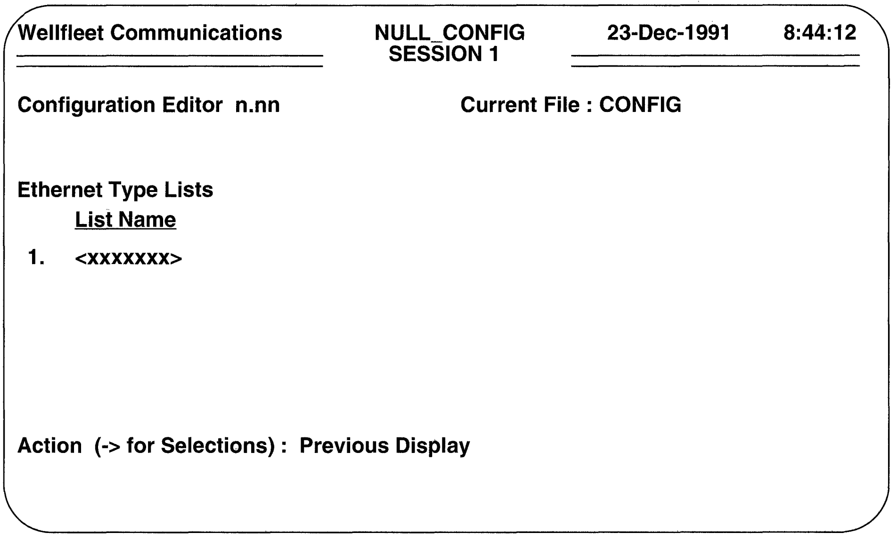
```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

List Name  :  <xxxxxxx>

                        List Members
   Ethernet Type (low)                    Ethernet Type (high)

1.  <xxxxxxxxxxxx>                        <xxxxxxxxxxxx>




Action  (-> for Selections) :  Previous Display
```

Figure 8-16 Ethernet Type List Members Screen

To add another range of Ethernet types, press the [RIGHTARROW] to display **Add** and then press [RETURN] to display the Ethernet Type Range Screen. Now follow the same procedure as before to add another Ethernet type address range; continue in this fashion until you have added all desired ranges to the list.

You construct additional Ethernet type lists from the List Access Screen. Enter <2> at **Enter Selection (0 for Previous Menu)** to display the Ethernet Type List Summary Screen (Figure 8-17).

To construct another Ethernet type list, press the [RIGHTARROW] to display **Add**, then press [RETURN]. Now follow the same procedure as before to construct an additional Ethernet type list; continue until you have constructed all Ethernet type lists.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn               Current File : CONFIG


Ethernet Type Lists
     List Name
 1.  <xxxxxxx>





Action  (-> for Selections) :  Previous Display
```

Figure 8-17 Ethernet Type List Summary Screen

8.10.3 SAP Lists

SAP lists specify ranges of destination or source service access points.

You construct a SAP list from the List Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No SAP Lists record(s) found
Do you wish to add SAP Lists record(s)?

Press `[RETURN]`. The screen prompts for a **List Name**.

□ **List Name** identifies the SAP list.

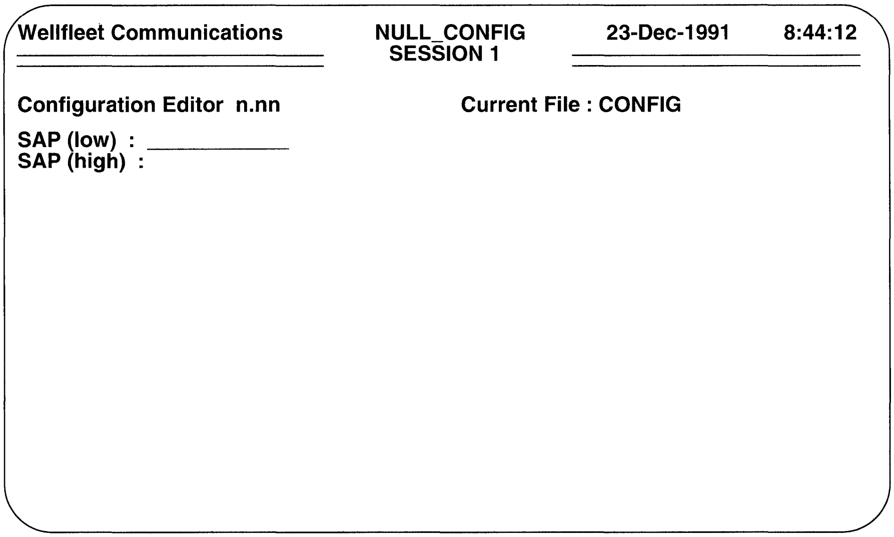
Enter a list name, and then press `[RETURN]`.

After you name the SAP list, the screen prompts for list members.

To assign a range of SAP values to the list, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen prompts:

No List Members record(s) found
Do you wish to add List Members record(s)?

Press `[RETURN]` to display the SAP Specification Screen (Figure 8-18).



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn              Current File : CONFIG

SAP (low)  : __________
SAP (high) :
```

Figure 8-18 SAP Specification Screen

- ❐ **SAP (low)** specifies the lower boundary of the filtered SAP range.

  Enter the SAP value, and then press `[RETURN]`.

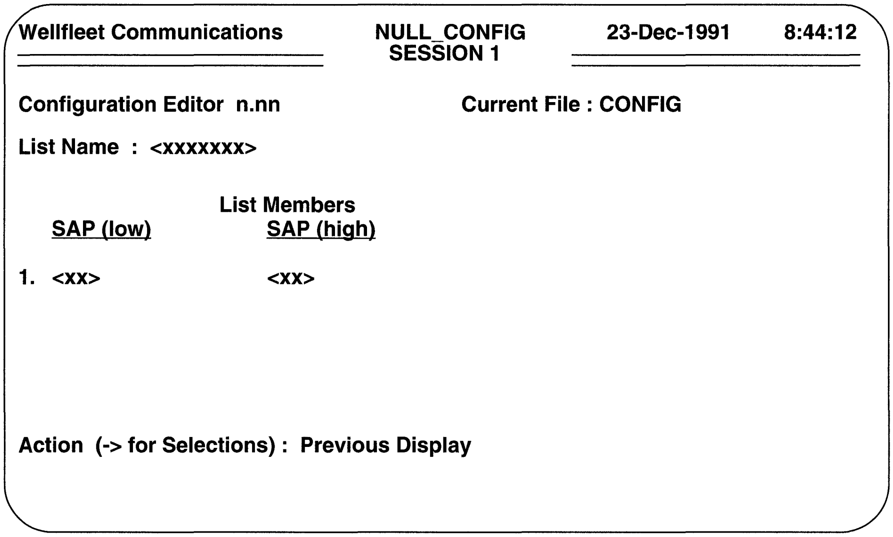
- ❐ **SAP (high)** specifies the upper boundary of the filtered SAP range.

  Enter the SAP value, and then press `[RETURN]`. If you want the list range to consist of a single value, entered in response to **SAP (low)**, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the List Member Access Screen.

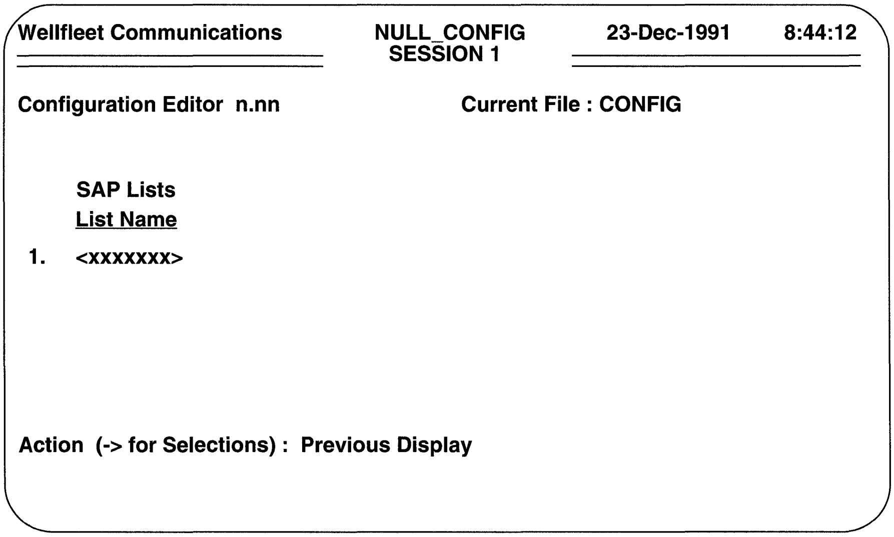
If you want, you can add other SAP ranges to the SAP list. To add a range, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the SAP Members Screen (Figure 8-19). To add another range of SAP values, press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the SAP Specification Screen. Now follow the same procedure as before to add another SAP range; continue in this fashion until you have added all desired ranges to the list.

You construct additional SAP lists from the List Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)** to display the SAP List Summary Screen (Figure 8-20).



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG

List Name  :  <xxxxxxx>

                       List Members
   SAP (low)               SAP (high)

1.  <xx>                   <xx>




Action  (-> for Selections) :  Previous Display
```

Figure 8-19 SAP List Members Screen



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG


      SAP Lists
      List Name

 1.   <xxxxxxx>




Action  (-> for Selections) :  Previous Display
```

Figure 8-20 SAP List Summary Screen

To construct another SAP list, press the [RIGHTARROW] to display **Add**, then press [RETURN]. Now follow the same procedure as before to construct an additional SAP list; continue until you have constructed all SAP lists.

8.10.4 Protocol ID/Organization Code Lists

Protocol ID lists specify ranges of SNAP protocol/organization identifiers.

You construct an organization list from the List Access Screen. Enter <4> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Protocol ID/Org. Code Lists record(s) found
Do you wish to add Protocol ID/Org. Code Lists record(s)?

Press [RETURN]. The screen prompts for a **List Name**.

- ❒ **List Name** identifies the SNAP/Protocol ID list.

  Enter a list name, and then press [RETURN].

After you name the protocol ID list, the screen prompts for list members.

To assign a range of protocol identifiers to the list, enter <1> at **Enter Selection (0 for Previous Menu)**. The screen prompts:

No List Members record(s) found
Do you wish to add List Members record(s)?

Press [RETURN] to display the Protocol ID Specification Screen (Figure 8-21).

- ❒ **Protocol ID/Org. Code (low)** specifies the lower boundary of the filtered protocol ID range.

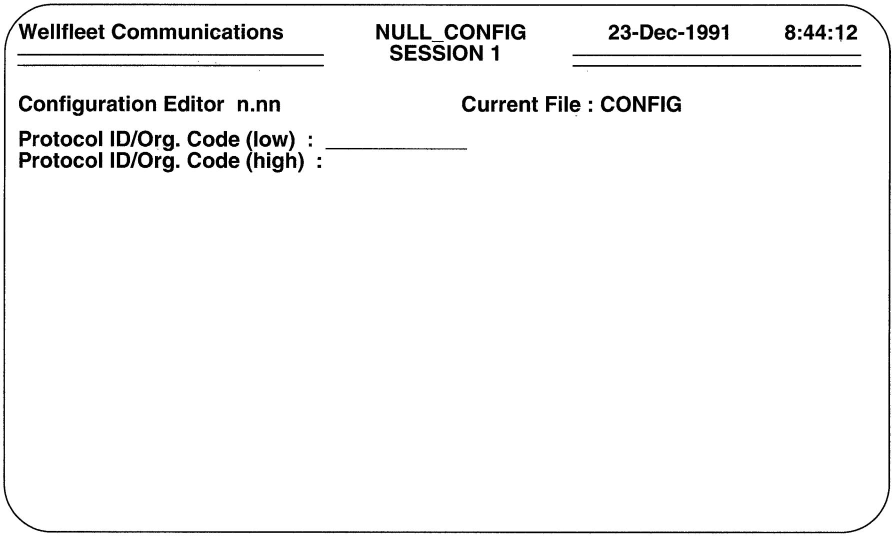
  Enter the protocol ID value.

- ❒ **Protocol ID/Org. Code (high)** specifies the upper boundary of the filtered protocol ID range.

  Enter the protocol ID value, and then press [RETURN]. If you want the list range to consist of a single value, entered in response to **Protocol ID/Org. Code (low)**, press [RETURN].

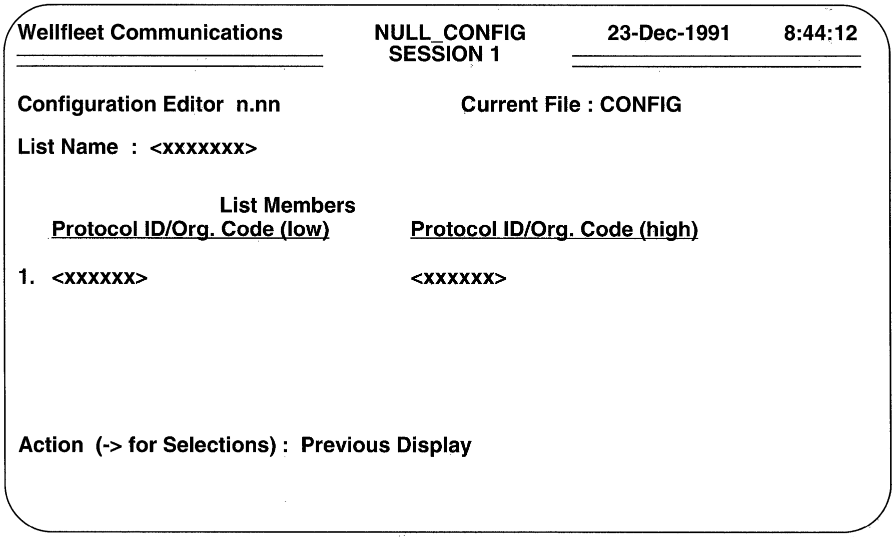
After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press [RETURN] to go back to the List Member Access Screen.

If you want, you can add other protocol ID ranges to the protocol ID list. To add a range, enter <1> at **Enter Selection (0 for Previous Menu)** to display the Protocol ID Members Screen (Figure 8-22). To add another range of protocol ID values, press the [RIGHTARROW] to display **Add** and then press [RETURN] to display the Protocol ID Specification Screen. Now follow the same procedure as before to add another protocol ID range; continue in this fashion until you have added all desired ranges to the list.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG

Protocol ID/Org. Code (low)  : ______________
Protocol ID/Org. Code (high)  :
```

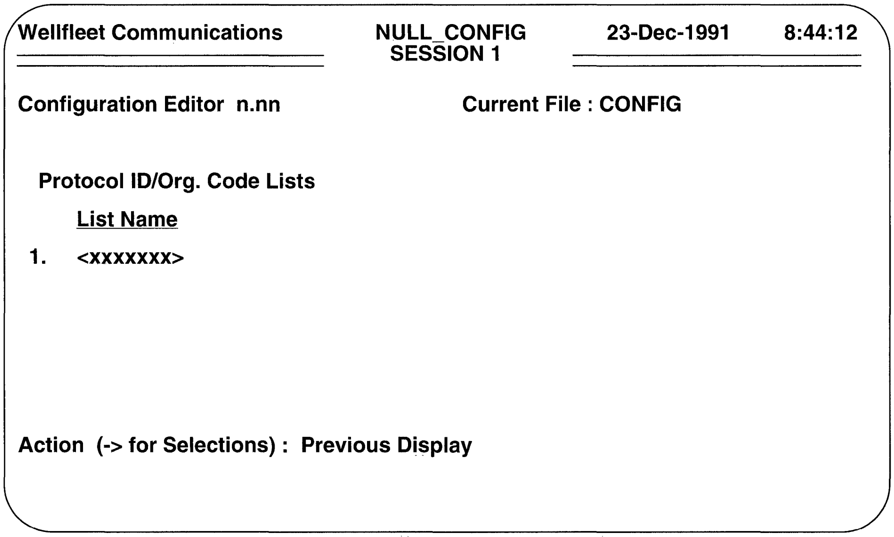
Figure 8-21 Protocol ID Specification Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG

List Name  :  <xxxxxxxx>

                      List Members
   Protocol ID/Org. Code (low)          Protocol ID/Org. Code (high)

1.  <xxxxxxx>                           <xxxxxxx>




Action  (-> for Selections) :  Previous Display
```

Figure 8-22 Protocol ID List Members Screen

You construct additional protocol ID lists from the List Access Screen. Enter `<4>` at **Enter Selection (0 for Previous Menu)** to display the Protocol ID List Summary Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG


  Protocol ID/Org. Code Lists
      List Name
 1.   <xxxxxxx>






Action  (-> for Selections) :  Previous Display
```

Figure 8-23 Protocol ID List Summary Screen

To construct another protocol ID list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the same procedure as before to construct an additional protocol ID list; continue until you have constructed all protocol ID lists.

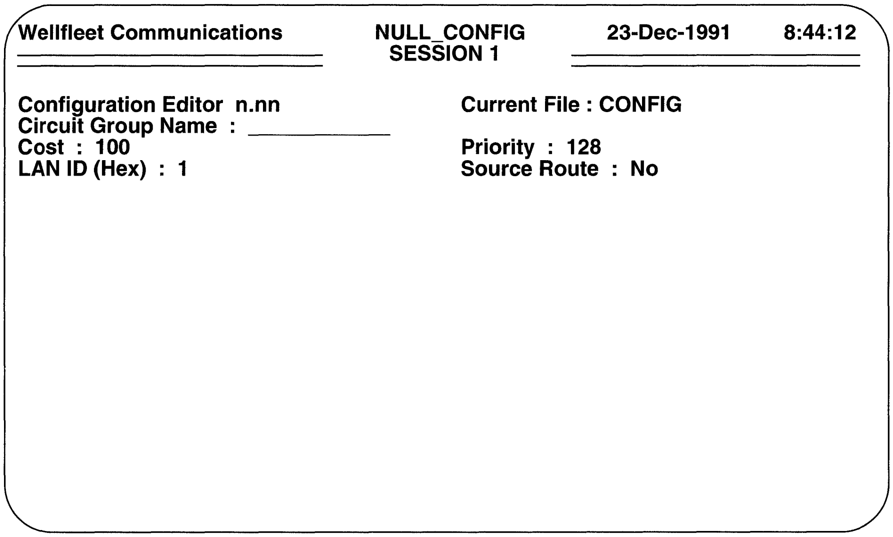
8.11 Defining Bridge Circuit Groups

Circuit groups provide the logical connections between the bridge and its attached networks. You need to define a circuit group for each bridge interface.

You define circuit groups from the Bridge Configuration Menu. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Circuit Groups record(s) found
Do you wish to add Circuit Groups record(s)?

Press `[RETURN]` to display the Bridge Circuit Group Parameters Screen (Figure 8-24).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
______________________________    SESSION 1      ____________________________

Configuration Editor  n.nn                    Current File : CONFIG
Circuit Group Name  :  __________
Cost  :  100                                  Priority  :  128
LAN ID (Hex)  :  1                            Source Route  :  No
```

Figure 8-24 Bridge Circuit Group Parameters Screen

❒ **Circuit Group Name** identifies the circuit group that connects the bridge and the attached LAN or network device.

Enter the name of the circuit group.

❒ **Cost** assigns a relative cost value to the circuit group.

Cost is meaningful only if you have enabled the spanning tree algorithm. If you have not enabled the algorithm, press **[RETURN]**.

Cost reflects the relative speed of the media, in that lower costs indicate high-speed media, while higher costs indicate low-speed media. You use **Cost** to direct network traffic to higher-speed media.

Use the **[RIGHTARROW]** to select a circuit group cost, then press **[RETURN]**.

❒ **Priority** assigns a relative priority value to the circuit group.

Priority is meaningful only if you have enabled the spanning tree algorithm. If you have not enabled the algorithm, press **[RETURN]**.

In the event of identical-cost circuit groups, the spanning tree algorithm selects the circuit group with the better (lower) priority value.

Use the **[RIGHTARROW]** to select a priority, then press **[RETURN]**.

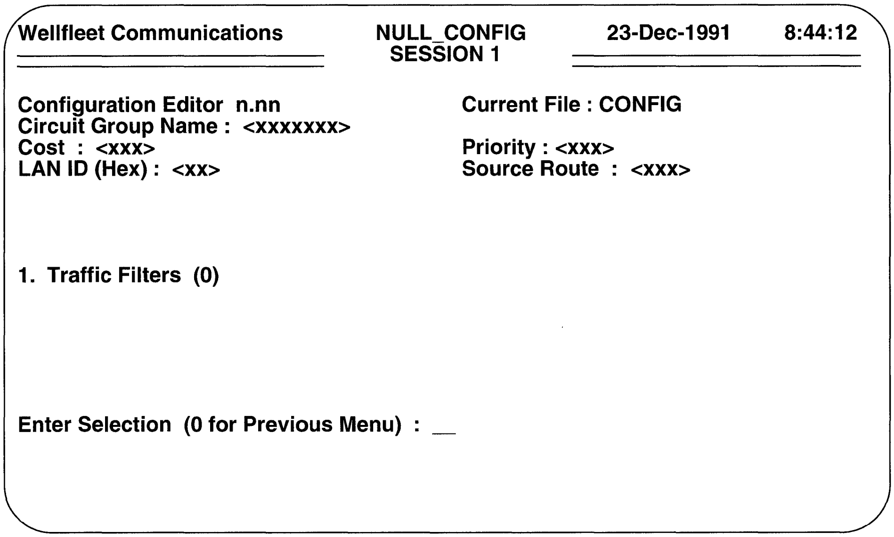
- ❒ **LAN ID (Hex)** assigns a numeric identifier to the network connected by **Circuit Group Name**. This identifier is used by the bridge as it constructs routing designators.

  If you will not enable source routing across **Circuit Group Name**, press `[RETURN]`. If you will enable source routing across **Circuit Group Name**, enter a hexadecimal value from 0 to FFF and then press `[RETURN]`.

- ❒ **Source Route** enables source routing on **Circuit Group Name**.

  Press the `[RIGHTARROW]` to enable (**Yes**) or disable (**No**) source routing across this circuit group, and then press `[RETURN]`.

After you press `[RETURN]`, the screen prompts for circuit-group-specific traffic filters.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Circuit Group Name :  <xxxxxxx>
Cost  :  <xxx>                                Priority : <xxx>
LAN ID (Hex) :  <xx>                          Source Route  :  <xxx>



1.  Traffic Filters  (0)




Enter Selection  (0 for Previous Menu)  :  __
```

Figure 8-25 Circuit Group Filter Access Screen

8.11.1 Traffic Filters

Traffic filters apply to all in-coming bridge traffic across the circuit group. You can, if you wish, construct up to 31 filters for each bridge circuit group.

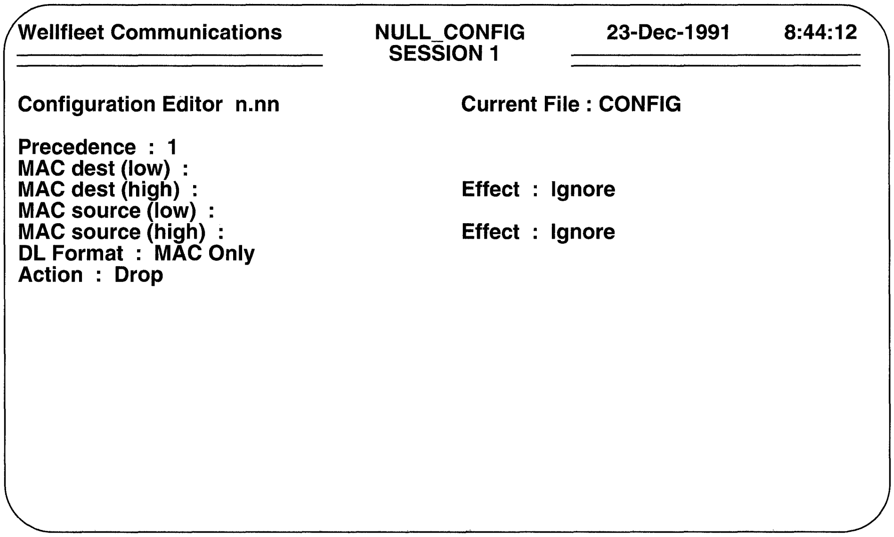
Conceptually a filter consists of a *rule* which identifies packets to be filtered, an *action* to take upon receipt of a frame that meets the conditions of the rule, and a *precedence* that identifies which action to take in the event of a frame that meets the conditions of more than one rule.

- A filter rule consists of three entities: a specified field (or fields) in the frame header; a value (or range of values) associated with the field; and an operator which specifies the relationship between field and value.
- A filter operator may take one of three values: ignore, match, or don't match.
- A filter precedence is designated by a decimal value from 1 to 31; the higher the value, the greater the precedence.

You begin the construction of all circuit-group-specific traffic filters from the Circuit Group Filter Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

No Traffic Filters record(s) found
Do you wish to add Traffic Filters record(s)?

Press `[RETURN]` to display the Bridge Filters Basic Parameters Screen.



```
Wellfleet Communications            NULL_CONFIG        23-Dec-1991      8:44:12
                                     SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Precedence  :  1
MAC dest (low)  :
MAC dest (high)  :                           Effect  :  Ignore
MAC source (low)  :
MAC source (high)  :                         Effect  :  Ignore
DL Format  :  MAC Only
Action  :  Drop
```

Figure 8-26 Bridge Filters Basic Parameters Screen

You use the Bridge Filters Basic Parameters Screen to construct MAC-level source and destination address filters and to construct encapsulation-specific filters. If you want to construct MAC-level source and/or destination address filters, proceed to Section 8.11.1.1. Otherwise, proceed to Section 8.11.1.2 to construct Ethernet filters; Section 8.11.1.3 to construct 802.2 LLC filters; Section 8.11.1.4 to construct 802.2 SNAP filters; or Section 8.11.1.5 to construct Novell filters.

8.11.1.1 MAC-Level Source and Destination Address Filters

MAC-level source and destination address filters enable you to drop or forward a frame on the basis of its source and destination addresses. Such filters can filter source addresses only, destination addresses only, or some specified combination of source and destination addresses.You can construct MAC-level source and/or destination address filters for any of the four supported encapsulation methods.

You construct MAC-level source and destination address filters from the Bridge Filters Basic Parameters Screen.

❐ **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

You can construct up to 31 filters per bridge interface. The **Precedence** value is used when an in-coming frame meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

NOTE

In the event of two filters with equal precedence, the first configured filter takes precedence.

Select a value from 1 to 31 and then press `[RETURN]`.

❐ **MAC dest (low)** specifies the lower boundary range of filtered MAC-level destination addresses.

If you do not want to filter MAC-level destination addresses, press `[RETURN]`.

To filter MAC-level destination addresses, do one of the following:

- enter the name of a MAC address list
- enter a MAC address at the lower boundary of the address range that you want to filter
- enter a single MAC address that you want to filter

After you enter a MAC address or a list name, press `[RETURN]`.

❐ **MAC dest (high)** specifies the upper boundary range of filtered MAC-level destination addresses.

If you do not want to filter MAC-level destination addresses, press `[RETURN]`.

To filter MAC-level destination addresses, do one of the following:

- if you entered the name of a MAC address list at **MAC dest (low)**, or if you want to filter the single MAC address entered at **MAC dest (low)**, press [RETURN].
- if you entered a lower boundary range value at **MAC dest (low)**, enter a MAC address at the upper boundary of the address range that you want to filter and then press [RETURN].

❒ **Effect** designates one of three operators applied to the MAC destination address pattern specified by **MAC dest (low)** and **MAC dest (high)**.

If the filter does not care about MAC destination address values, press [RETURN] to accept the default, **Ignore**.

To filter MAC-level destination addresses, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **MAC dest (low)** and **MAC dest (high)** includes the destination MAC address of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **MAC dest (low)** and **MAC dest (high)** does not include the destination MAC address of the frame.

Press the [RIGHTARROW] to select the operator, and then press [RETURN].

❒ **MAC source (low)** specifies the lower boundary range of filtered MAC-level source addresses.

If you do not want to filter MAC-level source addresses, press [RETURN].

To filter MAC-level source addresses, do one of the following:

- enter the name of a MAC address list
- enter a MAC address at the lower boundary of the address range that you want to filter
- enter a single MAC address that you want to filter

After you enter a MAC address or a list name, press [RETURN].

❒ **MAC source (high)** specifies the upper boundary range of filtered MAC-level source addresses.

If you do not want to filter MAC-level source addresses, press [RETURN].

To filter MAC-level source addresses, do one of the following:

- if you entered the name of a MAC address list at **MAC source (low)**, or if you want to filter the single MAC address entered at **MAC source (low)**, press [RETURN].
- if you entered a lower boundary range value at **MAC source (low)**, enter a MAC address at the upper boundary of the address range that you want to filter and then press [RETURN].

❒ **Effect** designates one of three operators applied to the MAC source address pattern specified by **MAC source (low)** and **MAC source (high)**.

If the filter does not care about MAC source address values, press `[RETURN]` to accept the default, **Ignore**.

To filter MAC-level source addresses, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **MAC source (low)** and **MAC source (high)** includes the source MAC address of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **MAC source (low)** and **MAC source (high)** does not include the source MAC address of the frame.

Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

❒ **DL Format** enables the construction of more complex filters that combine MAC-level source and destination address filtering with filtering on various encapsulation-specific fields.

To construct a filter that examines only MAC-level addresses, press `[RETURN]` to accept the default response, **MAC Only**.

If you want to construct more complex filters, proceed to Section 8.11.1.2 to construct Ethernet filters; Section 8.11.1.3 to construct 802.2 LLC filters; Section 8.11.1.4 to construct 802.2 SNAP filters; or Section 8.11.1.5 to construct Novell filters.

❒ **Action** specifies the disposition of frames that meet the filter rule.

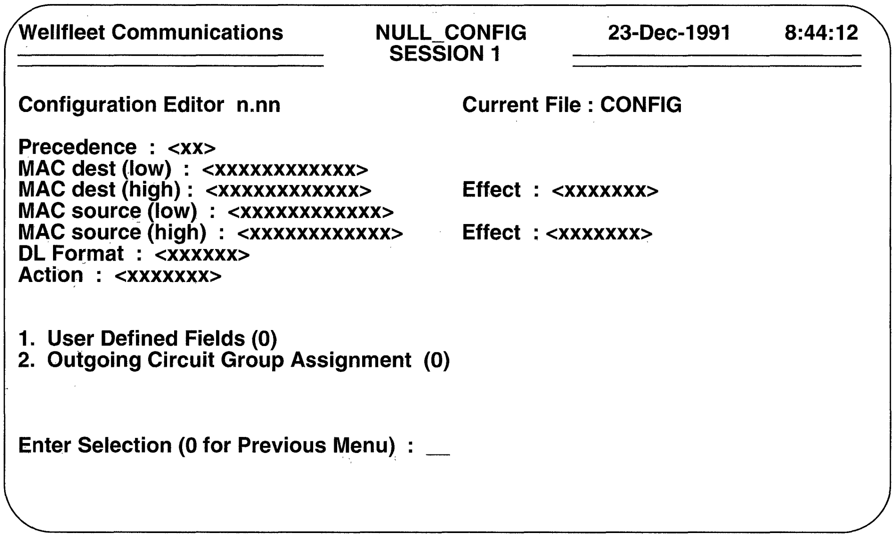
Drop discards a frame that meets the filter rule; **Drop and Log** discards the frame and records an event message in the event log; **Accept** relays a frame that meets the filter rule; **Accept and Log Drop** relays the frame and records an event message in the event log.

NOTE

The **Drop and Log** and **Accept and Log** actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming frames. Consequently, the log actions should generally be used only to record anomalous events.

After you select the required action, press `[RETURN]`.

The screen prompts for additional filtering data as shown in Figure 8-27.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG

Precedence  :  <xx>
MAC dest (low)  :  <xxxxxxxxxxxx>
MAC dest (high) :  <xxxxxxxxxxxx>              Effect  :  <xxxxxxx>
MAC source (low)  :  <xxxxxxxxxxxx>
MAC source (high)  :  <xxxxxxxxxxxx>           Effect  : <xxxxxxx>
DL Format  :  <xxxxxx>
Action  :  <xxxxxxx>


1.  User Defined Fields (0)
2.  Outgoing Circuit Group Assignment  (0)


Enter Selection (0 for Previous Menu)  :  __
```

Figure 8-27 Bridge Filters Detailed Parameters Access Screen

8.11.1.2 Ethernet Filters

Ethernet filters enable you to drop or forward a frame on the basis of its Ethernet type. Ethernet filters can filter Ethernet type values only, or some specified combination of Ethernet type values in conjunction with MAC-level source and destination addresses.

You construct Ethernet filters from the Bridge Filters Basic Parameters Screen. If you are constructing a complex filter (one that includes MAC-level source and destination addresses), proceed as described in Section 8.11.1.1 until the cursor is positioned in the **DL Format** field.

If you are constructing a filter that only examines Ethernet type values, you first set the filter precedence.

❐ **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

You can construct up to 31 filters per bridge interface. The **Precedence** value is used when an in-coming frame meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

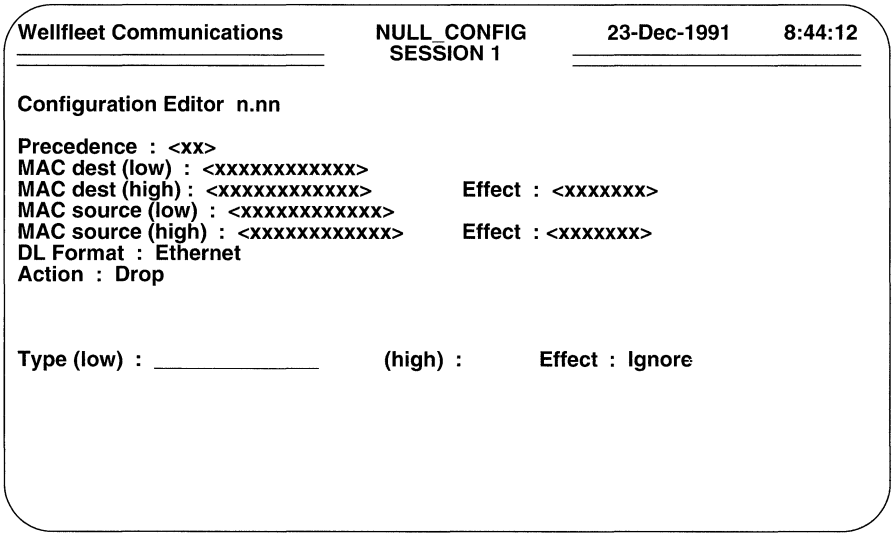
Select a value from 1 to 31 and then press `[RETURN]`.

Now press `[RETURN]` six times (thus ignoring MAC source and destination addresses) to move the cursor to the **DL Format** field.

□ **DL Format** specifies the encapsulation method.

Select **Ethernet**.

After you press `[RETURN]`, the screen displays the Ethernet Filter Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn

Precedence  :  <xx>
MAC dest (low)  :  <xxxxxxxxxxxx>
MAC dest (high) :  <xxxxxxxxxxxx>          Effect  :  <xxxxxxx>
MAC source (low)  :  <xxxxxxxxxxxx>
MAC source (high)  :  <xxxxxxxxxxxx>       Effect  : <xxxxxxx>
DL Format  :  Ethernet
Action  :  Drop


Type (low)  :  ____________        (high)  :        Effect  :  Ignore
```

Figure 8-28 Ethernet Filter Parameters Screen

□ **Type (low)** specifies the lower boundary range of filtered Ethernet type values.

To filter Ethernet types, do one of the following:

- enter the name of a Ethernet Type list
- enter an Ethernet type at the lower boundary of the type range that you want to filter
- enter a single Ethernet type that you want to filter

After you enter an Ethernet type or a list name, press `[RETURN]`.

□ **(high)** specifies the upper boundary range of filtered Ethernet type values.

To filter Ethernet type values, do one of the following:

- if you entered the name of an Ethernet Type list at **Type (low)**, or if you want to filter the single Ethernet type entered at **Type (low)**, press `[RETURN]`.

- if you entered a lower boundary range value at **Type (low)**, enter an Ethernet type at the upper boundary of the type range that you want to filter and then press `[RETURN]`.

❒ **Effect** designates one of three operators applied to the Ethernet type pattern specified by **Type (low)** and **(high)**.

If the filter does not care about Ethernet type values, press `[RETURN]` to accept the default, **Ignore**.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Type (low)** and **(high)** includes the Ethernet type of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Type (low)** and **(high)** does not include the Ethernet Type of the frame.

Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

❒ **Action** specifies the disposition of frames that meet the filter rule.

Drop discards a frame that meets the filter rule; **Drop and Log** discards the frame and records an event message in the event log; **Accept** relays a frame that meets the filter rule; **Accept and Log Drop** relays the frame and records an event message in the event log.

NOTE

The **Drop and Log** and **Accept and Log** actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming frames. Consequently, the log actions should generally be used only to record anomalous events.

After you select the required action, press `[RETURN]`.

The screen prompts for additional filtering data as shown in Figure 8-27.

8.11.1.3 802.2 LLC Filters

802.2 LLC filters enable you to drop or forward a frame on the basis of its destination and/or source service access points. 802.2 LLC filters can filter (1) only source service access points (SSAP), (2) only destination service access points (DSAP), (3) some combination of SSAP and DSAP values, or (4) some specified combination of SSAP/ DSAP values in conjunction with MAC-level source and destination addresses.

You construct 802.2 LLC filters from the Bridge Filters Basic Parameters Screen. If you are constructing a complex filter (one that includes MAC-level source and destination addresses), proceed as described in Section 8.11.1.1 until the cursor is positioned in the **DL Format** field.

If you are constructing a filter that only examines 802.2 LLC values, you first set the filter precedence.

❒ **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

You can construct up to 31 filters per bridge interface. The **Precedence** value is used when an in-coming frame meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

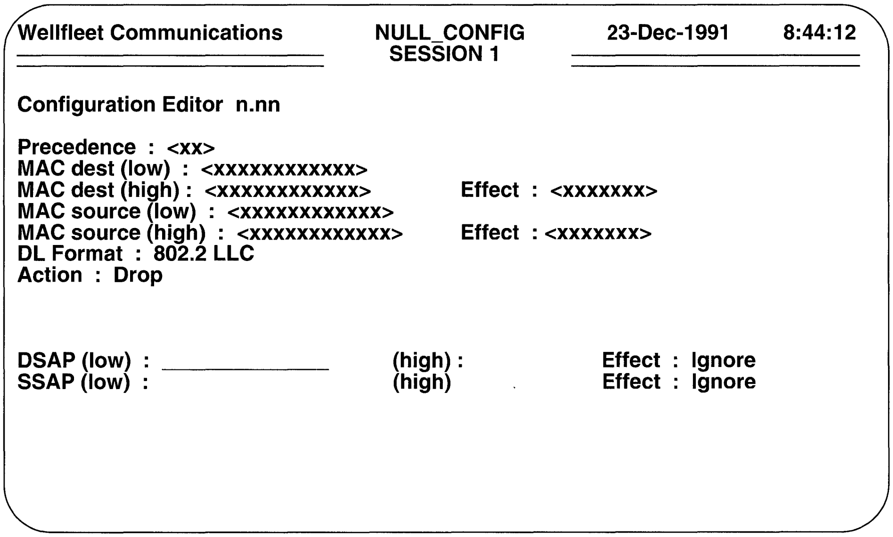
Select a value from 1 to 31 and then press `[RETURN]`.

Now press `[RETURN]` six times (thus ignoring MAC source and destination addresses) to move the cursor to the **DL Format** field.

❒ **DL Format** specifies the encapsulation method.

Select **802.2 LLC**, and then press `[RETURN]`.

After you press `[RETURN]`, the screen displays the 802.2 LLC Filter Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn

Precedence  :  <xx>
MAC dest (low)  :  <xxxxxxxxxxxxx>
MAC dest (high) :  <xxxxxxxxxxxxx>          Effect  :  <xxxxxxx>
MAC source (low)  :  <xxxxxxxxxxxxx>
MAC source (high)  :  <xxxxxxxxxxxxx>       Effect  : <xxxxxxx>
DL Format  :  802.2 LLC
Action  :  Drop


DSAP (low)  :  ______________          (high) :               Effect  :  Ignore
SSAP (low)  :                          (high)                 Effect  :  Ignore
```

Figure 8-29 802.2 LLC Filter Parameters Screen

❒ **DSAP (low)** specifies the lower boundary range of filtered destination service access points.

If you do not want to filter destination service access points, press `[RETURN]`.

To filter destination service access points, do one of the following:

- enter the name of a SAP list
- enter a destination service access point at the lower boundary of the DSAP range that you want to filter
- enter a single destination service access point that you want to filter

After you enter a DSAP value or a list name, press `[RETURN]`.

❒ **(high)** specifies the upper boundary range of filtered destination service access points.

If you do not want to filter destination service access points, press `[RETURN]`.

To filter destination service access points, do one of the following:

- if you entered the name of an SAP list at **DSAP (low)**, or if you want to filter the single destination service access point entered at **DSAP (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **DSAP (low)**, enter a destination service access point at the upper boundary of the range that you want to filter and then press `[RETURN]`.

❒ **Effect** designates one of three operators applied to the destination service access point pattern specified by **DSAP (low)** and **(high)**.

If the filter does not care about destination service access point values, press `[RETURN]` to accept the default, **Ignore**.

To filter destination service access points, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **DSAP (low)** and **(high)** includes the destination service access point of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **DSAP (low)** and **(high)** does not include the destination service access point of the frame.

Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

❒ **SSAP (low)** specifies the lower boundary range of filtered source service access points.

If you do not want to filter source service access points, press `[RETURN]`.

To filter source service access points, do one of the following:

- enter the name of a SAP list
- enter a source service access point at the lower boundary of the SSAP range that you want to filter
- enter a single source service access point that you want to filter

After you enter a SSAP value or a list name, press `[RETURN]`.

❒ **(high)** specifies the upper boundary range of filtered source service access points.

If you do not want to filter source service access points, press `[RETURN]`.

To filter source service access points, do one of the following:

- if you entered the name of an SAP list at **SSAP (low)**, or if you want to filter the single source service access point entered at **SSAP (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **SSAP (low)**, enter a source service access point at the upper boundary of the range that you want to filter and then press `[RETURN]`.

❒ **Effect** designates one of three operators applied to the source service access point pattern specified by **SSAP (low)** and **(high)**.

If the filter does not care about source service access point values, press `[RETURN]` to accept the default, **Ignore**.

To filter source service access points, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **SSAP (low)** and **(high)** includes the source service access point of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **SSAP (low)** and **(high)** does not include the source service access point of the frame.

Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

❒ **Action** specifies the disposition of frames that meet the filter rule.

Drop discards a frame that meets the filter rule; **Drop and Log** discards the frame and records an event message in the event log; **Accept** relays a frame that meets the filter rule; **Accept and Log Drop** relays the frame and records an event message in the event log.

NOTE

The **Drop and Log** and **Accept and Log** actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming frames. Consequently, the log actions should generally be used only to record anomalous events.

After you select the required action, press `[RETURN]`.

The screen prompts for additional filtering data as shown in Figure 8-27.

8.11.1.4 802.2 SNAP Filters

802.2 SNAP filters enable you to drop or forward a frame on the basis of its protocol or Ethernet type. 802.2 SNAP filters can filter (1) only protocol ID values, (2) only Ethernet type values, (3) some combination of protocol ID and Ethernet type values, or (4) some specified combination of protocol ID/Ethernet type values in conjunction with MAC-level source and destination addresses.

You construct 802.2 SNAP filters from the Bridge Filters Basic Parameters Screen. If you are constructing a complex filter (one that includes MAC-level source and destination addresses), proceed as described in Section 8.11.1.1 until the cursor is positioned in the **DL Format** field.

If you are constructing a filter that only examines 802.2 SNAP values, you first set the filter precedence.

❐ **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

You can construct up to 31 filters per bridge interface. The **Precedence** value is used when an in-coming frame meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

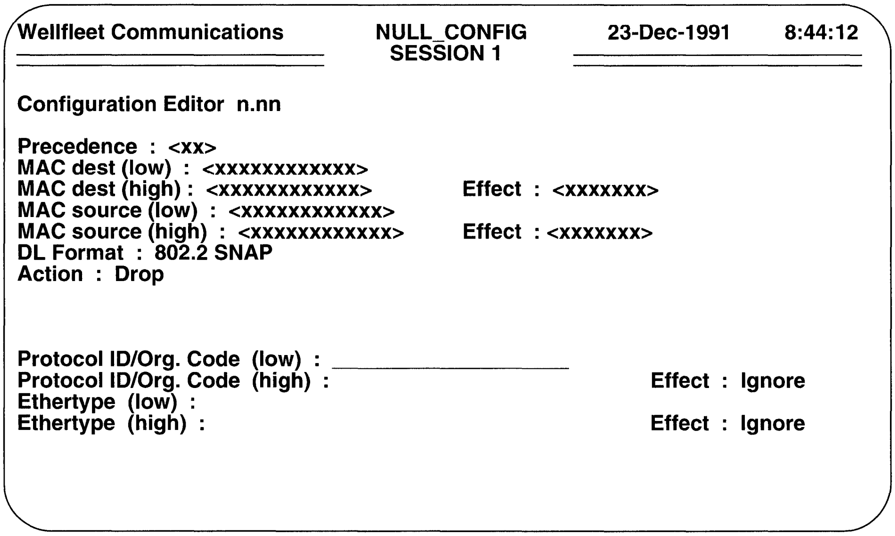
Select a value from 1 to 31 and then press `[RETURN]`.

Now press `[RETURN]` six times (thus ignoring MAC source and destination addresses) to move the cursor to the **DL Format** field.

❐ **DL Format** specifies the encapsulation method.

Select **802.2 SNAP**, and then press `[RETURN]`.

After you press `[RETURN]`, the screen displays the SNAP Filter Parameters Screen (Figure 8-30).



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn

Precedence  :  <xx>
MAC dest (low)  :  <xxxxxxxxxxxx>
MAC dest (high) :  <xxxxxxxxxxxx>          Effect  :  <xxxxxxx>
MAC source (low)  :  <xxxxxxxxxxxx>
MAC source (high)  :  <xxxxxxxxxxxx>       Effect  : <xxxxxxx>
DL Format  :  802.2 SNAP
Action  :  Drop


Protocol ID/Org. Code  (low)  : ___________________
Protocol ID/Org. Code  (high)  :                           Effect  :  Ignore
Ethertype  (low)  :
Ethertype  (high)  :                                       Effect  :  Ignore
```

Figure 8-30 802.2 SNAP Filter Parameters Screen

❒ **Protocol ID/Org. Code (low)** specifies the lower boundary range of the protocol ID.

If you do not want to filter protocol IDs, press `[RETURN]`.

To filter protocol IDs, do one of the following:

- enter the name of a Protocol ID list
- enter a protocol ID at the lower boundary of the ID range that you want to filter
- enter a single protocol Id that you want to filter

After you enter a protocol ID value or a list name, press `[RETURN]`.

❒ **Protocol ID/Org. Code (high)** specifies the upper boundary range of the protocol ID.

If you do not want to filter protocol IDs, press `[RETURN]`.

To filter protocol IDs, do one of the following:

- if you entered the name of a Protocol ID list at **Protocol ID/Org. Code (low)**, or if you want to filter the single protocol ID entered at **Protocol ID/Org. Code (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **Protocol ID/Org. Code (low)**, enter a protocol ID at the upper boundary of the range that you want to filter and then press `[RETURN]`.

❐ **Effect** designates one of three operators applied to the protocol ID pattern specified by **Protocol ID/Org. Code (low)** and **Protocol ID/Org. Code (high)**.

If the filter does not care about protocol ID values, press `[RETURN]` to accept the default, **Ignore**.

To filter protocol IDs, you choose between the **Match** and **Don't Match** operators.

To filter source service access points, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Protocol ID/Org. Code (low)** and **Protocol ID/ Org. Code (high)** includes the protocol ID of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Protocol ID/Org. Code (low)** and **Protocol ID/ Org. Code (high)** does not include the protocol ID of the frame.

Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

❐ **Ethertype (low)** specifies the lower boundary range of the Ethernet type.

If you do not want to filter Ethernet types, press `[RETURN]`.

To filter Ethernet types, do one of the following:

- enter the name of an Ethernet Type list
- enter an Ethernet type at the lower boundary of the type range that you want to filter
- enter a single Ethernet type that you want to filter

After you enter an Ethernet type value or a list name, press `[RETURN]`.

❐ **Ethertype (high)** specifies the upper boundary range of the Ethernet type.

If you do not want to filter Ethernet types, press `[RETURN]`.

To filter Ethernet types, do one of the following:

- if you entered the name of an Ethernet Type list at **Ethernet (low)**, or if you want to filter the single Ethernet type entered at **Ethernet (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **Ethernet (low)**, enter an Ethernet type at the upper boundary of the range that you want to filter and then press `[RETURN]`.

❐ **Effect** designates one of three operators applied to the Ethernet type pattern specified by **Ethertype (low)** and **Ethertype (high)**.

If the filter does not care about Ethernet type values, press `[RETURN]` to accept the default, **Ignore**.

To filter Ethernet types, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Ethernet (low)** and **Ethernet (high)** includes the Ethernet type of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Ethernet (low)** and **Ethernet (high)** does not include the Ethernet type of the frame.

Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

❐ **Action** specifies the disposition of frames that meet the filter rule.

Drop discards a frame that meets the filter rule; **Drop and Log** discards the frame and records an event message in the event log; **Accept** relays a frame that meets the filter rule; **Accept and Log Drop** relays the frame and records an event message in the event log.

NOTE

The **Drop and Log** and **Accept and Log** actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming frames. Consequently, the log actions should generally be used only to record anomalous events.

After you select the required action, press `[RETURN]`.

The screen prompts for additional filtering data as shown in Figure 8-27.

8.11.1.5 Novell Filters

Novell filters enable you to drop or forward Novell frames. You can, if you wish, construct such filters to examine Novell-encapsulated frames in conjunction with MAC-level source and destination addresses.

You construct Novell filters from the Bridge Filters Basic Parameters Screen. If you are constructing a complex filter (one that includes MAC-level source and destination addresses), proceed as described in Section 8.11.1.1 until the cursor is positioned in the **DL Format** field.

If you are constructing a Novell-only filter, you first set the filter precedence.

- ❒ **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

  You can construct up to 31 filters per bridge interface. The **Precedence** value is used when an in-coming frame meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

  Select a value from 1 to 31 and then press `[RETURN]`.

Now press `[RETURN]` six times (thus ignoring MAC source and destination addresses) to move the cursor to the **DL Format** field.

- ❒ **DL Format** specifies the encapsulation method.

  Select **Novell**, and then press `[RETURN]`.

- ❒ **Action** specifies the disposition of frames that meet the filter rule.

  Drop discards a frame that meets the filter rule; **Drop and Log** discards the frame and records an event message in the event log; **Accept** relays a frame that meets the filter rule; **Accept and Log Drop** relays the frame and records an event message in the event log.

NOTE

The **Drop and Log** and **Accept and Log** actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming frames. Consequently, the log actions should generally be used only to record anomalous events.

After you select the required action, press `[RETURN]`.

The screen prompts for additional filtering data as shown in Figure 8-27.

8.11.1.6 User-Defined Filters

In contrast with the pre-defined filters described in Sections 8.11.1.1 through 8.11.1.5, user-defined filters enable you to filter traffic based upon a specified bit pattern(s) contained within either the MAC or data-link header. User-defined filters can be used in conjunction with any pre-defined filters.

You construct user-defined filters from the Bridge Filters Basic Parameters Screen. If you are constructing a complex filter (one that includes any of the pre-defined filter types), proceed as described in Sections 8.11.1.1 through 8.11.1.5 until the cursor is positioned in the **Action** field.

If you are constructing a filter that only examines user-defined values, you first set the filter precedence.

- ❒ **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

  You can construct up to 31 filters per bridge interface. The **Precedence** value is used when an in-coming frame meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

  Select a value from 1 to 31 and then press `[RETURN]`.

Now press `[RETURN]` seven times (thus ignoring MAC source and destination addresses and the data-link format) to move the cursor to the **Action** field.

- ❒ **Action** specifies the disposition of frames that meet the filter rule.

  Drop discards a frame that meets the filter rule; **Drop and Log** discards the frame and records an event message in the event log; **Accept** relays a frame that meets the filter rule; **Accept and Log Drop** relays the frame and records an event message in the event log.

NOTE

The **Drop and Log** and **Accept and Log** actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming frames. Consequently, the log actions should generally be used only to record anomalous events.

After you select the required action, press `[RETURN]`.

The console screen prompts for additional filtering data as shown in Figure 8-27. To continue constructing a user-defined filter, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No User Defined Fields record(s) found
Do you wish to add User Defined Fields record(s)?

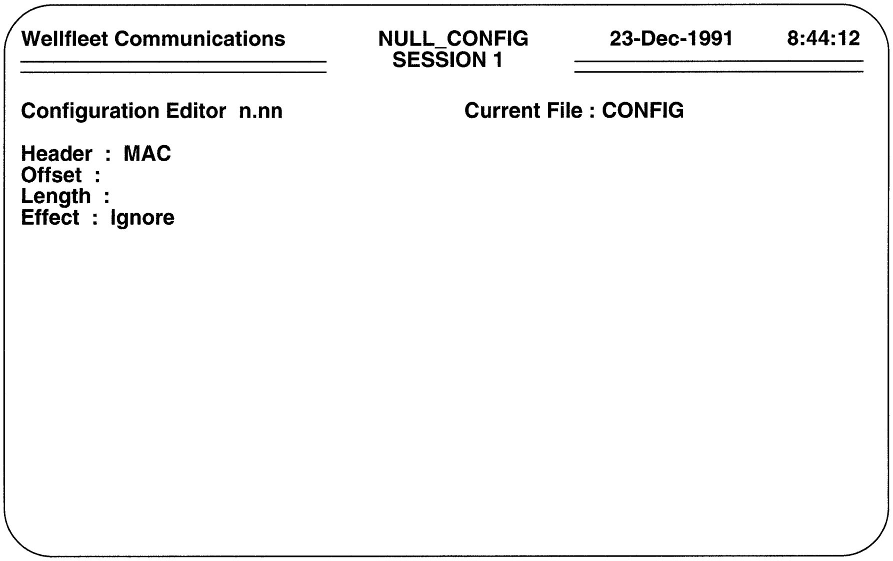
Press `[RETURN]` to display the User-Defined Filter Parameters Screen (Figure 8-31).

- ❒ **Header** positions the filtered bit pattern within the incoming frame.

  If the filtered bit pattern is found within the MAC-level header, press `[RETURN]` to accept the default response, **MAC**. If the pattern is found within the data-link header, press the `[RIGHTARROW]` to display **Data Link** and press `[RETURN]`.

- ❒ **Offset** positions the filtered bit pattern within either the MAC-level or data-link-level header.

  The first (most significant) bit of either the MAC-level or data-link-level header is referenced as bit 0. Enter the starting location of the filtered bit pattern with reference to the most significant bit of the header and then press `[RETURN]`.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn              Current File : CONFIG

Header  :  MAC
Offset  :
Length  :
Effect  :  Ignore
```

Figure 8-31 User-Defined Filter Parameters Screen

For example, an Ethernet multicast address is designated by setting the lowest-order bit in the highest-order byte of the Ethernet address. Consequently, the following are valid Ethernet multicast addresses: 010000009999, 0F0000009999. To filter multicast addresses, you would examine the multicast bit by entering 7 at **Offset**.

❒ **Length** specifies the bit length of the filtered field.

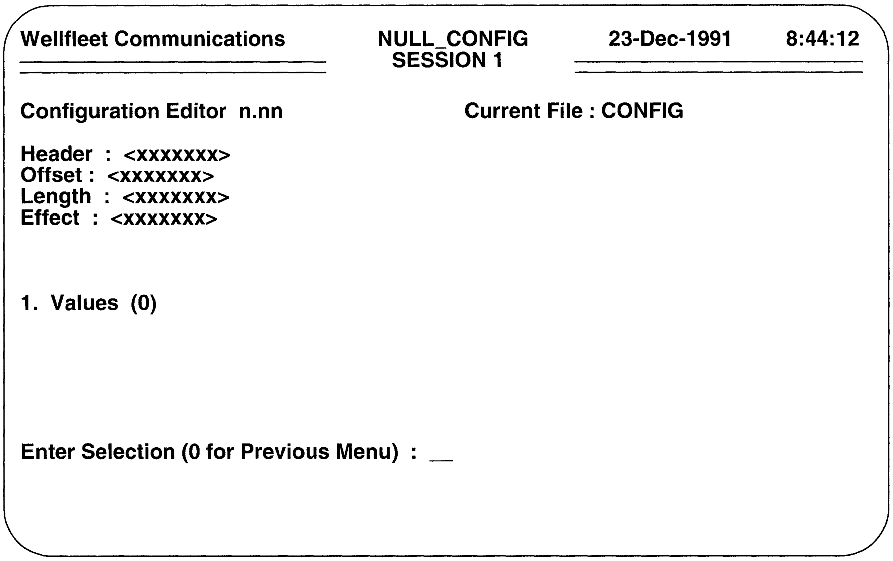
Enter the field length, and then press `[RETURN]`.

❒ **Effect** designates the operator applied to the user-defined pattern.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **Header**, **Offset,** and **Length** matches the contents of the frame.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Header**, **Offset,** and **Length** does not match the contents of the frame.

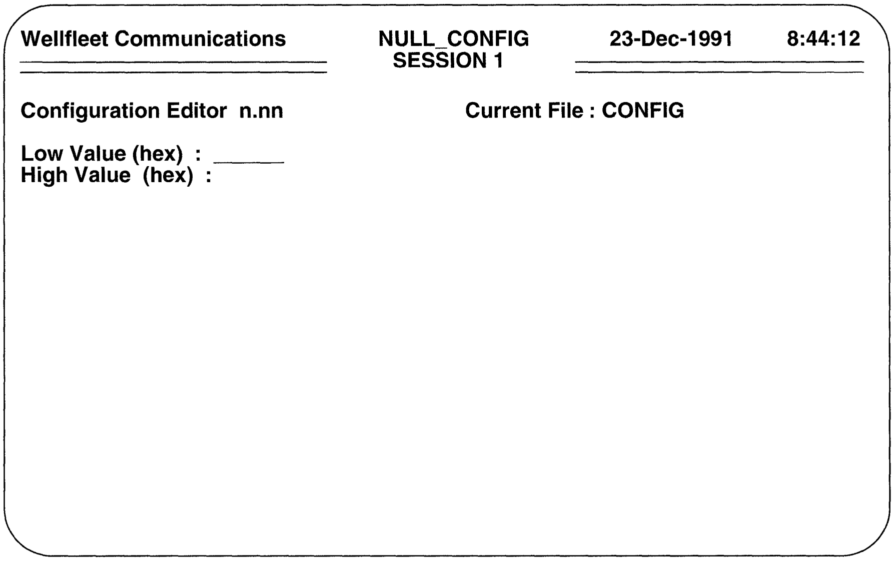
Press the `[RIGHTARROW]` to select the operator, and then press `[RETURN]`.

The screen then prompts for a value to associate with the bit field described by **Offset** and **Length** (Figure 8-32).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                    SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG

Header  :  <xxxxxxxx>
Offset :  <xxxxxxxx>
Length  :  <xxxxxxxx>
Effect  :  <xxxxxxxx>


1.  Values  (0)




Enter Selection (0 for Previous Menu)  :  __
```

Figure 8-32 User-Defined Filter Values Access Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                    SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG

Low Value (hex)  :  ______
High Value  (hex)  :
```

Figure 8-33 User-Defined Filter Values Screen

To specify a value, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The console screen prompts for a range of values as shown in Figure 8-33.

- ❒ **Low Value (hex)** specifies the lower boundary range of the user-defined pattern.

  To filter user-defined values, do one of the following:

  - enter a hexadecimal value at the lower boundary of the user-defined range that you want to filter
  - enter a single hexadecimal value that you want to filter

  After you enter a value, press `[RETURN]`.

- ❒ **High Value (hex)** specifies the upper boundary range of the user-defined pattern.

  To filter user-defined values, do one of the following:

  - if you entered a lower boundary range value at **Low Value (hex)**, enter an upper boundary of the user-defined range that you want to filter and then press `[RETURN]`.
  - if you want to filter the single value entered at **Low Value (hex)**, press `[RETURN]`.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to revert to the Bridge Filters Detailed Parameters Access Screen.

8.11.1.7 Forwarding Filtered Traffic

Traffic that is forwarded as a result of filtering is generally treated as any other traffic. Frames destined for known destinations are directed to a bridge port "in the direction" of the destination, while frames for unknown destinations are flooded to all interfaces. You can arrange, however, to direct filtered traffic to specific interfaces.

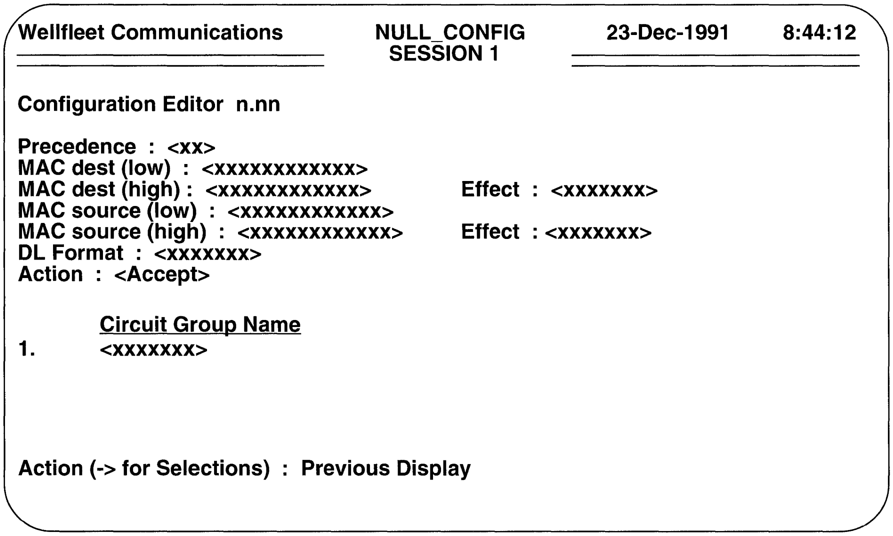
You direct filtered traffic to a specific interface from the Bridge Filters Detailed Parameters Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Outgoing Circuit Group Assignment record(s) found
Do you wish to add Outgoing Circuit Group Assignment record(s)?

Press `[RETURN]`. The screen prompts for a circuit group name.

At **Circuit Group Name** enter the name of the circuit group that provides the outbound path for filtered traffic, and then press `[RETURN]`. When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Bridge Filters Detailed Parameters Access Screen.

You can, if you wish, specify that filtered traffic be directed to more than one interface (for example, to support multicast addressing). You identify additional interfaces from the Bridge Filters Detailed Parameters Access Screen. Enter `<2>` at the **Enter Selection (0 for Previous Menu)** prompt. The console screen displays the Filter/ Circuit Group Summary Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn

Precedence  :  <xx>
MAC dest (low)  :  <xxxxxxxxxxxx>
MAC dest (high) :  <xxxxxxxxxxxx>          Effect  :  <xxxxxxx>
MAC source (low)  :  <xxxxxxxxxxxx>
MAC source (high)  :  <xxxxxxxxxxxx>       Effect  : <xxxxxxx>
DL Format  :  <xxxxxxx>
Action  :  <Accept>

          Circuit Group Name
1.        <xxxxxxx>



Action (-> for Selections)  :  Previous Display
```

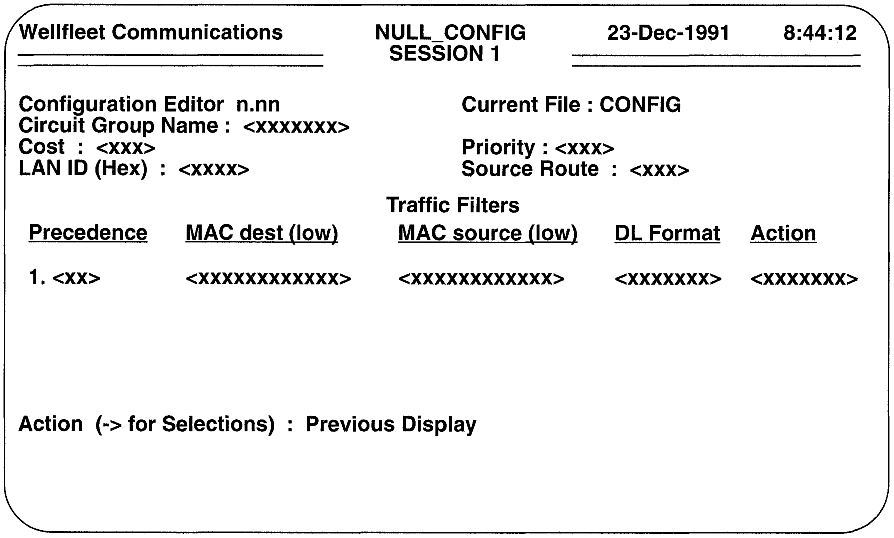
Figure 8-34 Filter/Circuit Group Summary Screen

At **Action (-> for Selections)** press the `[RIGHTARROW]` to display **Add**, and then press `[RETURN]`. At **Circuit Group Name** enter the name of an additional circuit group that provides an outbound path for filtered traffic, and then press `[RETURN]`. When the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the Bridge Filters Detailed Parameters Access Screen. Continue in this manner until you have added all circuit groups to the filter.

8.11.1.8 Construction of Additional Filters

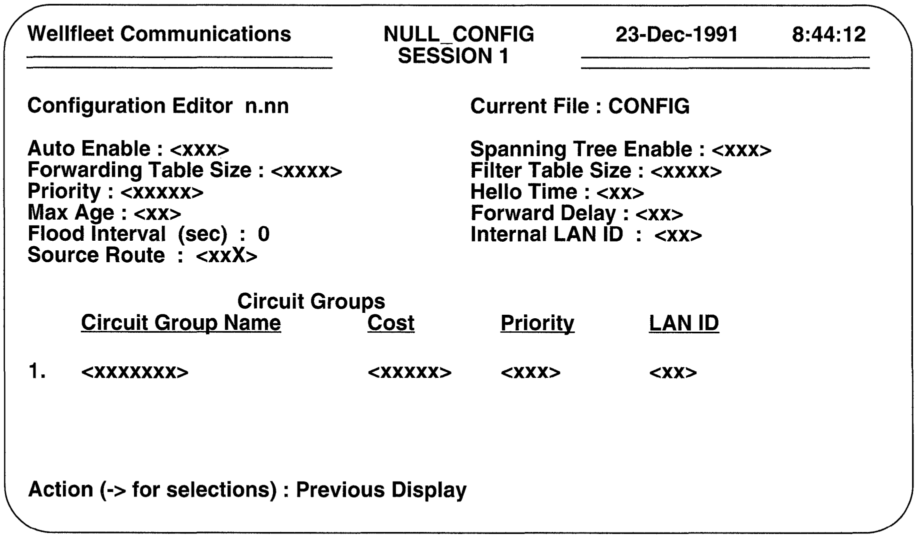
You construct additional filters from the Circuit Group Filter Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the Bridge Filters Summary Screen (Figure 8-35).

At **Action (-> for Selections)** press the `[RIGHTARROW]` to display **Add**, and then press `[RETURN]` to display the Bridge Filters Basic Parameters Screen. Now follow the procedures contained in Sections 8.11.1.1 through 8.11.1.6 to construct additional filters.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Circuit Group Name :  <xxxxxxx>
Cost  :  <xxx>                                Priority : <xxx>
LAN ID (Hex)  :  <xxxx>                       Source Route  :  <xxx>
                                         Traffic Filters
 Precedence   MAC dest (low)     MAC source (low)    DL Format   Action

 1. <xx>      <xxxxxxxxxxxx>     <xxxxxxxxxxxx>      <xxxxxxx>   <xxxxxxx>



Action  (-> for Selections)  :  Previous Display
```

Figure 8-35 Bridge Filters Summary Screen



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG

Auto Enable : <xxx>                           Spanning Tree Enable : <xxx>
Forwarding Table Size : <xxxx>                Filter Table Size : <xxxx>
Priority : <xxxxx>                            Hello Time : <xx>
Max Age : <xx>                                Forward Delay : <xx>
Flood Interval  (sec)  :  0                   Internal LAN ID  :  <xx>
Source Route  :  <xxX>

                        Circuit Groups
     Circuit Group Name          Cost        Priority       LAN ID

1.   <xxxxxxx>                   <xxxxx>     <xxx>          <xx>



Action (-> for selections) : Previous Display
```

Figure 8-36 Bridge Circuit Groups Summary Screen

8.11.2 Designating Additional Circuit Groups

You assign additional bridge circuit groups from the Bridge Configuration Menu. Enter `<2>` at **Enter Selection (0 for Previous Menu)** to display the Bridge Circuit Groups Summary Screen (Figure 8-36).

To designate another circuit group, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Bridge Circuit Group Parameters Screen. Now follow the same procedure as before to designate an additional bridge circuit group; repeat this procedure until you have designated all circuit groups associated with the bridge.

8.11.3 Configuring the Load-Balancing Option

If you wish, you can configure a load-balancing option, which directs specified traffic (identified by a designated Ethernet type field value) to a specified circuit. For example, you can configure all CHAOSNet frames (type field = 0804) to travel over a specific circuit.

Only one load-balancing option can be configured. However, you can assign multiple protocol types and circuits to the load-balancing option.

You configure load-balancing from the Bridge Configuration Menu. Enter `<3>` at **Enter Selection (0 for Previous Menu)**.The screen displays the following prompt:

No Circuit Group Load Balancing record(s) found
Do you wish to add Circuit Group Load Balancing record(s)?

Press `[RETURN]`. The screen prompts for a circuit group name.

At **Circuit Group Name** enter the name of the circuit group over which traffic will be balanced, and then press `[RETURN]`.

The console screen displays the Load-Balancing Definition Screen (Figure 8-37).

Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

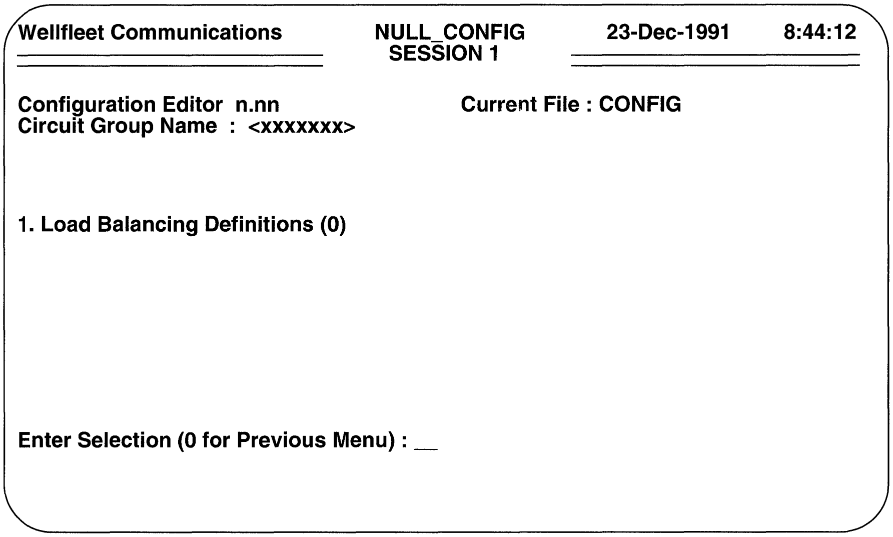
No Load Balancing Definitions record(s) found
Do you wish to add Load Balancing Definitions records?

Press `[RETURN]` to display the Load Balancing Selection Screen (Figure 8-38).

Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

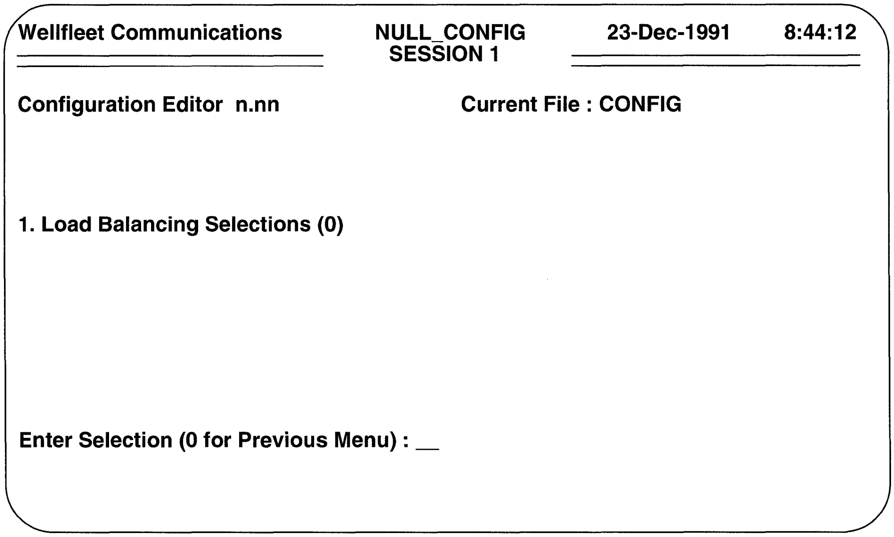
No Load Balancing Selections record(s) found
Do you wish to add Load Balancing Selections records?

Press `[RETURN]` to display the Load Balancing Parameters Screen (Figure 8-39).



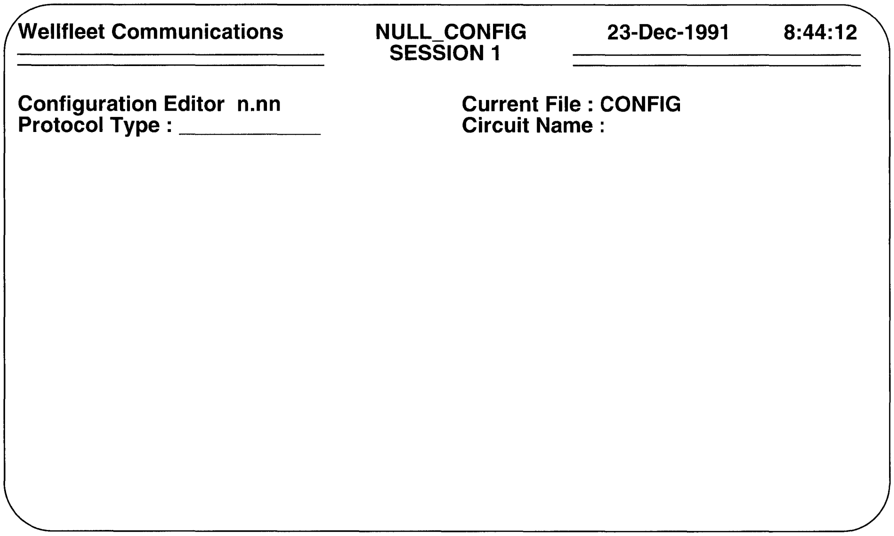
```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Group Name  :  <xxxxxxx>


1. Load Balancing Definitions (0)




Enter Selection (0 for Previous Menu) : __
```

Figure 8-37 Load-Balancing Definition Screen



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG


1. Load Balancing Selections (0)




Enter Selection (0 for Previous Menu) : __
```

Figure 8-38 Load Balancing Selection Screen



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                Current File : CONFIG
Protocol Type : ___________               Circuit Name :
```

Figure 8-39 Load Balancing Parameters Screen

❒ **Protocol Type** identifies the protocol that you wish to filter.

Enter the 12-digit hexadecimal protocol-type value that identifies the protocol that you wish to relay to a specific circuit.

❒ **Circuit Name** identifies the circuit (not circuit group) that carries the traffic specified by **Protocol Type**.

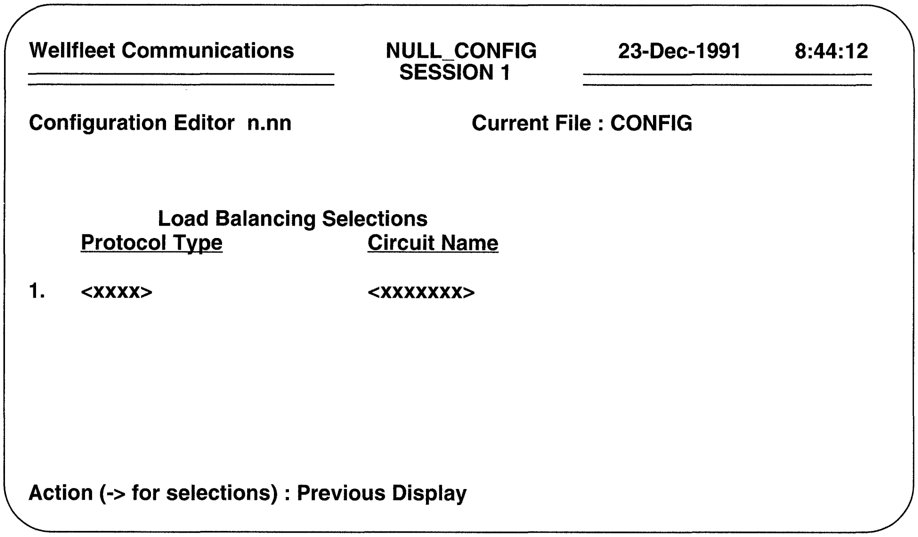
Enter the name of the specific circuit to carry **Protocol Type**-traffic, then press `[RETURN]`. Note that **Circuit Name** will drop any traffic whose type field does not match **Protocol Type**.

After you specify the circuit name, the screen prompts **Hit Return to Continue**. After you press `[RETURN]`, the screen displays the Load-Balancing Selection Screen.

If you want to configure additional load-balancing selections, you can do so from the Load-Balancing Selection Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the Load-Balancing Summary Screen (Figure 8-40).

To add load-balancing selections, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the Load-Balancing Parameters Screen.

Now follow the same steps you did before to configure a load-balancing selection; repeat this process until you have configured all your load-balancing selections.



```
Wellfleet Communications          NULL_CONFIG       23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG



              Load Balancing Selections
     Protocol Type                Circuit Name

1.   <xxxxx>                      <xxxxxxxx>





Action (-> for selections) : Previous Display
```

Figure 8-40 Load-Balancing Summary Screen

9 Configuring TCP/IP

This chapter tells you how to configure TCP/IP.

The TCP/IP implementation fully support the Internet standards listed in Table 9-1. Before attempting to configure TCP/IP functionality, users should acquaint themselves with the contents of appropriate Internet Request for Comments (RFCs).

Table 9-1: Internet Request for Comments

RFC	Specifies	RFC	Specifies
768	User Datagram Protocol (UDP)	1009	Gateway requirements
783	Trivial File transfer Protocol (TFTP)	1042	IP over IEEE 802.x networks
791	Internet Protocol (IP)	1058	Routing Information Protocol (RIP)
792	Internet Control Message Protocol (ICMP)	1063	Maximum Transmission Unit (MTU) discovery option
793	Transmission Control Protocol (TCP)	1084	BOOTP vendor extensions
826	Address Resolution Protocol (ARP)	1131	Open Shortest Path First Protocol (OSPF)
877	IP over X.25 networks	1155	Structure and Identification of Management Information
904	Exterior Gateway Protocol (EGP)	1156	Internet Management Information Base (MIB)
950	Internet sub-netting	1157	Simple Network Management Protocol (SNMP)
951	Bootstrap (BOOTP) Protocol	1188	IP over FDDI networks

9.1 Filtering IP Packets

Filters enable the router to relay or drop a particular frame based on the contents of specific fields within the IP datagram, UDP datagram, or TCP segment headers. Filters examine the following fields either singly or in combination: destination network, source network, destination port, and source port. In addition, IP filtering supports the user-specification of specific fields and bit patterns within IP or upper level protocol headers.

Filtering decisions are based on user-defined rules. An IP filter rule consists of an IP/UDP/TCP field (or fields); a value (or list of values); an operator (*match* or *don't match*) which specifies the relationship between the contents of the field and the value; an action (*drop* or *forward*); and a filter precedence.

For example, IP Filter-rule-A depicted in Figure 9-1 prevents Telnet access from IP address 128.16.4.100 to IP address 192.32.1.65.

IP Filter-rule-B isolates an IP host, 192.32.1.65, probably storing sensitive or confidential access, from all access except from a single host, 128.10.10.10.

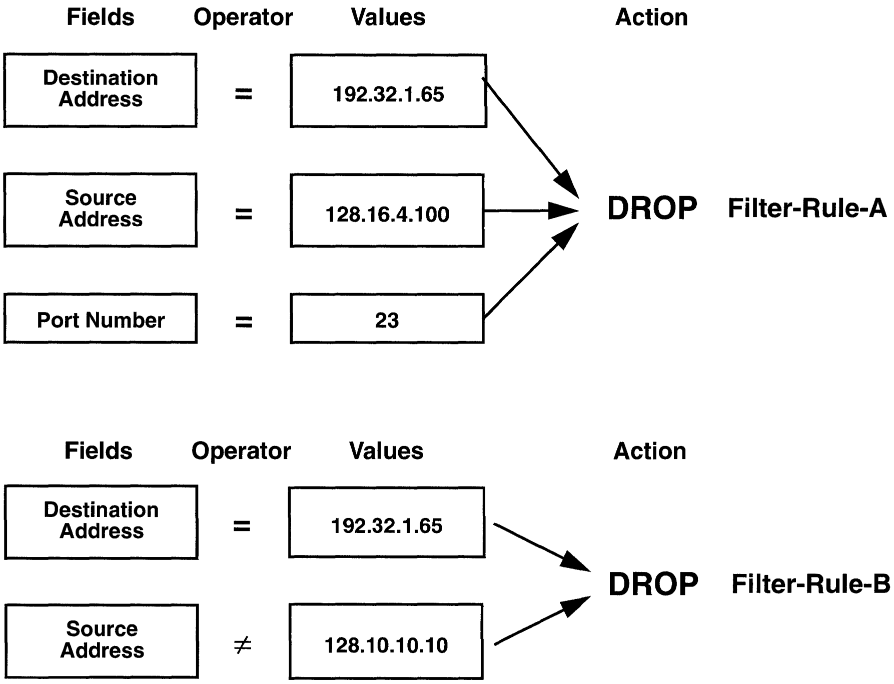


Figure 9-1 IP Sample Filters

9.2 Setting TCP/IP Basic Parameters

To begin TCP/IP configuration, you assign values to the basic parameters listed in Table 9-2.

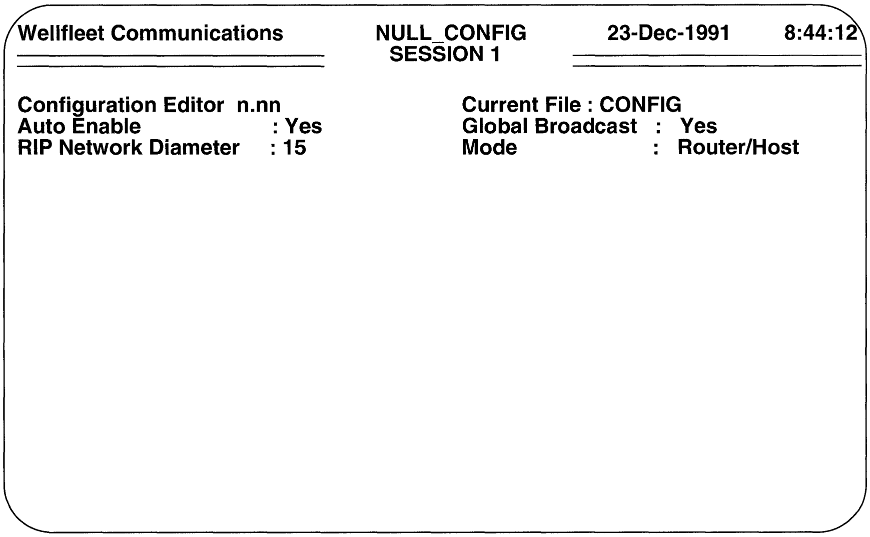
Table 9-2: TCP/IP Basic Parameters

Parameter	Function
Auto Enable	specifies the initialization state
Global Broadcast	specifies response to the receipt of a global broadcast message
RIP Network Diameter	enables/disables “extended” RIP
Mode	enables/disables “end-node” operation

You set basic parameters from the Configuration Menu. At **Enter Selection (0 for Previous Menu)**, enter the number that appears to the left of **DoD Internet Router**. The screen displays the following:

No DoD Internet Router record(s) found
Do you wish to add DoD Internet Router record(s)?

Press `[RETURN]` to display the TCP/IP Basic Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Auto Enable              : Yes              Global Broadcast  :  Yes
RIP Network Diameter     : 15               Mode              :  Router/Host
```

Figure 9-2 TCP/IP Basic Parameters Screen

- ❐ **Auto Enable** specifies the initial state of TCP/IP.

  This TCP/IP-specific **Auto Enable** works in conjunction with the global auto enable parameter (refer to Section 2.1) to enable or disable TCP/IP.

  When global auto enable is **No**, TCP/IP is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable TCP/IP with NCL commands after the router boots.

  When global auto enable is **Yes**, TCP/IP is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable TCP/IP) or **No** (disable TCP/IP), then press `[RETURN]`. If you choose **No**, you will later need to enable TCP/IP with NCL commands after the router boots.

- ❐ **Global Broadcast** determines the response to receipt of a global broadcast message (a message containing an all-1s IP destination address).

  If you select **Yes**, TCP/IP accepts the message; if you select **No**, TCP/IP discards the message.

  Because the RIP protocol uses global broadcast messages to propagate periodic routing updates, you should exercise care before setting this parameter to **No** (and thereby effectively disabling RIP).

- ❐ **RIP Network Diameter** specifies the value, or hop count, used by RIP to denote infinity.

NOTE

It is strongly recommended that you accept the default value (**15**) when setting the **RIP Network Diameter** parameter. Proper operation of the Routing Information Protocol requires that *every* router within the network use the *identical* network diameter value.

If *every* router within the internet can be configured to accept the *identical* number of hops, you can increase the **RIP Network Diameter** value up to a maximum of 127.

Press `[RETURN]` to accept the default value of **15**, or enter a new value (up to a maximum of 127).

- ❐ **Mode** enables the multiprotocol router, acting as a bridge, to receive IP datagrams addressed to it, while continuing to bridge all other IP and non-IP traffic.

  Router/Host selects “router/host” mode of operation in which TCP/IP processes all IP packets explicitly addressed to it, and routes all other IP packets. If you are *not* bridging IP traffic, select this mode.

If you are bridging IP traffic, and wish to provide management access (through Telnet, TFTP, or SNMP) to the multiprotocol router, press the `[RIGHTARROW]` to display **Host Only** and press `[RETURN]` to enable "end-node" operation.

In "end-node" mode the TCP/IP functions as if it were a virtual host on one of the bridged interfaces. For instance, Figure 9-3 shows a multiprotocol router (functioning in "end-node" mode, and with an IP address of 192.32.1.1) bridging traffic for three connected networks.

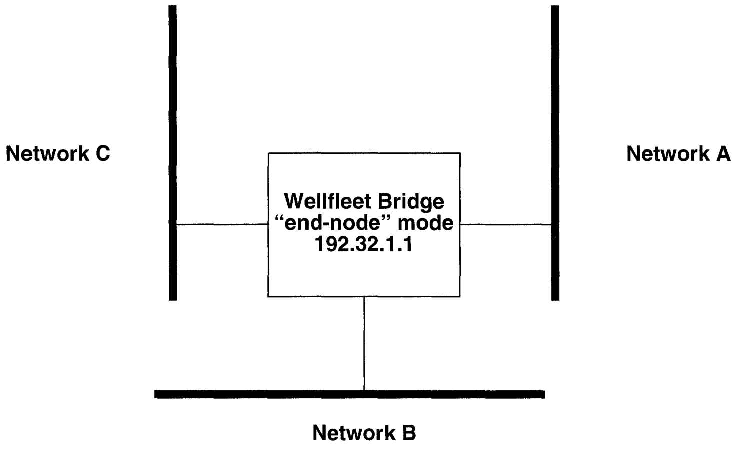


Figure 9-3 "End-node" Operation

The system assigns the virtual host to the first circuit of the first circuit group to which the IP address has been assigned Assuming that all circuit groups contain a single member and that the interface to Network A was initially configured, the virtual host configuration is shown in Figure 9-4.

Traffic relayed from the multiprotocol router to a host on Network A appears only on Network A; traffic sent from the multiprotocol router to a host on Network B, however, appears on both Network B and Network A. Furthermore, if the interface to Network A should become disabled for any reason, the multiprotocol router becomes inaccessible to hosts on any connected network.

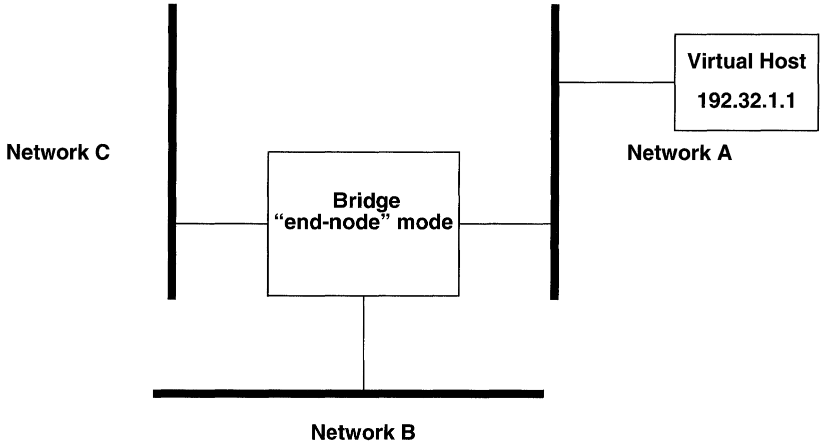


Figure 9-4 Virtual Host Configuration

NOTE

Because no IP routing can take place in "end-node" mode, the Bridge must be configured for each circuit group that conveys IP datagrams. IP datagrams that are not addressed to the multiprotocol router are forwarded by the Bridge.

You must later configure a network interface for each circuit group over which management access is desired. Each interface must specify an identical IP address and mask combination.

After you specify **Mode**, the screen displays the TCP/IP Detailed Parameters Access Screen (Figure 9-5).

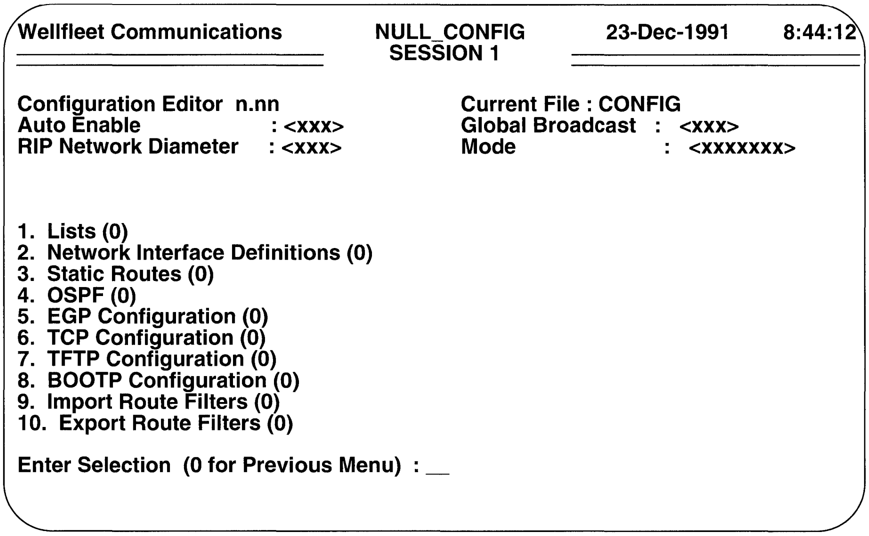
9.3 Compiling IP Filter Lists

Filter lists (while not required) may facilitate the configuration of filters if you wish the filter to apply to non-contiguous value ranges. A list contains a range of values that can be used within a filter rule. A list consists of a symbolic name and a collection of ranges. When a filter specifies a list name, packets are checked against the range of values specified by the list.

You compile lists from the IP Detailed Parameters Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

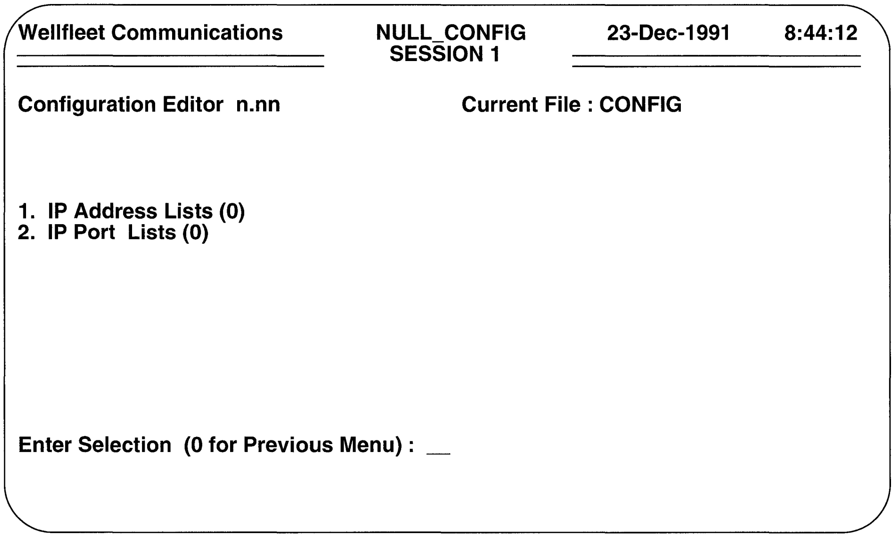
No Lists record(s) found
Do you wish to add Lists record(s)?

Press `[RETURN]` to display the IP List Access Screen (Figure 9-6).



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Auto Enable               : <xxx>              Global Broadcast  :  <xxx>
RIP Network Diameter      : <xxx>              Mode              :  <xxxxxxx>


1.  Lists (0)
2.  Network Interface Definitions (0)
3.  Static Routes (0)
4.  OSPF (0)
5.  EGP Configuration (0)
6.  TCP Configuration (0)
7.  TFTP Configuration (0)
8.  BOOTP Configuration (0)
9.  Import Route Filters (0)
10.  Export Route Filters (0)

Enter Selection  (0 for Previous Menu)  : __
```

Figure 9-5 TCP/IP Detailed Parameters Access Screen



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG


1.  IP Address Lists (0)
2.  IP Port  Lists (0)


Enter Selection  (0 for Previous Menu) :  __
```

Figure 9-6 IP List Access Screen

9.3.1 Address Lists

Address lists specify ranges of IP network addresses.

You compile an address list from the IP List Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

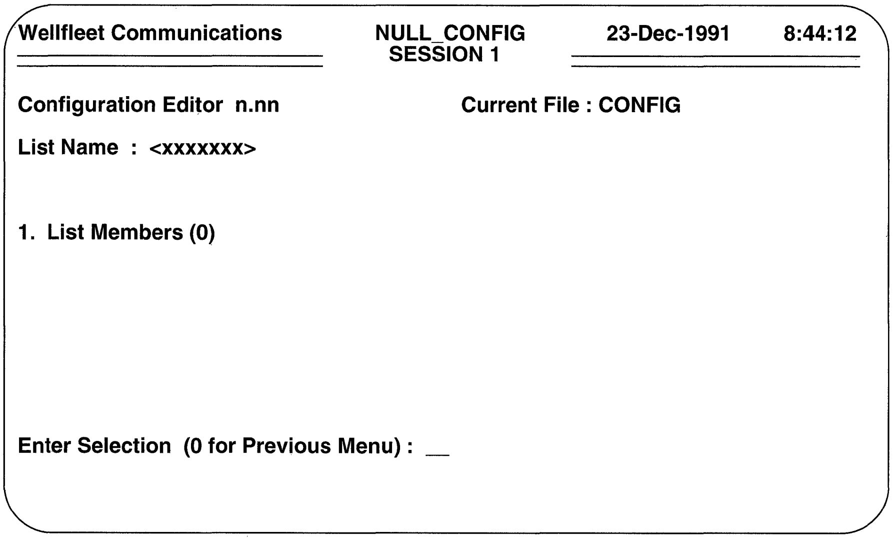
> **No IP Address Lists record(s) found**
> **Do you wish to add IP Address Lists record(s)?**

Press `[RETURN]`. The screen prompts for a **List Name**.

- ❐ **List Name** identifies the IP address list.

  Enter a list name.

After you name the address list, the screen prompts for list members.



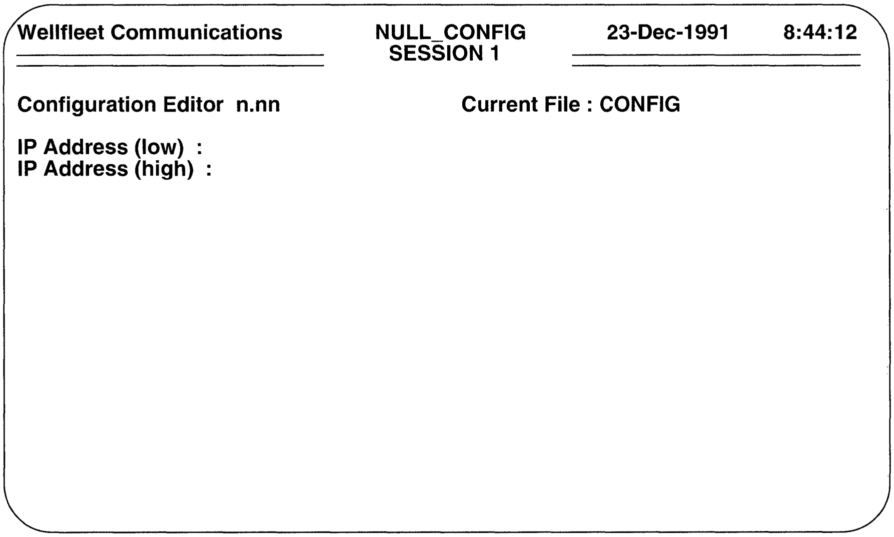
```
Wellfleet Communications        NULL_CONFIG      23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn               Current File : CONFIG

List Name  :  <xxxxxxxx>


1.  List Members (0)







Enter Selection  (0 for Previous Menu) :  __
```

Figure 9-7 IP List Member Access Screen

To assign a range of IP addresses to the list, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen prompts:

> **No List Members record(s) found**
> **Do you wish to add List Members record(s)?**

Press `[RETURN]` to display the IP Address Range Screen (Figure 9-8).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn               Current File : CONFIG

IP Address (low)  :
IP Address (high)  :
```

Figure 9-8 IP Address Range Screen

- ❒ **IP Address (low)** specifies the lower boundary of the IP address range.

  Enter an IP address in dotted decimal notation.

- ❒ **IP Address (high)** specifies the upper boundary of the filtered IP address range.

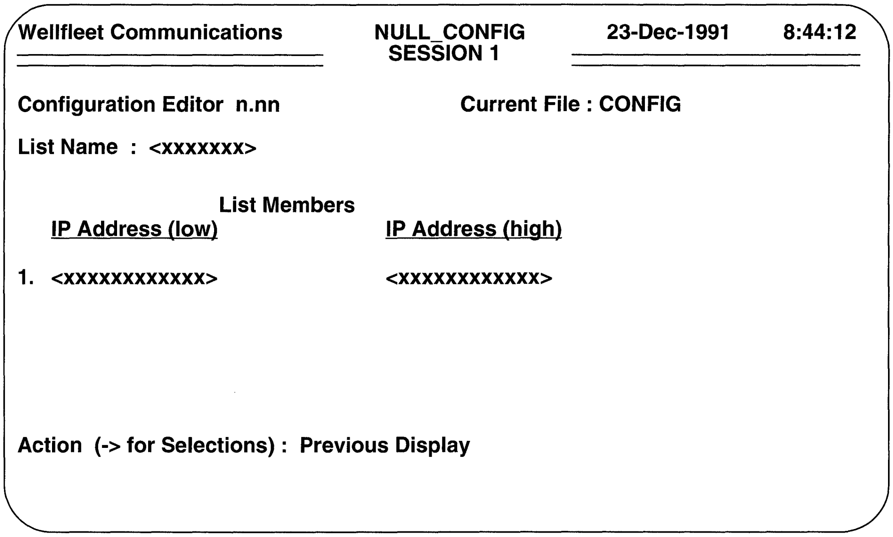
  Enter an IP address, and then press `[RETURN]`. If you want the list range to consist of a single value, that entered in response to the **IP Address (low)** parameter, press `[RETURN]`.

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the IP List Member Access Screen.

If you want, you can add other address ranges to the list. To add an additional range, enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the IP Address List Members Screen (Figure 9-9).

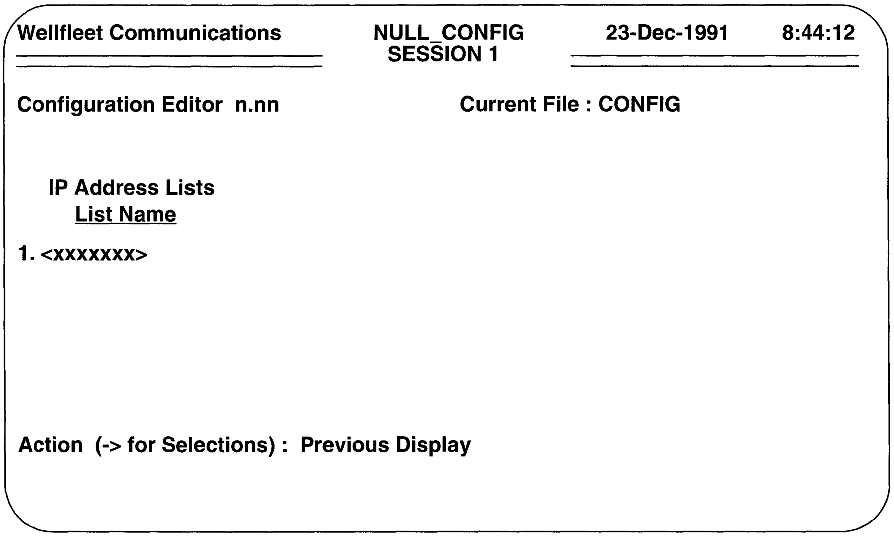
To add another range of IP addresses press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the IP Address Range Screen. Now follow the same procedure as before to add another address range; continue in this fashion until you have added all desired ranges to the list.

You construct additional address lists from the IP List Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the IP Address List Summary Screen (Figure 9-10).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                        Current File : CONFIG

List Name  :  <xxxxxxx>

                           List Members
   IP Address (low)                         IP Address (high)

1.  <xxxxxxxxxxxx>                          <xxxxxxxxxxxx>




Action  (-> for Selections) :  Previous Display
```

Figure 9-9 IP Address List Members Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                        Current File : CONFIG


   IP Address Lists
      List Name

1. <xxxxxxx>




Action  (-> for Selections) :  Previous Display
```

Figure 9-10 IP Address List Summary Screen

To compile another address list, press the [RIGHTARROW] to display **Add**, then press [RETURN]. Now follow the previously described procedure to compile an additional network number list; repeat this procedure until you have compiled all address lists.

9.3.2 Port Lists

Port lists specify ranges of IP port numbers.

The User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are internet transport-level protocols. TCP provides a reliable, connection-mode while UDP provides connectionless, datagram service. UDP datagrams and TCP segments are originated by and addressed to ports. Ports are logical abstractions used by transport-level protocols to distinguish between multiple sources and destinations at a single host.

In order to facilitate application-to-application data flow, the Internet has assigned *well-known port numbers* to certain commonly-used application programs. Examples of well-known port numbers include port numbers assigned to remote-login (TELNET) programs, to file-transfer programs, and to remote-job-entry (RJE) programs.

Table 9-3 lists well-known port numbers used by UDP and TCP.

You construct a port list from the IP List Access Screen. Enter <2> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No IP Port Lists record(s) found
Do you wish to add IP Port Lists record(s)?

Press [RETURN]. The screen prompts for a **List Name**.

❒ **List Name** identifies the port list.

Enter a list name.

After you name the port list, the screen prompts for list members.

To assign a range of port numbers to the list, enter <1> at **Enter Selection (0 for Previous Menu)**. The screen prompts:

No List Members record(s) found
Do you wish to add List Members record(s)?

Press [RETURN] to display the IP Port Range Screen (Figure 9-11).

❒ **IP Port (low)** specifies the lower boundary of the port range.

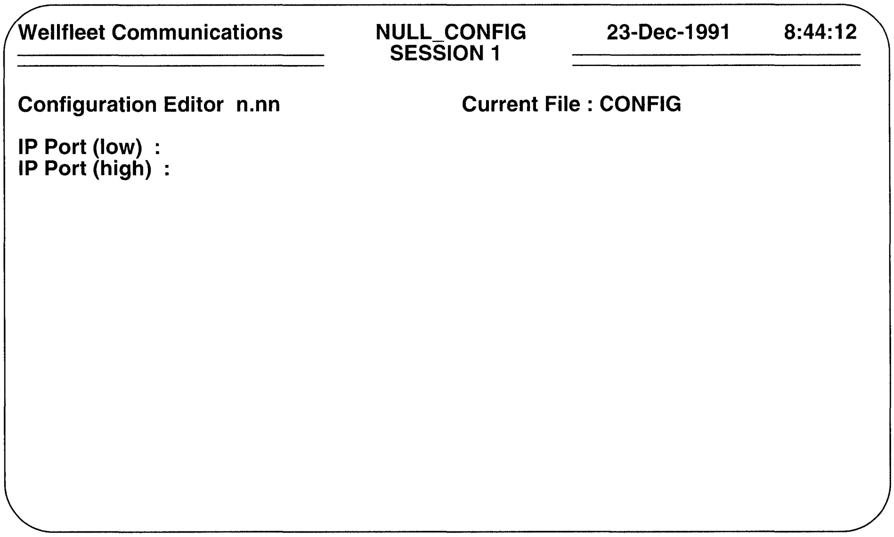
Enter an IP port number.

❒ **IP Port (high)** specifies the upper boundary of the port range.

Enter an IP port number, and then press [RETURN]. If you want the list range to consist of a single value, that entered in response to the **IP Port (low)** parameter, press [RETURN].

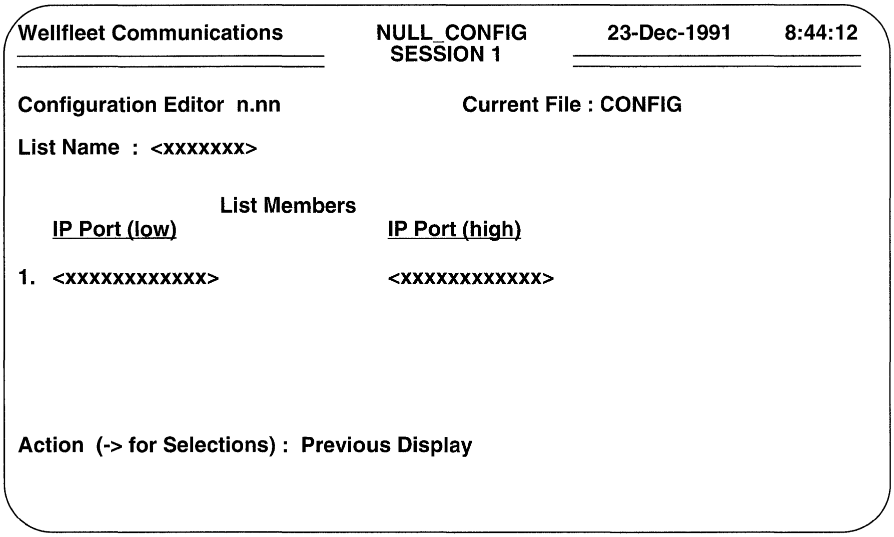
Table 9-3: TCP & UDP Well Known Port Numbers

Port	Protocol	Usage	Port	Protocol	Usage
0	reserved	--	42	NAMESERVER	TCP & UDP
1	unassigned	--	43	NICNAME	TCP & UDP
2	unassigned	--	53	DOMAIN	TCP & UDP
3	unassigned	--	67	BOOTPS	TCP & UDP
4	unassigned	--	68	BOOTPC	TCP & UDP
5	RJE	TCP & UDP	69	TFTP	TCP & UDP
7	ECHO	TCP & UDP	75	private dial	TCP & UDP
9	DISCARD	TCP & UDP	77	private RJE	TCP & UDP
11	USERS	TCP & UDP	79	FINGER	TCP & UDP
13	DAYTIME	TCP & UDP	95	SUPDUP	TCP
15	NETSTAT	TCP & UDP	101	HOSTNAME	TCP
17	QUOTE	TCP & UDP	102	ISO-TSAP	TCP
19	CHARGEN	TCP & UDP	113	AUTH	TCP
20	FTP-DATA	TCP	117	UUCP-PATH	TCP
21	FTP	TCP	123	NTP	TCP & UDP
23	TELNET	TCP	133-159	unassigned	--
25	SMTP	TCP	160-223	reserved	--
37	TIME	TCP & UDP	224-241	unassigned	--
39	RLP	TCP & UDP	247-255	unassigned	--



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

IP Port (low)  :
IP Port (high)  :
```

Figure 9-11 IP Port Range Screen



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

List Name  :  <xxxxxxx>

                       List Members
   IP Port (low)                        IP Port (high)

1.  <xxxxxxxxxxxx>                      <xxxxxxxxxxxx>




Action  (-> for Selections) :  Previous Display
```

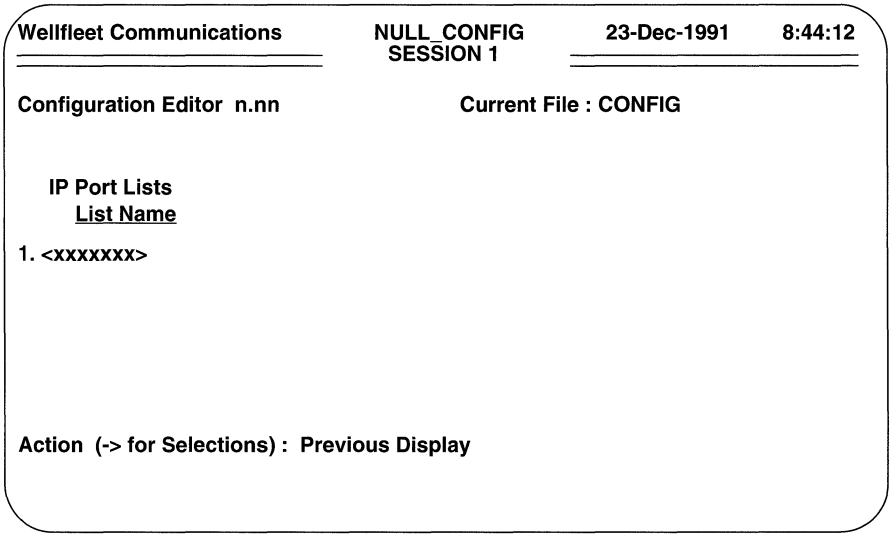
Figure 9-12 IP Port List Members Screen

After you specify the upper boundary, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the IP List Member Access Screen.

If you want, you can add other port numbers to the list. To add an additional range, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt to display the IP Port List Members Screen (Figure 9-12).

To add another range of ports press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`. The screen displays the IP Port Range Screen. Now follow the same procedure as before to add another port range; continue in this fashion until you have added all desired ranges to the list.

You compile additional port lists from the IP List Access Screen. To begin, enter `<2>` at **Enter Selection (0 for Previous Menu)** to display the IP Port List Summary Screen. To compile another port list, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. Now follow the previously described procedure to compile an additional port list; repeat this procedure until you have compiled all port lists.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991    8:44:12
                                 SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG


   IP Port Lists
      List Name

1. <xxxxxxx>






Action  (-> for Selections) :  Previous Display
```

Figure 9-13 IP Port List Summary Screen

9.4 Defining an IP Network Interface

Depending on the complexity of your network topology, the IP router is connected to at least two -- and in most instances, more than two -- TCP/IP networks. Each connection (circuit group) constitutes a network interface and has its own unique IP address. For example, in the sample network shown in Figure 9-14, the IP router has three network interfaces.

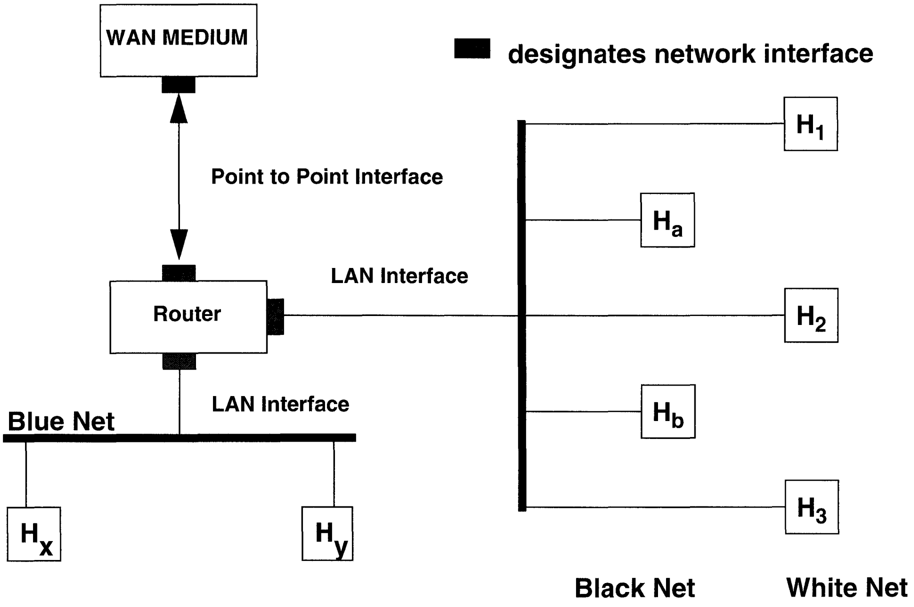


Figure 9-14 Sample TCP/IP Router Topology

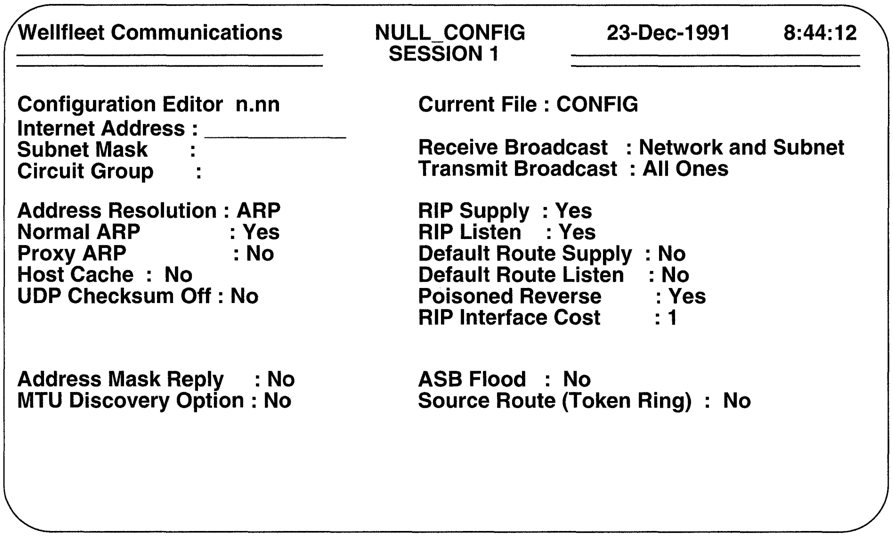
As shown in Figure 9-14, there are two types of network interfaces. A LAN interface connects the router to an Ethernet, FDDI, or IEEE 802.x local area medium. A Point to Point interface connects the router to a single long haul medium. The long haul medium can be terminated by a remote peer, host or gateway. Regardless of interface type, each network interface requires specific definition.

The node can support multiple networks on a single network interface. Consequently, in Figure 9-14, one interface provides a connection to both the "Black" and "White" networks.

You define a specific network interface from the TCP/IP Detailed Parameters Access Screen. Enter <2> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Network Interface Definitions record(s) found
Do you wish to add Network Interface Definitions record(s)?

Press [RETURN] to display the Network Interface Definition Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn              Current File : CONFIG
Internet Address : ___________
Subnet Mask      :                      Receive Broadcast  : Network and Subnet
Circuit Group    :                      Transmit Broadcast : All Ones

Address Resolution : ARP                RIP Supply  : Yes
Normal ARP         : Yes                RIP Listen  : Yes
Proxy ARP          : No                 Default Route Supply : No
Host Cache  :  No                       Default Route Listen  : No
UDP Checksum Off : No                   Poisoned Reverse      : Yes
                                        RIP Interface Cost    : 1


Address Mask Reply    : No              ASB Flood  :  No
MTU Discovery Option : No               Source Route (Token Ring)  :  No
```

Figure 9-15 Network Interface Definition Screen

- ❒ **Internet Address** specifies the 32-bit IP address of the network interface.

  Enter the IP address in dotted decimal notation.

NOTE

If you are configuring an X.25 DDN interface, **Internet Address** must be the same as the DDN **Internet Address** parameter.

- ❒ **Subnet Mask** specifies the network and subnetwork portion of the 32-bit IP address.

  Enter the mask value in dotted decimal notation.

- ❒ **Circuit Group** identifies the connection between the IP router and the attached network.

  Enter the name of the circuit group that provides the router/network interface.

NOTE

If you are configuring an X.25 DDN or an X.25 PDN interface, **Circuit Group** must be the same as the **Upper Circuit Name** parameter.

- ❐ **Receive Broadcast** specifies the types of broadcast messages that the IP router receives.

  Network and Subnet, is preferable in most applications in that IP accepts both network and sub-network broadcast messages.

  A network broadcast message takes one of the following forms:

  <Net_ID> <0's>
  <Net_ID> <1's>

  where `<Net_ID>` is the Network Information Center (NIC) assigned 8-bit, 16-bit, or 32-bit network address and `<0's>` or `<1's>` is a string of 8, 16, or 32 ones or zeroes.

  A sub-network broadcast message takes one of the following forms:

  <Net_ID> <Subnet_ID> <0's>
  <Net_ID> <Subnet_ID> <1's>

  where `<Net_ID>` is the NIC-assigned 8-bit, 16-bit, or 32-bit network address, <Subnet_ID> is the locally assigned sub-network identifier and `<0's>` or `<1's>` is a string of ones or zeroes.

  If you select **Network Only**, the router accepts only the network broadcasts. You should choose this option only if the router operates in a non-subnetted environment.

- ❐ **Transmit Broadcast** identifies the interface-specific transmit broadcast address.

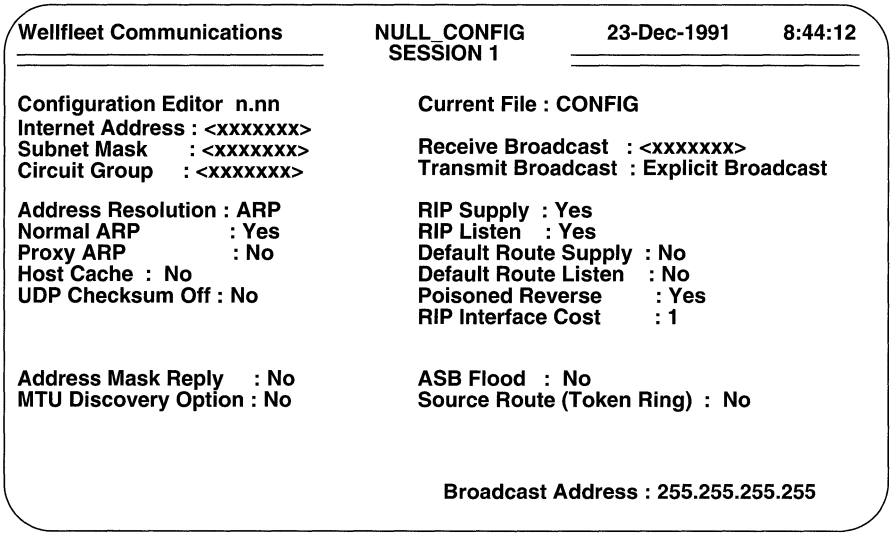
  If you select **All Ones** or **All Zeros**, IP uses either a default mask or the subnet mask (if one is specified at **Subnet Mask**) and places either all zeros or all ones in the host portion of the transmit broadcast address.

  You can also assign an explicit transmit broadcast address by selecting **Explicit Broadcast**. The screen prompts for an explicit broadcast address (Figure 9-16).

NOTE

If you are defining an interface that serves multiple networks, you must use an explicit broadcast address. Press `[RETURN]` at **Broadcast Address** to select an explicit broadcast address of 255.255.255.255.

Enter the explicit address in dotted decimal notation.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn             Current File : CONFIG
Internet Address : <xxxxxxx>
Subnet Mask      : <xxxxxxx>           Receive Broadcast  : <xxxxxxx>
Circuit Group    : <xxxxxxx>           Transmit Broadcast : Explicit Broadcast

Address Resolution : ARP               RIP Supply  : Yes
Normal ARP         : Yes               RIP Listen  : Yes
Proxy ARP          : No                Default Route Supply  : No
Host Cache  :  No                      Default Route Listen  : No
UDP Checksum Off : No                  Poisoned Reverse      : Yes
                                       RIP Interface Cost    : 1


Address Mask Reply    : No             ASB Flood  :  No
MTU Discovery Option : No              Source Route (Token Ring)  :  No



                                         Broadcast Address : 255.255.255.255
```

Figure 9-16 Explicit Broadcast Address Screen

- ❒ **Address Resolution** enables or disables address resolution (the mapping of 32-bit IP addresses to 48-bit Ethernet addresses).

  ARP conditionally enables IP-to-Ethernet address mapping using the Address Resolution Protocol (ARP, as described in RFC 826) and the Proxy ARP Protocol.

  HP Probe enables the proprietary Hewlett Packard *Probe* protocol, an address resolution mechanism that functions much like ARP. IP supports the following Probe messages:

  - *Unsolicited Reply* (incoming and outgoing)
  - *Name Request* (incoming)
  - *Name Reply* (outgoing)
  - *Virtual Address Request* (incoming and outgoing)
  - *Virtual Address Reply* (incoming and outgoing)
  - *Gateway Request* (incoming)
  - *Gateway Reply* (outgoing)

  ARP & HP Probe enables concurrent operation of HP Probe and ARP. With both address resolution protocols enabled, IP uses the first-in resolved media address until the address is modified by subsequent updates.

DDN enables the DDN address resolution algorithm. You must select this value if the network interface provides X.25 DDN service.

PDN enables a table-based RFC 877-compliant address resolution mechanism. You must select this value if the network interface provides X.25 PDN service.

None disables address mapping. With mapping disabled, you must configure all MAC-address-to-IP address relationships statically.

❐ **Normal ARP** enables or disables ARP.

ARP maps a 32-bit IP address to a 48-bit Ethernet address. In order to enable ARP, you must have set the **Address Resolution** parameter to **ARP** or **ARP & HP Probe**.

Select either **Yes** (enable ARP), or **No** (disable ARP).

NOTE

If the network interface provides either X.25 DDN or X.25 PDN service, you must set **Normal ARP** to **No**.

❐ **Proxy ARP** enables or disables the Proxy ARP protocol.

Proxy ARP allows IP to respond on a local interface to ARPs for a remote network. This response enables the router to assume responsibility for IP datagrams destined for the remote network. In order to enable Proxy ARP, you must have set **Address Resolution** to **ARP** or **ARP & HP Probe**.

Select either **No** (disable Proxy ARP), or **Yes** (enable Proxy ARP).

NOTE

If the network interface provides either X.25 DDN or X.25 PDN service, you must set **Proxy ARP** to **No**.

❐ **Host Cache** enables or disables the aging of physical-level addresses learned by any of the address resolution protocols.

With the address resolution cache disabled (**Host Cache** equal to **No**), entries in the address resolution cache are not aged out. With the address resolution cache enabled (**Host Cache** equal to **Yes**), cache entries that have not been accessed within two minutes are removed from the cache. Once an entry has been removed, IP must re-acquire the physical level address via an address resolution protocol.

❐ **UDP Checksum Off** enables or disables UDP checksum processing for the interface.

In virtually all instances, you should select **No** to enable checksum processing. **Yes** disables checksum processing and provides backward compatibility with UNIX BSD 4.1.

❒ **RIP Supply** (along with **RIP Listen**, **Default Route Supply**, **Default Route Listen**, **Poisoned Reverse**, and **RIP Interface Cost**) implement certain features of the Routing Information Protocol. RIP is a distance-vector protocol that enables the exchange of routing information between routers in the same autonomous system.

RIP Supply specifies whether IP transmits periodic RIP updates to neighboring routers. If you select **Yes**, IP transmits RIP updates; if you select **No**, IP does not transmit updates. If you wish to supply default route information, you must set **RIP Supply** to **Yes**.

NOTE

Because X.25 DDN service does not support RIP you must set **RIP Supply, RIP Listen, Default Route Supply,** and **Default Route Listen** to **No** if the network interface provides X.25 DDN service.

❒ **RIP Listen** specifies whether IP adds routing information (received in RIP updates from neighboring routers) to its internal routing table.

If you select **Yes**, IP adds received routing information to its internal routing table; if you select **No**, IP does not add received routing information to its internal routing table. If you wish to listen for default route information, you must set **RIP Listen** to **Yes**.

❒ **Default Route Supply** specifies whether IP advertises default routes in RIP updates sent to neighboring routers.

If you select **No**, IP does not advertise default routes; if you select **Yes**, IP does advertise default routes. If you enable **Default Route Supply**, you must also enable **RIP Supply**.

❒ **Default Route Listen** specifies whether IP adds default route information to its internal routing table.

If you select **No**, IP does not add received default route information to its internal routing table; if you select **Yes**, IP does add default route information to this table. If you enable **Default Route Listen**, you must also enable **RIP Listen**.

❒ **Poisoned Reverse** specifies how IP advertises routes it has learned from a neighboring router in periodic updates subsequently sent to the neighbor.

If you select **Yes**, IP implements poisoned reverse. With poisoned reverse enabled, IP advertises routes learned from a neighbor in RIP updates subsequently sent to that neighbor with a hop count of **RIP Network Diameter** plus 1 (thus declaring the destination unreachable).

If you select **No**, IP implements a split-horizon, and omits routes learned from a neighbor in RIP updates subsequently sent to that neighbor.

❒ **RIP Interface Cost** sets the cost for each router hop.

Standard RIP implementations assign a cost of 1 to each hop. You can increase this cost by entering a new value and pressing `[RETURN]`. You should keep in mind, however, that if you increase the RIP increment, the upper bound set by **RIP Network Diameter** (beyond which a network is declared unreachable) is more rapidly attained.

❒ **Address Mask Reply** enables or disables the generation of ICMP *address mask reply* messages at boot time and in response to valid *address mask request* messages.

If you enable this feature, the router generates such messages in compliance with the relevant sections of RFCs 950 and 1009.

NOTE

Neither X.25 DDN service nor X.25 PDN service support the *address mask reply* facility. Consequently, you must set **Address Mask Reply** to **No** if the network interface provides X.25 DDN or PDN service.

❒ **ASB Flood** enables certain IP broadcast datagrams received on one interface to be flooded across other router interfaces.

An all-subnet broadcast datagram is a datagram whose destination address is equal to the broadcast address for an entire subnet. If, for example, a network interface serves the subnet 128.10.2.1 (with a subnet mask of 255.255.255.0), any datagram with a destination address of 128.10.255.255 is considered an all-subnet broadcast.

With all-subnet broadcasting enabled, IP floods all-subnet broadcasts received on this interface to other interfaces which service the same subnet. Similarly, all-subnet broadcasts received on other interfaces are flooded to this interface. With all-sub-net broadcasting disabled, no flooding occurs.

❒ **MTU Discovery Option** enables or disables *Probe MTU* and *Reply MTU* options (IP options number 11 and 12, specified in RFC 1063).

These options enable IP to learn the minimum MTU of all networks traversed by an IP datagram from source to destination. The MTU option can significantly decrease network load by eliminating the need for transit fragmentation and destination reassembly.

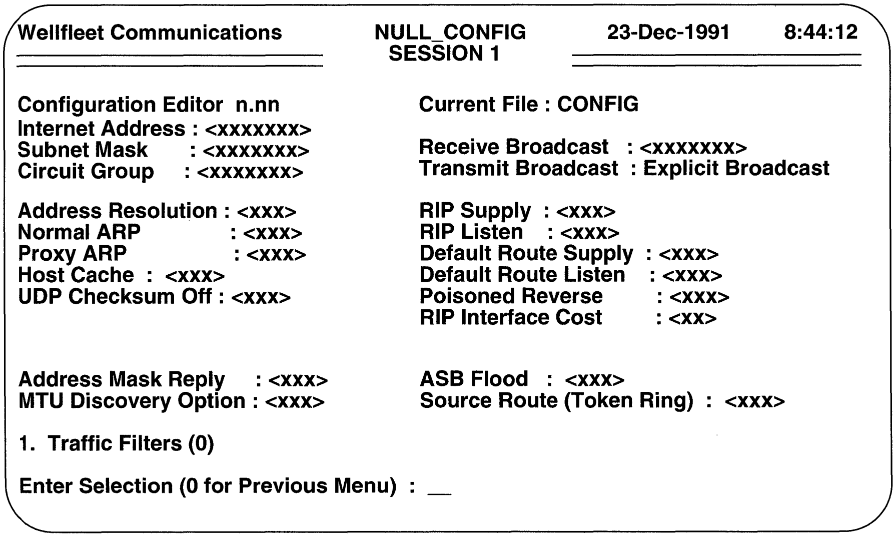
NOTE

Neither X.25 DDN service nor X.25 PDN service support the *mtu discovery* facility. Consequently, you must set **MTU Discovery Option** to **No** if the network interface provides X.25 DDN or PDN service.

❒ **Source Route (Token Ring)** enables source routing end node support over a token ring network. End node support establishes a peer relationship between the multiprotocol router and token ring endstation. Such a peer relationship enables a transition between source route bridging and TCP/IP routing environments and allows the IP router to transmit and receive source routed packets from a remote host through one (or a series of) token ring networks. With this feature enabled, network end stations that support both source route bridging and IP routing are able to use bridging within a local environment and routing on the internetwork.

Select **Yes** or **No** to enable or disable end node support, and then press `[RETURN]`.

The screen prompts for **Traffic Filters**.



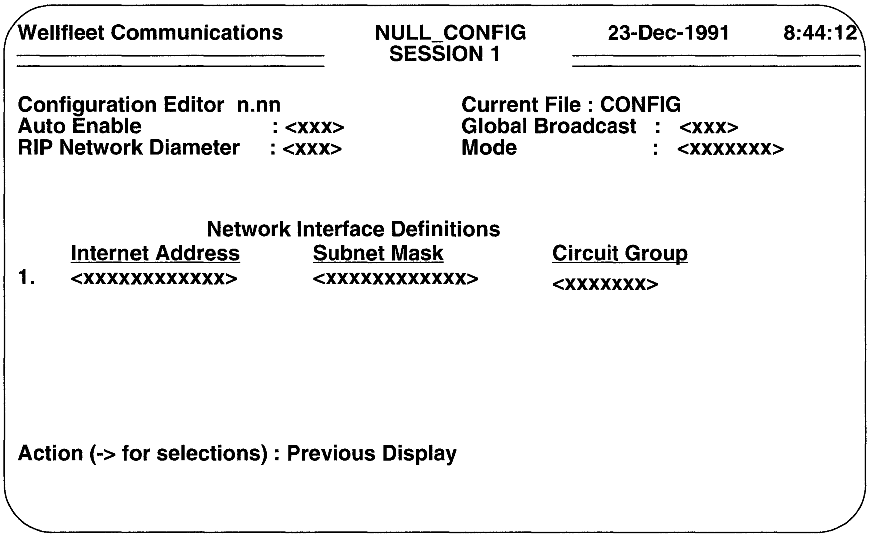
```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn              Current File : CONFIG
Internet Address : <xxxxxxx>
Subnet Mask      : <xxxxxxx>            Receive Broadcast  : <xxxxxxx>
Circuit Group    : <xxxxxxx>            Transmit Broadcast : Explicit Broadcast

Address Resolution : <xxx>              RIP Supply  : <xxx>
Normal ARP         : <xxx>              RIP Listen  : <xxx>
Proxy ARP          : <xxx>              Default Route Supply  : <xxx>
Host Cache  :  <xxx>                    Default Route Listen  : <xxx>
UDP Checksum Off : <xxx>                Poisoned Reverse      : <xxx>
                                        RIP Interface Cost    : <xx>


Address Mask Reply    : <xxx>           ASB Flood  :  <xxx>
MTU Discovery Option : <xxx>            Source Route (Token Ring)  :  <xxx>

1.  Traffic Filters (0)

Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-17 IP Filters Configuration Screen

To configure interface-specific filters, proceed to Section 9.13, *Configuring IP Filters*. If you do not want to configure filters enter <0> at **Enter Selection (0 for Previous Display)** to return to the TCP/IP Detailed Parameters Access Screen. Now proceed to the next section to define additional IP interfaces.

9.5 Defining Additional IP Interfaces

You define an additional network interface from the TCP/IP Detailed Parameters Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Network Interface Definitions Summary Screen.



```
Wellfleet Communications         NULL_CONFIG       23-Dec-1991      8:44:12
                                  SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Auto Enable             : <xxx>              Global Broadcast  :  <xxx>
RIP Network Diameter    : <xxx>              Mode              :  <xxxxxxx>


                    Network Interface Definitions
     Internet Address        Subnet Mask             Circuit Group
1.   <xxxxxxxxxxxxx>         <xxxxxxxxxxxxx>         <xxxxxxxx>




Action (-> for selections) : Previous Display
```

Figure 9-18 Network Interface Definitions Summary Screen

Press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Network Interface Definition Screen. Now follow the previously described procedures to define an additional network interface. Repeat these procedures until you have defined all network interfaces.

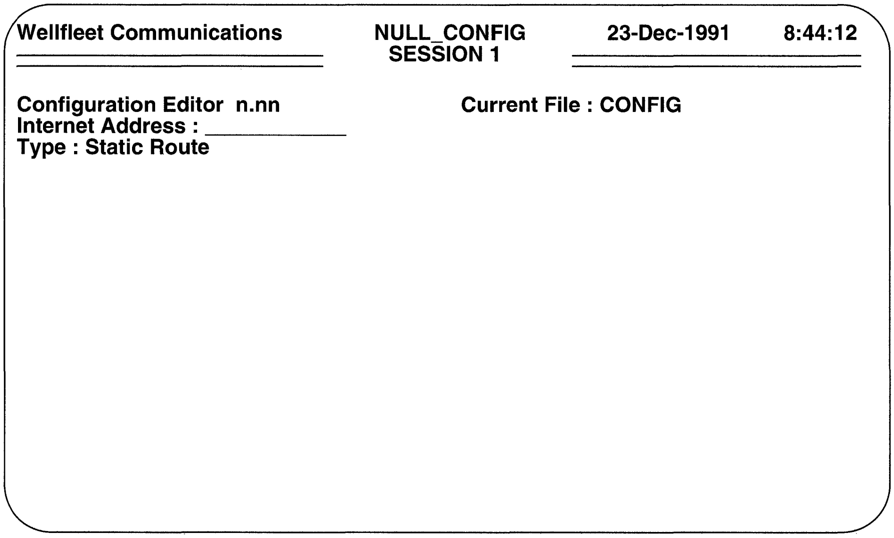
9.6 Configuring Static Routes

Static routes are manually configured routes that specify transmission paths that datagrams are to follow on the basis of the datagram's destination address. Unlike routes learned through routing protocols (RIP, EGP, or OSPF) static routes remain in the IP routing tables until they are explicitly removed.

You configure static routes from the TCP/IP Detailed Parameters Access Screen. Enter `<3>` at **Enter Selection (0 for Previous Menu)**. The screen prompts:

> **No Static Routes record(s) found**
> **Do you wish to add Static Routes record(s)?**

Press **`[RETURN]`** to display the Static Route Configuration Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Internet Address : ____________
Type : Static Route
```

Figure 9-19 Static Route Configuration Screen

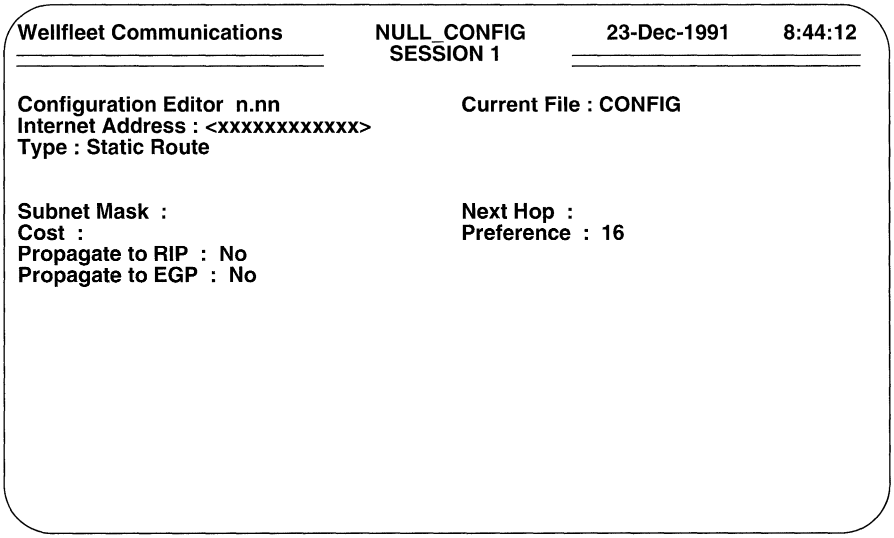
You use the Static Route Configuration Screen to configure four types of static routes:

- *Static routes*, which specify a path to another router
- *Default routes*, which also specify a path to another router
- *Adjacent host routes*, which specify a path to a host
- *Static adjacencies*, which specify a Frame Relay path to a host

9.6.1 Static Route

You configure a static route (a route to another router), from the Static Route Configuration Screen. To begin, enter the destination IP address (in dotted decimal notation) at **Internet Address**.

After the cursor moves to the **Type** field, select **Static Route**. The screen displays the Static Route Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Internet Address : <xxxxxxxxxxxx>
Type : Static Route

Subnet Mask  :                              Next Hop  :
Cost  :                                     Preference  :  16
Propagate to RIP  :  No
Propagate to EGP  :  No
```

Figure 9-20 Static Route Parameters Screen

❐ **Subnet Mask** specifies the range of the static route.

For example, if **Internet Address** is equal to 192.32.1.0 and **Subnet Mask** is equal to 255.255.255.0, the static route applies to all 192.32.1.xx traffic.

❐ **Next Hop** is the IP address of the next hop router.

Enter this address in dotted decimal notation.

❐ **Cost** is the number of router hops that a datagram traverses before the destination is reached.

Check your network topology drawing if necessary and enter the number (from `1` to `99`) of router hops.

❐ **Preference** specifies a weighted value used by IP to select from multiple routes to a single destination.

IP maintains a routing pool which contains information supplied by up to three routing protocols (RIP, EGP, OSPF) in addition to manually configured static routes. Consequently, the routing pool may contain multiple routes to the same destination. By default, IP uses manually configured static and/or default routes in preference to routes gathered by protocol exchanges.

Preference contains a numeric value within the range from 0 to 16; the higher the value, the greater the preference of the route. That is, routes with higher values will be selected (used for routing) by IP in preference to routes with lower values.

Enter a decimal value from 0 (lowest preference) to 16 (greatest preference).

❐ **Propagate to RIP** specifies whether the static route is advertised by the RIP protocol.

If you want RIP to advertise this static route, select **Yes**; if you do not want RIP to advertise this static route, select **No**.

NOTE

RIP Supply enables the RIP advertising function. If RIP is enabled (**RIP Supply** equals **Yes**), the setting of the **Propagate to RIP** parameter specifies whether an individual static route is advertised. If RIP is not enabled (**RIP Supply** equals **No**), the **Propagate to RIP** parameter is non-functional.

❐ **Propagate to EGP** specifies whether the static route is advertised by the EGP protocol.

If you want EGP to advertise this static route, select **Yes**; if you do not want EGP to advertise this static route, select **No**.

The screen prompts you to **Hit Return to Continue**. When you press `[RETURN]`, the screen displays the TCP/IP Detailed Parameters Access Screen.

9.6.2 Default Route

A default route is a form of static route. Default routes minimize the size of the internal routing table, and reduce the data transmitted in periodic routing table updates. Default routes are most efficiently used when the IP router has a small number of directly connected networks, and has a single connection to another routing device. Upon receiving a datagram, IP scans its internal table for the destination address. With a default route specified, if the router does not find the destination address, it uses the default route

You configure a default route from the Static Route Configuration Screen. Enter 0.0.0.0 at **Internet Address**. After the cursor moves to the **Type** field, select **Static Route**. The screen displays the Static Route Parameters Screen.

❒ **Subnet Mask** is not used for default routes.

Press **[RETURN]**.

❒ **Next Hop** is the IP address of the next hop router.

Enter this address in dotted decimal notation.

❒ **Cost** is the number of intermediate systems that a datagram traverses before it reaches the edge of its destination autonomous system.

Check your network topology drawing to determine this number. Enter the number, then press **[RETURN]**.

❒ **Preference** specifies a weighted value used by the IP router to select from multiple default routes to a single destination.

You can configure up to four default routes to the same destination network. By configuring multiple routes, you ensure that a datagram can be re-routed if the interface associated with the default route is disabled. You assign priority values to each default route, to determine which default route is the most preferred.

If the highest priority default route is unavailable, IP uses the next most-preferred default route. If this interface is also unavailable, the router then chooses the next most-preferred default route. Should a disabled default route with a higher priority value re-enable, IP uses it as the default route.

Preference contains a numeric value within the range from 1 to 16; the higher the value, the greater the preference of the route. That is, routes with higher values will be selected (used for routing) by IP in preference to routes with lower values.

Enter a decimal value from 0 (lowest preference) to 16 (greatest preference).

❒ **Propagate to RIP** specifies whether the default route is advertised by the RIP protocol.

If you want RIP to advertise this default route, select **Yes**; if you do not want RIP to advertise this default route, select **No**.

NOTE

RIP Supply enables the RIP advertising function. If RIP is enabled (**RIP Supply** equals **Yes**), the setting of the **Propagate to RIP** parameter specifies whether an individual default route is advertised. If RIP is not enabled (**RIP Supply** equals **No**), the **Propagate to RIP** parameter is non-functional.

❒ **Propagate to EGP** specifies whether the default route is advertised by the EGP protocol.

If you want EGP to advertise this default route, select **Yes**; if you do not want EGP to advertise this default route, select **No**.

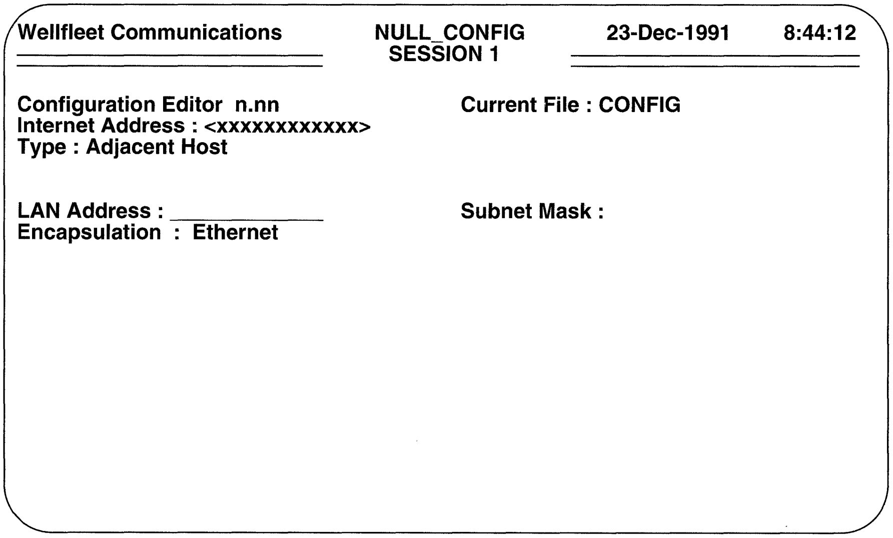
The screen prompts you to **Hit Return to Continue**. When you press `[RETURN]`, the screen displays the TCP/IP Detailed Parameters Access Screen.

9.6.3 Adjacent Host Route

Adjacent hosts are systems on a locally-attached network. You need to specify an adjacent host if you are setting up a protected network; or if a particular local host or hosts do not respond to ARP requests.

You configure an adjacent host route from the Static Route Configuration Screen . Enter the destination IP address (in dotted decimal notation) at **Internet Address**. After the cursor moves to the **Type** field, select **Adjacent Host**, then press `[RETURN]`.

The screen displays the Adjacent Host Route Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Internet Address : <xxxxxxxxxxxx>
Type : Adjacent Host

LAN Address : ____________                   Subnet Mask :
Encapsulation  :  Ethernet
```

Figure 9-21 Adjacent Host Route Parameters Screen

- **LAN Address** is the 48-bit Ethernet address of the adjacent host.

  Enter the 48-bit Ethernet address as a 12-digit hexadecimal number.

- **Subnet Mask** specifies the part of **Internet Address** that refers to the subnet.

If **LAN Address** is located in a subnet, type in the subnet mask value in dotted decimal notation, then press `[RETURN]`. If the host address is not in a subnet, press `[RETURN]`.

- ❐ **Encapsulation** selects from three available encapsulation methods.

If you are defining a point-to-point network interface, or any type of X.25 interface, you must select standard Ethernet 2.0 encapsulation.

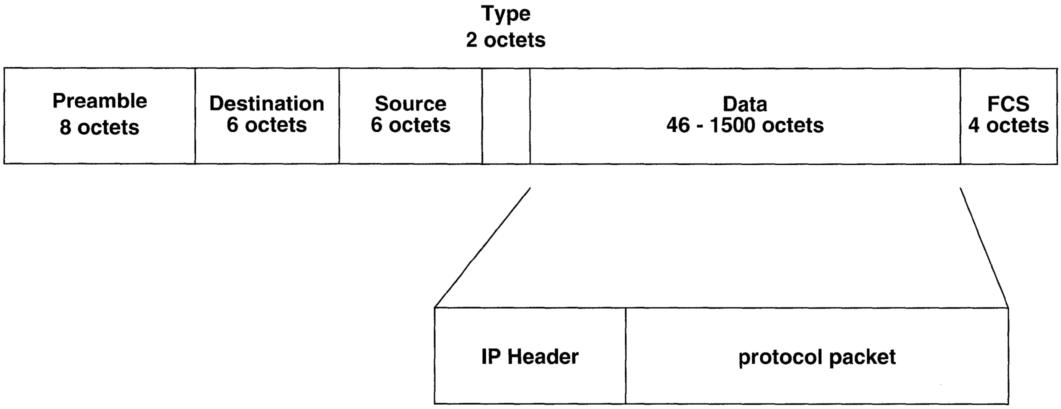


Figure 9-22 IP Ethernet Encapsulation

Ethernet encapsulation prefixes an eight-octet preamble, six octets of destination-address information, six octets of source-address information, and two octets of protocol type information (hexadecimal 0800) to the IP packet. It appends a four-octet frame check sequence to the packet.

If you are defining a LAN interface (Ethernet or IEEE 802.x), you must specify the encapsulation method supported by the attached network. In addition to **Ethernet** encapsulation, you can specify **SNAP** or **802.2** encapsulation.

802.2 encapsulation (shown in Figure 9-23) prefixes one octet of destination service access point (DSAP) information, one octet of source service access point (SSAP) information, and one octet of control information to the IP packet. The 802.2 structure is further encapsulated within a medium-specific 802.x packet.

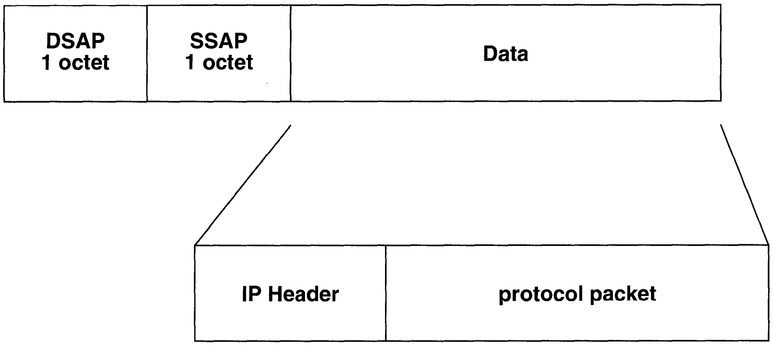


Figure 9-23 IP 802.2 Encapsulation

SNAP encapsulation (shown in Figure 9-24) is an extension of 802.2 encapsulation. It prefixes one octet of DSAP information (hexadecimal AA), one octet of SSAP information (hexadecimal AA), one octet of control information, three octets of organizational information (hexadecimal 0), and two octets of Ethernet Type information (hexadecimal 0800) to the IP packet. The SNAP structure is further encapsulated within a medium-specific 802.x packet.

Press the `[RIGHTARROW]` to select **Ethernet**, **802.2**, or **SNAP** on the basis of the encapsulation method used by the connected network.

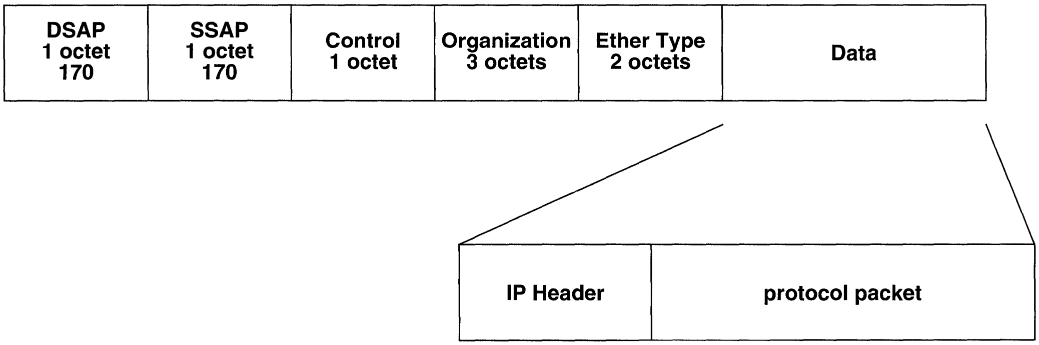


Figure 9-24 IP SNAP Encapsulation

The screen prompts **Hit Return to Continue**. When you press `[RETURN]`, the screen displays the TCP/IP Detailed Parameters Access Screen.

9.6.4 Static Adjacency

A static adjacency provides a static Frame Relay route.

You configure a static adjacency from the Static Route Configuration Screen. Enter the destination IP address (in dotted decimal notation) at **Internet Address**. After the cursor moves to the **Type** field, select **Static Adjacency**, then press `[RETURN]`.

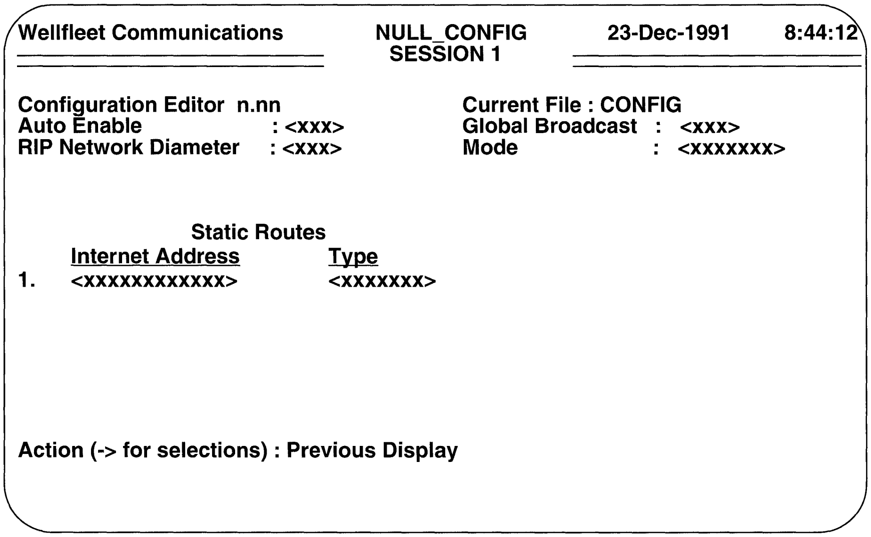
- ❐ **DLCI** specifies the Frame Relay Data Link Connection Identifier to the target host.

  Enter the DLCI as a decimal number.

The screen prompts **Hit Return to Continue**. When you press `[RETURN]`, the screen displays the TCP/IP Detailed Parameters Access Screen.

9.6.5 Configuring Additional Static Routes

You specify additional static, default, static adjacencies, or adjacent host routes from the TCP/IP Detailed Parameters Access Screen. Enter `<2>` at **Enter Selection (0 for Previous Menu)**. The screen displays the Static Routes Summary Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG
Auto Enable              : <xxx>                Global Broadcast  :  <xxx>
RIP Network Diameter     : <xxx>                Mode              :  <xxxxxxx>


                  Static Routes
     Internet Address          Type
1.   <xxxxxxxxxxxx>            <xxxxxxx>




Action (-> for selections) : Previous Display
```

Figure 9-25 Static Routes Summary Screen

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Static Route Configuration Screen. Now follow the previously described procedures to configure additional static, default, or adjacent host routes. Repeat these procedures until you have configured all such routes.

9.7 Configuring OSPF

OSPF (for Open Shortest Path First) is, like RIP, an internal gateway routing protocol. Unlike RIP, however, OSPF uses a link-state algorithm to route datagrams through an internet.

For RIP (a distance-vector protocol) the “best” path between source and destination is the shortest path. RIP computes distance as a metric, usually the number of hops from the origin network to the target network. For RIP, the best path is the one with the fewest hops.

OSPF is more sophisticated in recognizing that a simplistic hop-count takes no account of available bandwidth. Passing through an extra hop to get to a 1.54 Mb T1 channel, for instance, may be more efficient than traversing a shorter, but congested route. For OSPF, the “best” path is the one that offers the least delay.

In order to reduce the level of protocol traffic OSPF allows collections of contiguous networks and hosts to be grouped together. This grouping of contiguous networks and hosts along with the routers having an interface(s) to any of the included networks is called an *area*. The topology of an area is invisible to non-area residents; similarly routers that reside within a single area know nothing of the topology external to the area. Figure 9-26 illustrates OSPF area configuration.

Segmentation of an autonomous system in OSPF areas leads to two types of routing: *intra-area routing* and *inter-area routing*. Intra-area routing routes packets between sources and destinations that reside within the same area; Inter-area routing routes packets between sources and destinations that reside within different areas.

In intra-area routing, packets are routed solely on the basis of information obtained within the area; external information need not (and can not) be used. In inter-area routing, packets are routed in three stages: (1) an internal router (a router whose directly connected networks all reside within the same area) directs the packet to an area border router (a router that services multiple areas); (2) the area border router directs the packet across the OSPF backbone to the destination network; (3) an internal router forwards the packet to the destination.

Table 9-4 briefly describes the types of routers within an OSPF domain. Router types are not mutually exclusive: area border routers are also backbone routers, while backbone routers can, depending upon the topology, be internal routers.

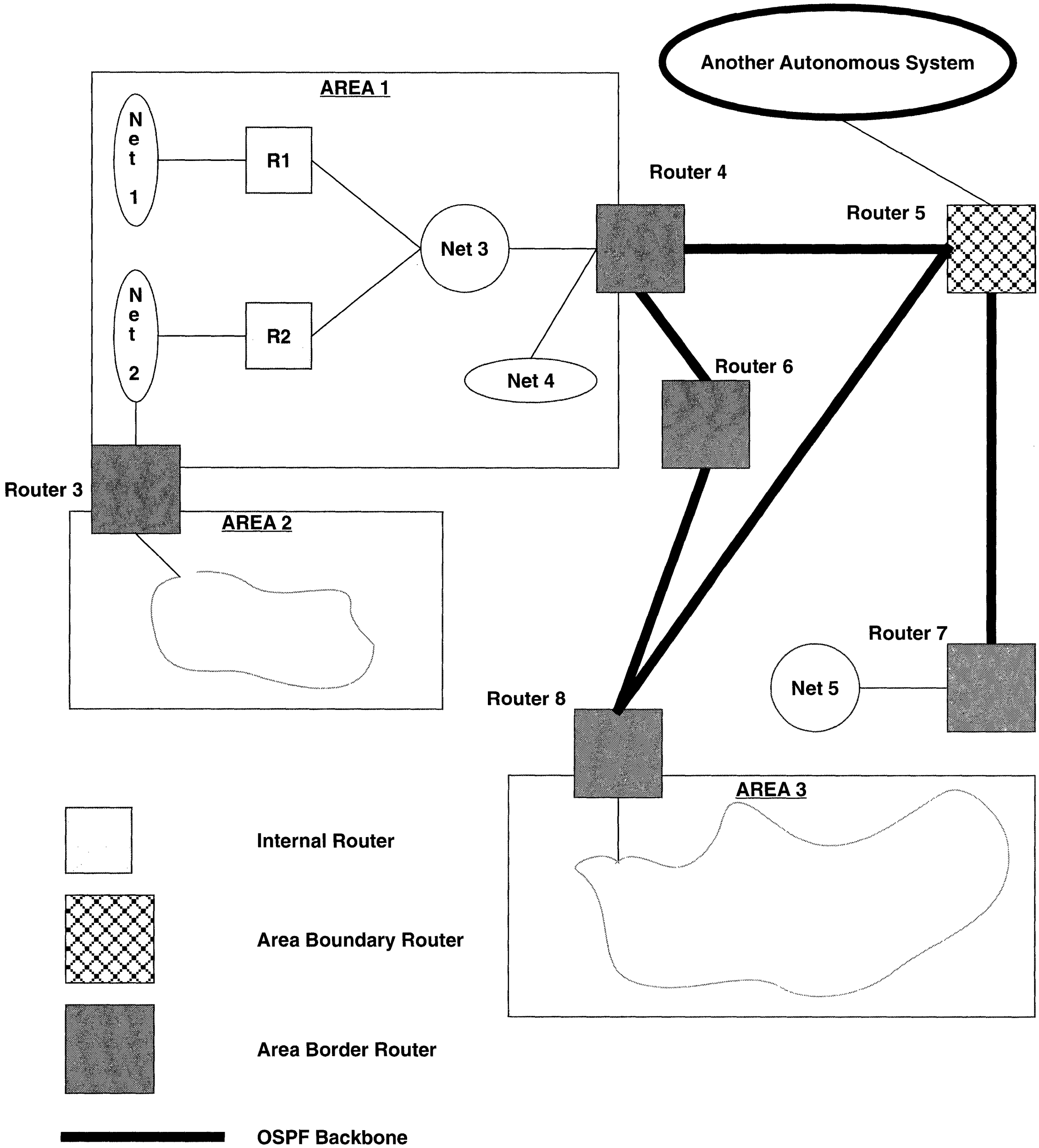


Figure 9-26 Sample OSPF Topology

Table 9-4: OSPF Router Types

Router Type	Description
Internal	a router with all directly connected networks belonging to the same area -- an internal router maintains a single copy of the routing algorithm
Area Border	a router with directly connected networks belonging to more than one area -- an area border router maintains a copy of the routing algorithm for each attached network and for the OSPF backbone (networks not contained within any area, their attached routers, and routers that service multiple areas)
Backbone	a router that connects to the backbone -- by definition area border routers are backbone routers (routers with all interfaces connected to the backbone are considered to be internal routers)
AS Boundary	A router that exchanges routing information with other autonomous systems

The OSPF *backbone* consists of networks not contained within any area (network 5 in Figure 9-26), their attached routers (router 7 in Figure 9-26), and those routers that belong to multiple areas (router 3 in Figure 9-26). Area border routers (routers 3, 4, and 8 in Figure 9-26) and routers that attach only to the OSPF backbone (router 6 in Figure 9-26) must be configured to reflect their backbone connectivity.

The backbone distributes routing information between OSPF areas. The backbone has all the properties of an OSPF area (the topology of the backbone is hidden from other areas, while other area know nothing of the backbone topology). The area id 0.0.0.0 is assigned to the backbone.

The OSPF backbone must be contiguous. Depending on network topology and area definition, it is possible to construct an OSPF topology in which the backbone is no longer contiguous. For example, in Figure 9-26, router 3 is not contiguous to the OSPF backbone. In such cases, *virtual links* are required to restore contiguousness.

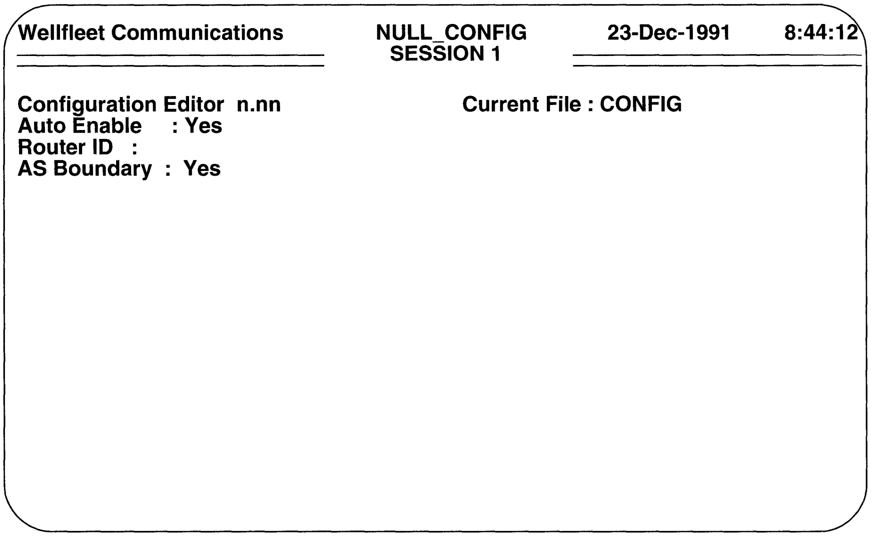
Virtual links are statically configured backbone components that join two backbone routers that have an interface to a common non-backbone area (routers 3 and 4 in Figure 9-26). The OSPF protocol treats a virtual link as if it were a point-to-point network connection between the two backbone routers.

9.7.1 Setting Basic OSPF Parameters

You set basic OSPF parameters from the TCP/IP Detailed Parameters Access Screen. Enter `<4>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No OSPF record(s) found
Do you wish to add OSPF record(s)?

Press `[RETURN]` to display the OSPF Basic Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Auto Enable    : Yes
Router ID  :
AS Boundary  :  Yes
```

Figure 9-27 OSPF Basic Parameters Screen

- ❒ **Auto Enable** specifies the initial state of OSPF. This OSPF-specific **Auto Enable** works in conjunction with the global auto enable parameter (refer to Section 2.1) to enable or disable OSPF when the router boots.

  When global auto enable is **No**, OSPF is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable OSPF with NCL commands after the router boots.

  When global auto enable is **Yes**, OSPF is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable OSPF) or **No** (disable OSPF), then press `[RETURN]`. If you select **No**, you will later need to enable OSPF with NCL commands after the router boots.

- ❐ **Router ID** uniquely identifies the IP router within the OSPF domain.

  Enter the router's ID in dotted decimal notation.

NOTE

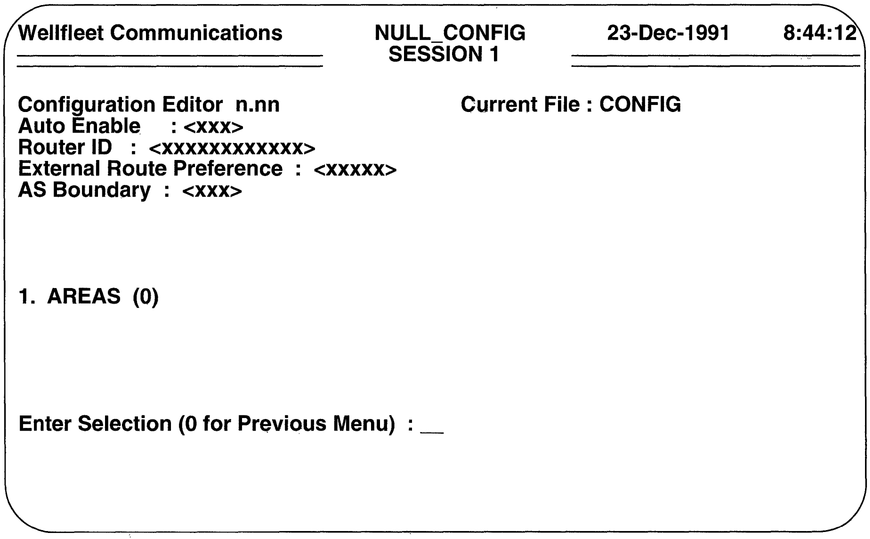
One algorithm for **Router ID** assignment is to choose the largest or smallest IP address assigned to the router.

- ❐ **AS Boundary** opens the OSPF routing pool to routing information obtained from sources external to OSPF.

  If you want the OSPF routing pool to include manually configured routes and routes obtained from RIP and EGP, press `[RETURN]` to accept the default response, **Yes**.

  If you want to restrict the OSPF routing pool to those routes acquired by OSPF, press the `[RIGHTARROW]` to display **No**, and then press `[RETURN]`.

After you press `[RETURN]`, the screen prompts for OSPF area information.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Auto Enable    : <xxx>
Router ID  :  <xxxxxxxxxxxxx>
External Route Preference  :  <xxxxxx>
AS Boundary  :  <xxx>



1.  AREAS  (0)




Enter Selection (0 for Previous Menu)  : __
```

Figure 9-28 OSPF Area Access Screen

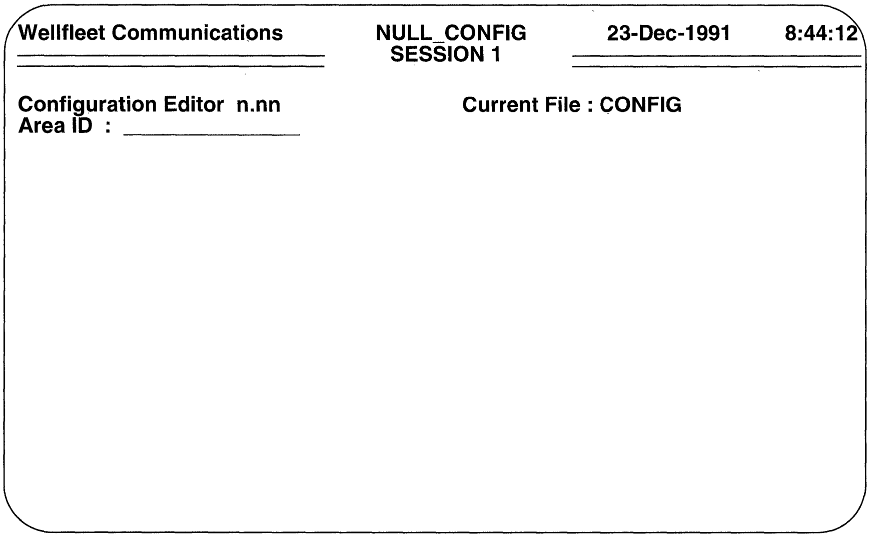
9.7.2 Configuring OSPF Backbone Connections

If the IP router provides a connection to the OSPF backbone, follow the procedures in this section to establish the backbone connection. If the router does not connect to the backbone, proceed to Section 9.7.3 to configure OSPF non-backbone areas.

You configure OSPF backbone connections from the OSPF Area Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No AREAS record(s) found
Do you wish to add AREAS record(s)?

Press `[RETURN]` to display the OSPF Area Identification Screen.

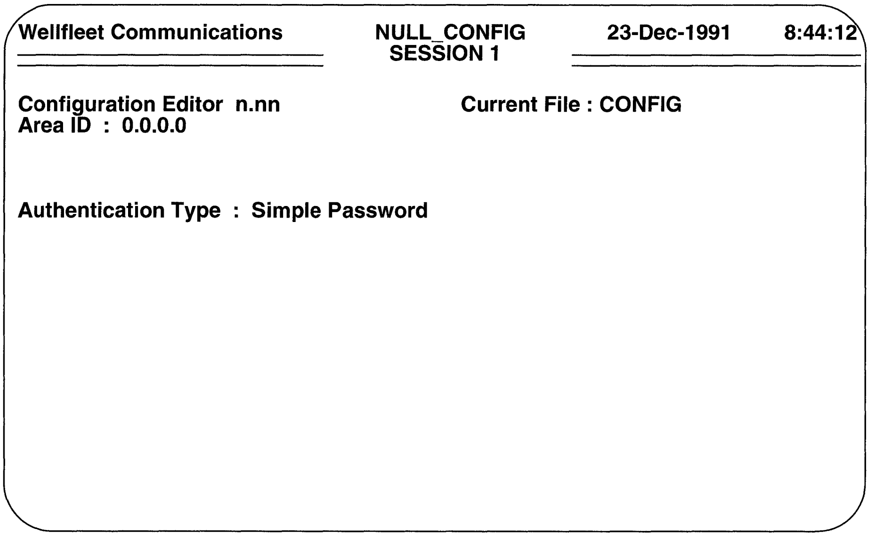


```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Area ID  :  ____________
```

Figure 9-29 OSPF Area Identification Screen

At **Area ID** enter `0.0.0.0` (the backbone area identifier)

After you specify the backbone area identifier, the screen prompts for more backbone-area-specific data (Figure 9-30).All OSPF packet exchanges can be authenticated by means of a password contained within the OSPF packet. Authentication is enabled on an area basis.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991    8:44:12
                                  SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Area ID  :  0.0.0.0


Authentication Type  :  Simple Password
```

Figure 9-30 OSPF Backbone Authentication Screen

The **Authentication Type** parameter enables or disables password authentication. To enable password authentication across the OSPF backbone, press `[RETURN]` to accept the default response, **Simple Password**. To disable password authentication, press the `[RIGHTARROW]` to display **No Authentication** and then press `[RETURN]`.

After you specify the authentication type the screen displays the OSPF Backbone Detailed Parameters Access Screen (Figure 9-31).

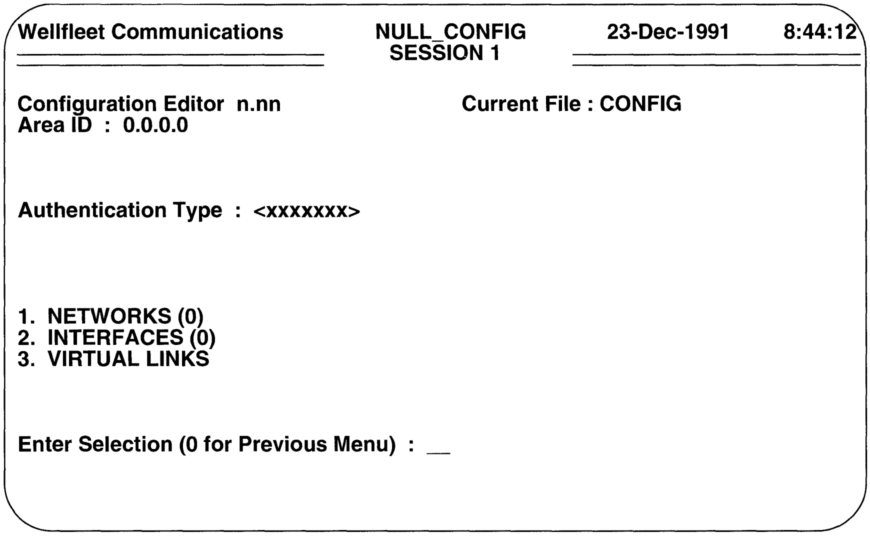
9.7.2.1 Backbone Networks

An OSPF backbone network is a network not contained within any area (for example, network 5 in Figure 9-26). If your topology includes such a network(s), you configure the network from the OSPF Backbone Detailed Parameters Access Screen. If your topology does not include such a network(s), proceed to Section 9.7.2.2.

To begin configuring an OSPF backbone network, enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen responds:

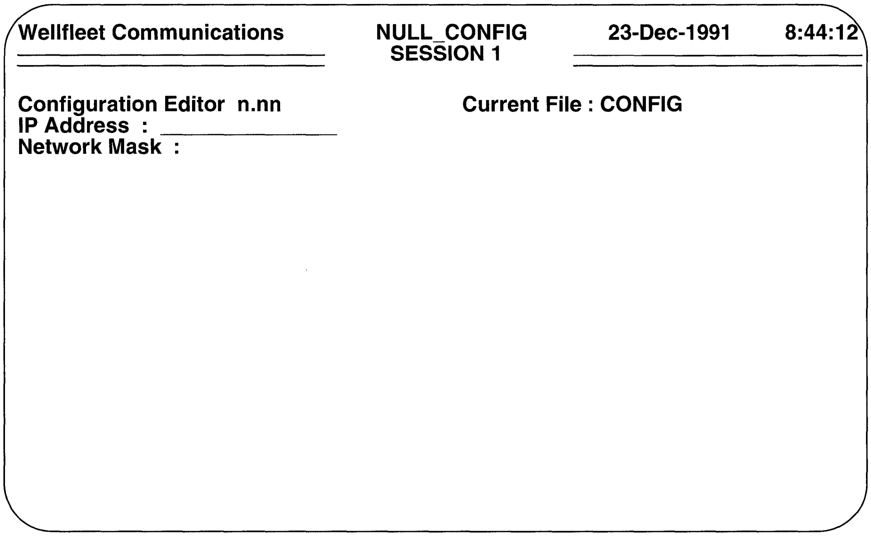
No NETWORK record(s) found
Do you wish to add NETWORK record(s)?

Press `[RETURN]` to display the OSPF Network Identification Screen (Figure 9-32).



```
Wellfleet Communications         NULL_CONFIG       23-Dec-1991      8:44:12
                                  SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Area ID  :  0.0.0.0


Authentication Type  :  <xxxxxxxx>



1.  NETWORKS (0)
2.  INTERFACES (0)
3.  VIRTUAL LINKS


Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-31 OSPF Backbone Detailed Parameters Access Screen



```
Wellfleet Communications         NULL_CONFIG       23-Dec-1991      8:44:12
                                  SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
IP Address  :  _______________
Network Mask  :
```

Figure 9-32 OSPF Network Identification Screen

- ❐ **IP Address** identifies the backbone network.

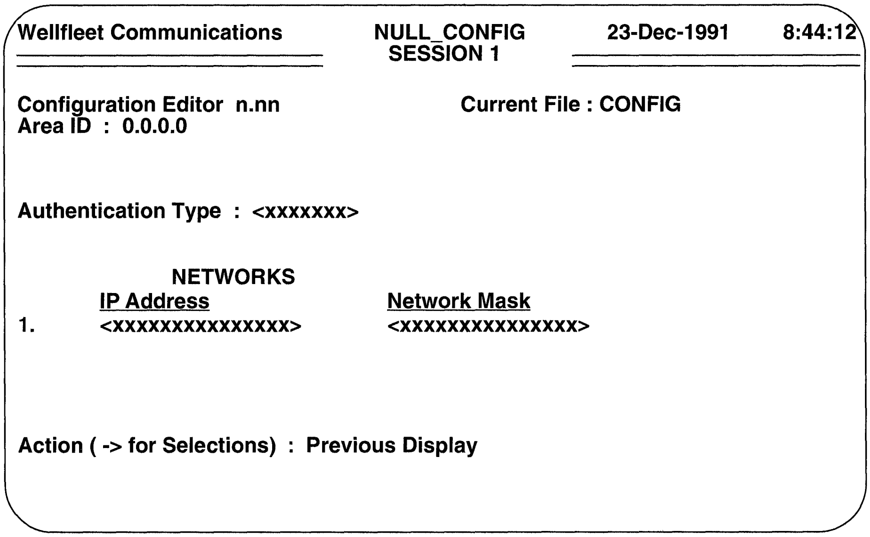
  Enter the IP network address in dotted decimal notation, and then press `[RETURN]`.

- ❐ **Network Mask** specifies the network/sub-net mask value (identifying those bits in the 32-bit IP address that specify `Net_ID` and `Subnet_ID`).

  Enter the mask value in dotted decimal notation, and then press `[RETURN]`.

After you specify the network mask, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the OSPF Backbone Detailed Parameters Access Screen.

If necessary, you add backbone networks from this screen. To add a network, enter `<1>` at the **Enter Selections (0 for Previous Menu)** prompt. The screen displays the OSPF Backbone Area Networks Summary Screen.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Area ID  :  0.0.0.0


Authentication Type  :  <xxxxxxxx>


                NETWORKS
        IP Address                  Network Mask
1.      <xxxxxxxxxxxxxxxx>          <xxxxxxxxxxxxxxxx>



Action ( -> for Selections)  :  Previous Display
```

Figure 9-33 OSPF Backbone Area Networks Summary Screen

At **Action (--> for Selections)** press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`. The screen displays the OSPF Network Identification Screen. Now proceed as before to add network information; continue until you have configured all backbone networks.

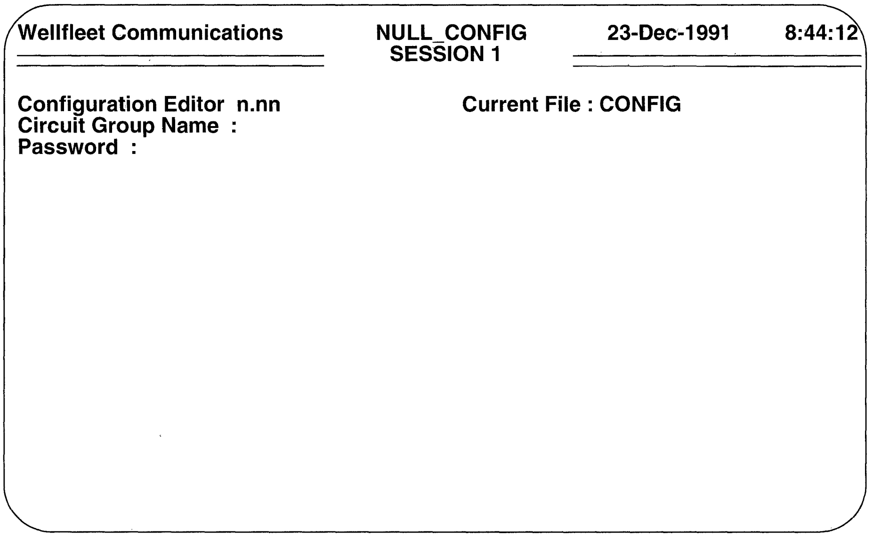
9.7.2.2 Backbone Interfaces

After configuring backbone networks (if any), you configure the actual interface(s) between the OSPF backbone router and adjacent backbone routers or networks. With reference to Figure 9-26, for example, assuming that router 7 was being configured, you would configure the interfaces to Net 5 and router 5.

You begin backbone interface configuration from the OSPF Backbone Detailed Parameters Access Screen. Enter <2> at the **Enter Selection (0 for Previous Menu)** prompt. The screen responds:

No INTERFACES record(s) found
Do you wish to add INTERFACES record(s)?

Press [RETURN] to display the OSPF Interface Basic Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Circuit Group Name  :
Password  :
```

Figure 9-34 OSPF Interface Basic Parameters Screen

❒ **Circuit Group Name** identifies the circuit group that provides the interface between the OSPF backbone router and an adjacent backbone device.

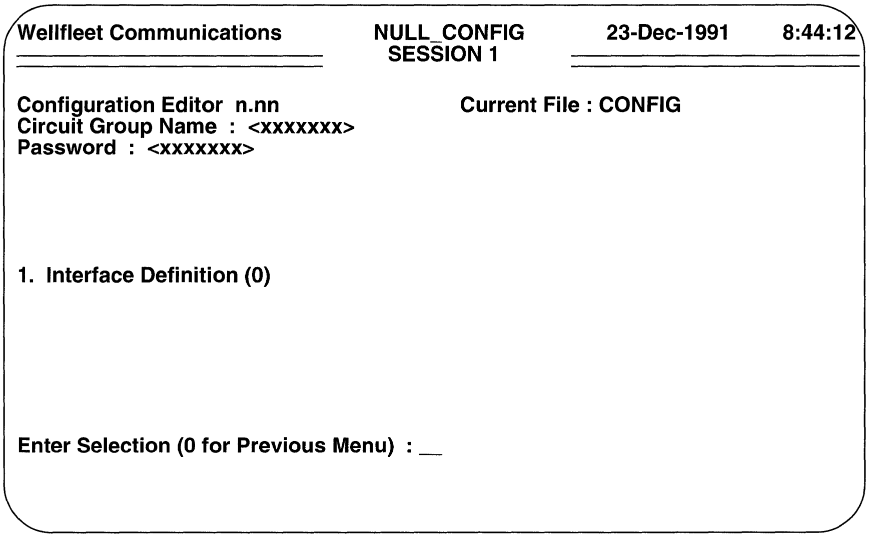
Enter the name of the circuit group, and then press [RETURN].

❒ **Password** specifies the authentication key used across this interface.

If you have not enabled authentication across the backbone, press [RETURN].

If you have enabled authentication, **Password** specifies a one-to-eight character ASCII string that appears in the authentication field of all OSPF packets across this interface. Enter the character string from the keyboard, and then press `[RETURN]`.

After you press `[RETURN]`, the screen prompts for additional interface-specific data.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Circuit Group Name  :  <xxxxxxx>
Password  :  <xxxxxxx>



1.  Interface Definition (0)




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-35 OSPF Interface Definition Access Screen

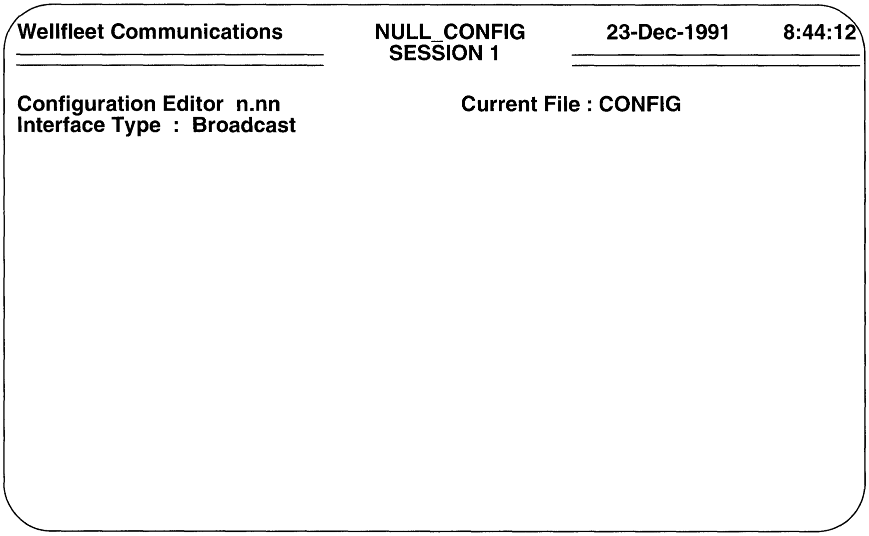
Enter `<1>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen displays the following:

> **No Interface Definition record(s) found**
> **Do you wish to add Interface Definition record(s)?**

Press `[RETURN]` to display the OSPF Interface Selection Screen (Figure 9-36).

OSPF recognizes three types of interface (or networks): a point-to-point network connects a single pair of OSPF routers; a broadcast network supports multiple (more than two) routers and provides the ability to address a single physical message to all of the attached routers; a non-broadcast multi-access network, for example a public switched packet network, supports multiple (more than two) routers but does not provide the ability to address a single physical message to all routers. **Interface Type** selects between these three interface/network types.

If this interface connects to an OSPF broadcast-type media, press `[RETURN]` to accept the default response, **Broadcast**.



```
Wellfleet Communications            NULL_CONFIG        23-Dec-1991      8:44:12
                                     SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Interface Type  :  Broadcast
```

Figure 9-36 OSPF Interface Selection Screen

If this interface connects to a single remote peer, press the `[RIGHTARROW]` to display **Point-to-Point** and then press `[RETURN]`.

If this interface connects to a multi access network such as a PDN, press the `[RIGHTARROW]` to display **Non-Broadcast Multi-Access** and then press `[RETURN]`.

Now proceed to Section 9.7.2.2.1 if you are configuring a broadcast interface, to Section 9.7.2.2.2 if you are configuring a point-to-point interface, or to 9.7.2.2.3 it you are configuring a multi-access interface.

9.7.2.2.1 Broadcast Backbone Interfaces

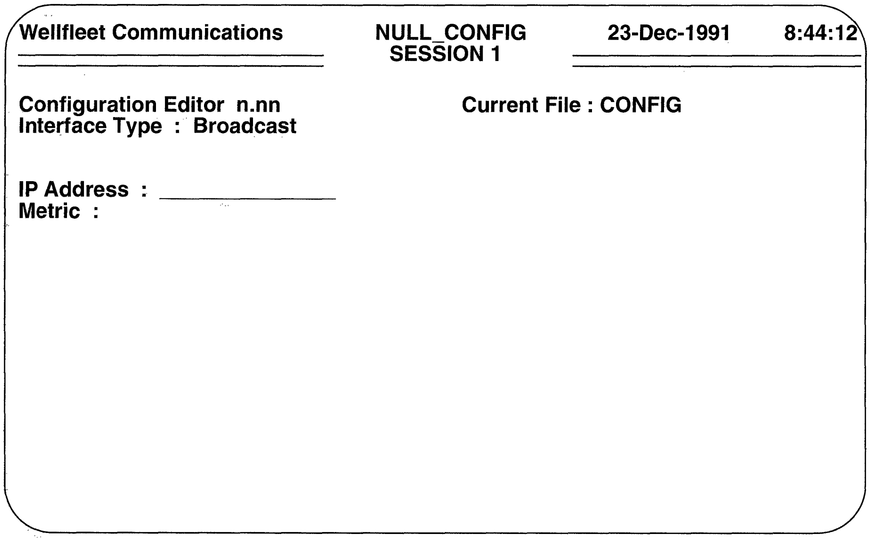
If you are configuring a broadcast-type interface, the screen prompts for additional information (Figure 9-37).

- **IP Address** specifies the IP address of the interface.

  Enter the interface's IP address in dotted decimal notation, and then press `[RETURN]`.

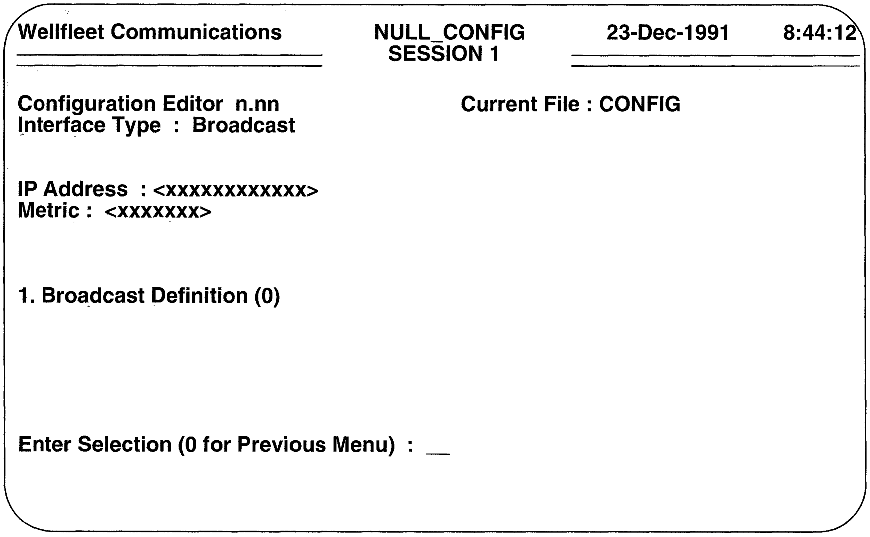
- **Metric** assigns a cost to the transit hop from the router across the interface.

  Enter a cost value from the keyboard, and then press `[RETURN]`.



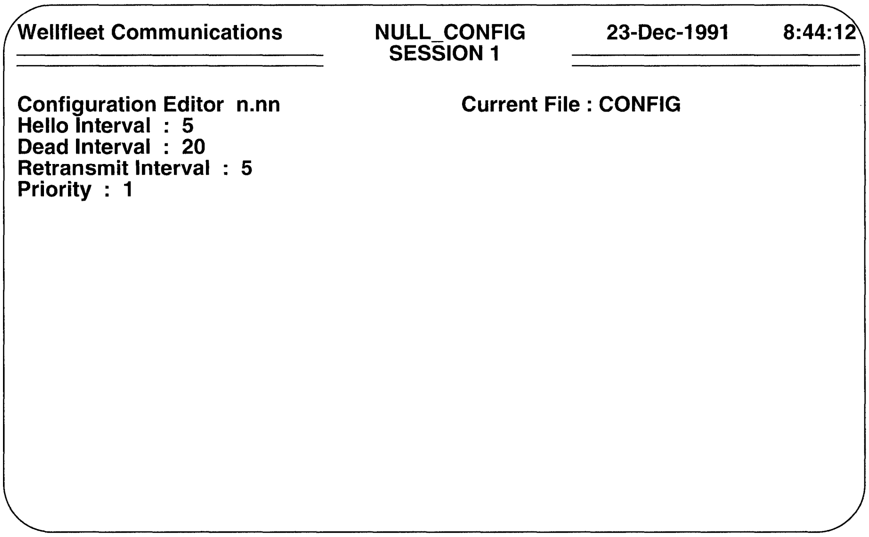
```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Interface Type  :  Broadcast


IP Address  :  _______________
Metric  :
```

Figure 9-37 OSPF Broadcast Interface Parameters Screen



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Interface Type  :  Broadcast


IP Address  : <xxxxxxxxxxxx>
Metric :  <xxxxxxx>


1. Broadcast Definition (0)




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-38 OSPF Broadcast Definition Access Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Hello Interval  :  5
Dead Interval  :  20
Retransmit Interval  :  5
Priority  :  1
```

Figure 9-39 OSPF Broadcast Definition Detailed Parameters Screen

After you press `[RETURN]`, the screen prompts for additional information (Figure 9-38).

At **Enter Selection (0 for Previous Menu)** enter `<1>` and then press `[RETURN]`. The screen displays the following:

No Broadcast Definition record(s) found
Do you wish to add Broadcast Definition record(s)?

Press `[RETURN]` to display the OSPF Broadcast Definition Detailed Parameters Screen (Figure 9-39).

❐ **Hello Interval** specifies the number of seconds between the router's transmission of OSPF *Hello* packets.

Hello packets are transmitted across each OSPF interface. On broadcast interfaces they are used to elect the designated and the backup designated router, and to discover and maintain neighbor relationships.

Press `[RETURN]` to accept the default value of **5** seconds, or use the `[RIGHTARROW]` to display one of the other available options (**10**, **15**, **20**, **30**, or **60**) and then press `[RETURN]`.

NOTE

All routers connected to the OSPF backbone must be configured with the same values for **Hello Interval** and **Dead Interval**.

- ❒ **Dead Interval** specifies the number of seconds before a "silent" router is declared down.

  Press `[RETURN]` to accept the default value of **20** seconds, or use the `[RIGHTARROW]` to display one of the other available options (**360**, **300**, **240**, **220**, **200**, **180**, **160**, **140**, **120**, **100**, **80**, **60**, or **40**) and then press `[RETURN]`.

- ❒ **Retransmit Interval** specifies the number of seconds between the router's retransmission of OSPF link state advertisements.

  Press `[RETURN]` to accept the default value of **5** seconds, or use the `[RIGHTARROW]` to display one of the other available options (**30**, **20**, **15**, or **10**) and then press `[RETURN]`.

NOTE

Retransmit Interval should be set to a value greater than the expected round trip delay between any two routers on the backbone.

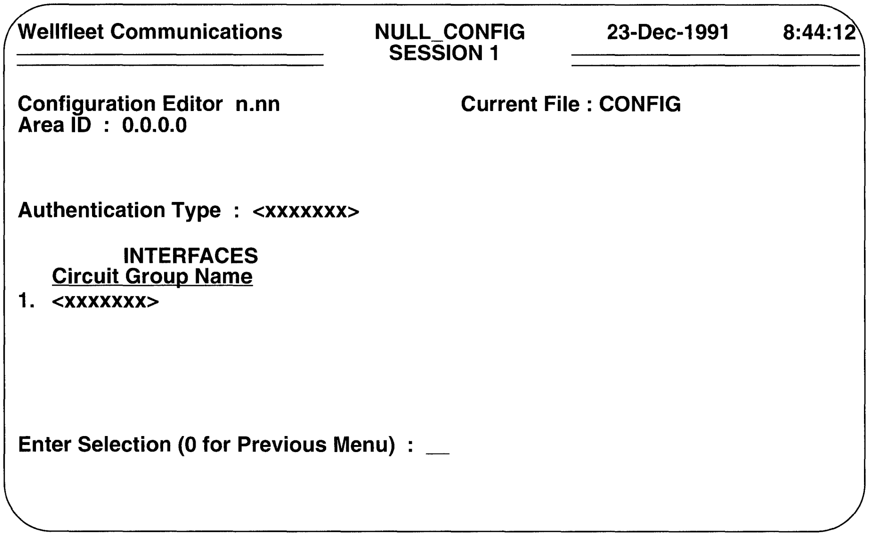
- ❒ **Priority** specifies a weighted value used in the designated router and backup designated router selection algorithm.

  When two routers attached to the backbone both attempt to become designated router, the one with the highest **Priority** value takes precedence. In the case of equal **Priority** values, the router with the highest **Router ID** takes precedence.

  Use the `[RIGHTARROW]` to select one of the available options, from 0 to 15.

After you designate the router priority, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the OSPF Broadcast Definition Access Screen. Now press [`RETURN]` twice to go back to the OSPF Backbone Detailed Parameters Access Screen.

You configure additional OSPF backbone broadcast interfaces from the OSPF Backbone Detailed Parameters Access Screen. To begin, enter `<2>` at **Enter Selection (0 for Previous Menu)** to display the OSPF Backbone Interface Summary Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Area ID  :  0.0.0.0


Authentication Type  :  <xxxxxxx>

            INTERFACES
   Circuit Group Name
1.  <xxxxxxx>




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-40 OSPF Backbone Interface Summary Screen

Press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the OSPF Interface Basic Parameters Screen. Now follow the previously described procedures to configure an additional backbone broadcast interface; continue until you have configured all backbone broadcast interfaces.

9.7.2.2.2 Point-to-Point Backbone Interfaces

If you are configuring a point-to-point type interface, the console screen prompts for additional information as shown in Figure 9-41.

- ❒ **IP Address** specifies the IP address of the interface.

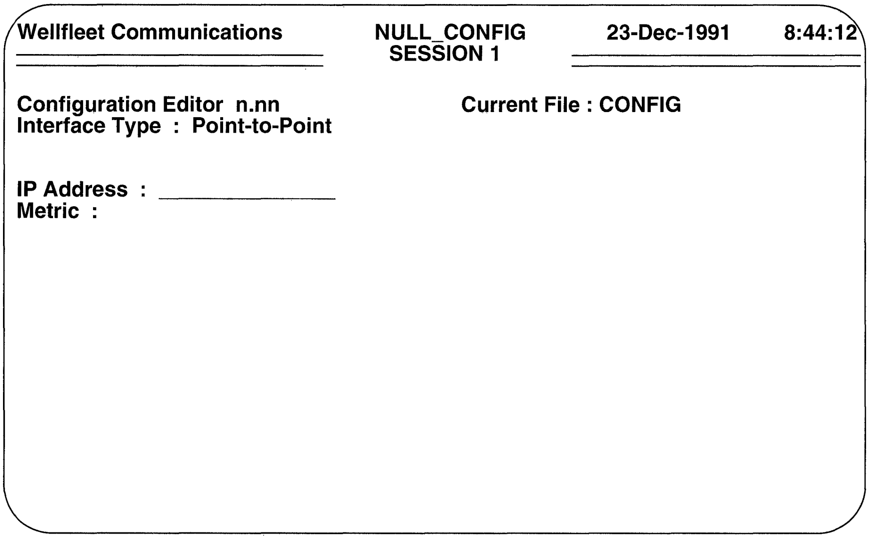
  Enter the interface's IP address in dotted decimal notation, and then press `[RETURN]`.

- ❒ **Metric** assigns a cost to the transit hop from the router across the interface.

  Enter a cost value from the keyboard, and then press `[RETURN]`.

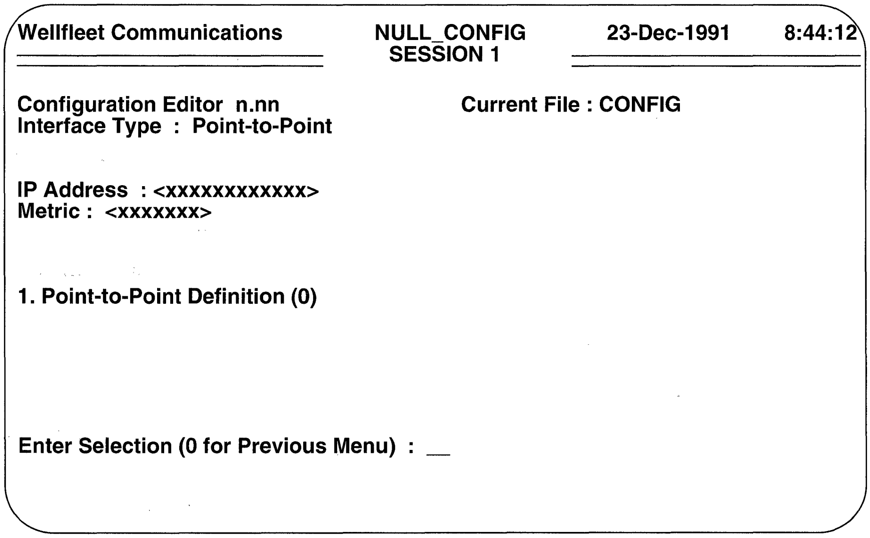
After you press `[RETURN]`, the screen prompts for additional information as shown in Figure 9-42.

At **Enter Selection (0 for Previous Menu)** enter `<1>` and then press `[RETURN]`. The screen displays the following:



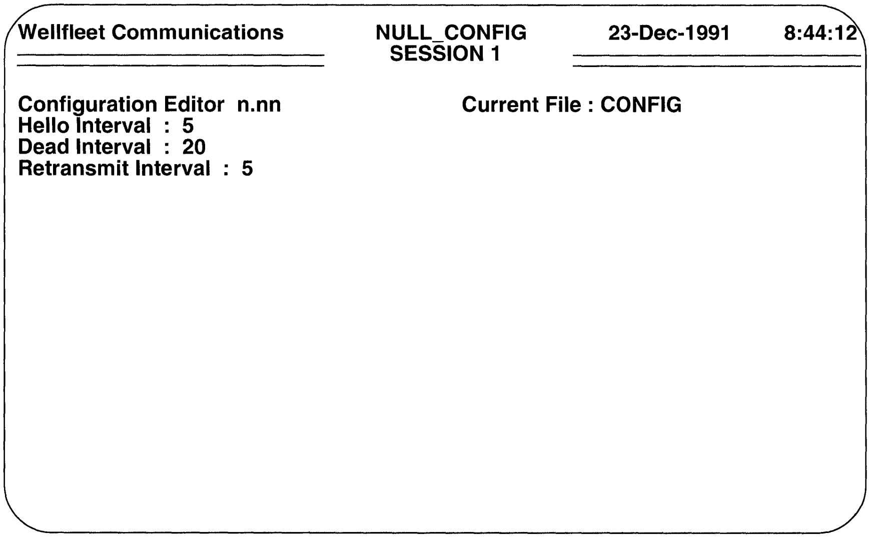
```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Interface Type  :  Point-to-Point


IP Address  :  _______________
Metric  :
```

Figure 9-41 OSPF Point-to-Point Interface Parameters Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Interface Type  :  Point-to-Point


IP Address  : <xxxxxxxxxxxxx>
Metric :  <xxxxxxxx>


1. Point-to-Point Definition (0)




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-42 OSPF Point-to-Point Definition Access Screen



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Hello Interval  :  5
Dead Interval  :  20
Retransmit Interval  :  5
```

Figure 9-43 OSPF Point-to-Point Definition Detailed Parameters Screen

No Point-to-Point Definition record(s) found
Do you wish to add Point-to-Point Definition record(s)?

Press [RETURN] to display the OSPF Point-to-Point Definition Detailed Parameters Screen (Figure 9-43).

❒ **Hello Interval** specifies the number of seconds between the router's transmission of OSPF *Hello* packets.

Hello packets are transmitted across each OSPF interface. On point-to-point interfaces they are used to discover and maintain neighbor relationships.

Press [RETURN] to accept the default value of **5** seconds, or use the [RIGHTARROW] to select one of the other available options.

❒ **Dead Interval** specifies the number of seconds before a "silent" router is declared down.

Press [RETURN] to accept the default value of **20** seconds, or use the [RIGHTARROW] to select one of the other available options.

❒ **Retransmit Interval** specifies the number of seconds between the router's retransmission of OSPF link state advertisements.

Press [RETURN] to accept the default value of **5** seconds, or use the [RIGHTARROW] to select one of the other available options.

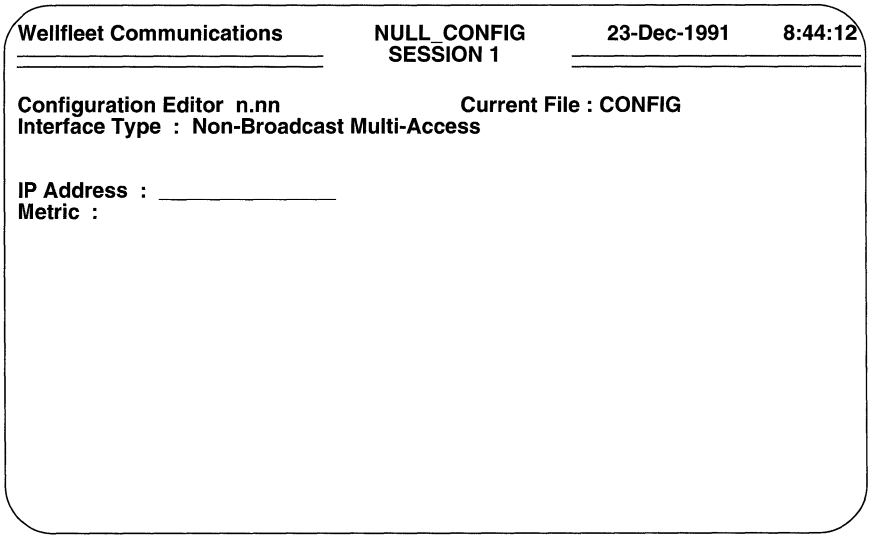
After you designate the retransmit interval, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the OSPF Point-to-Point Definition Access Screen. Now press `[RETURN]` twice to go back to the OSPF Backbone Detailed Parameters Access Screen.

You configure additional OSPF backbone point-to-point interfaces from the OSPF Backbone Detailed Parameters Access Screen. Enter `<2>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen displays the OSPF Backbone Interface Summary Screen.

Press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the OSPF Interface Basic Parameters Screen. Now use the previously described procedures to configure an additional backbone point-to-point interface; continue until you have configured all backbone point-to-point interfaces.

9.7.2.2.3 Non-Broadcast Multi-Access Interfaces

If you are configuring a non-broadcast multi-access type interface, the screen prompts for additional information.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Interface Type  :  Non-Broadcast Multi-Access


IP Address  :  ____________
Metric  :
```

Figure 9-44 OSPF Non-Broadcast Multi-Access Interface Parameters Screen

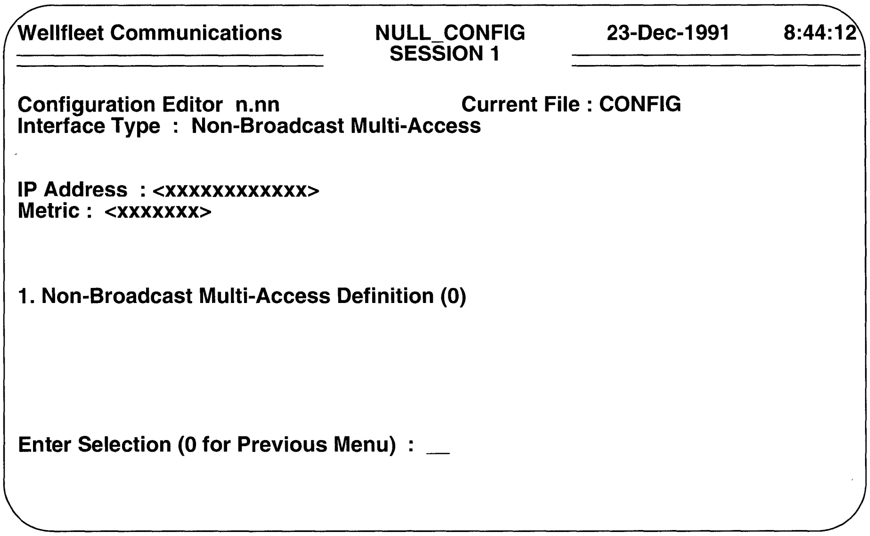
❐ **IP Address** specifies the IP address of the interface.

Enter the interface's IP address in dotted decimal notation, and then press `[RETURN]`.

- ❐ **Metric** assigns a cost to the transit hop from the router across the interface.

  Enter a cost value from the keyboard, and then press `[RETURN]`.

After you press `[RETURN]`, the screen prompts for additional information.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG
Interface Type  :  Non-Broadcast Multi-Access

IP Address  : <xxxxxxxxxxxx>
Metric :  <xxxxxxx>


1. Non-Broadcast Multi-Access Definition (0)




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-45 OSPF Non-Broadcast Multi-Access Definition Access Screen

At **Enter Selection (0 for Previous Menu)** enter `<1>` and then press `[RETURN]`. The screen displays the following:

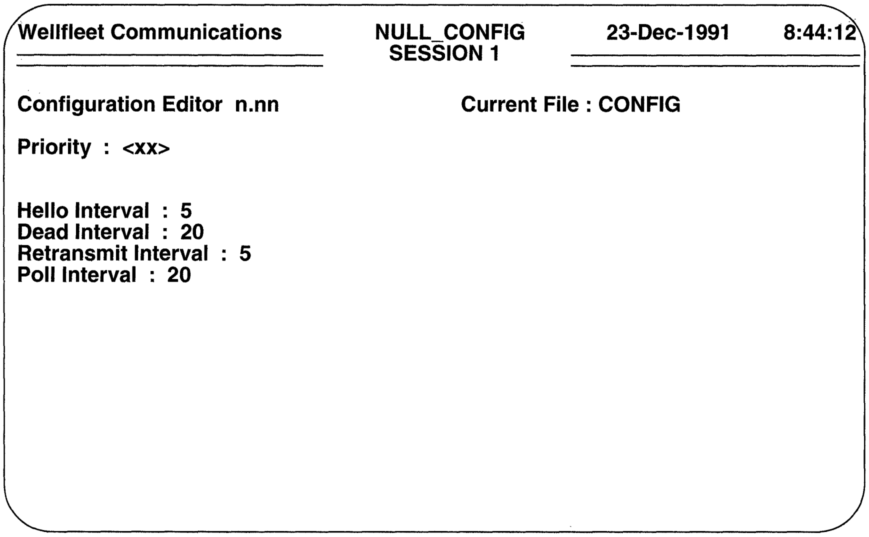
> **No Non-Broadcast Multi-Access Definition record(s) found**
> **Do you wish to add Non-Broadcast Multi-Access Definition record(s)?**

Press `[RETURN]`.

- ❐ **Priority** specifies a weighted value used in the designated router and backup designated router selection algorithm.

  When two routers attached to the backbone both attempt to become designated router, the one with the highest **Priority** value takes precedence. In the case of equal **Priority** values, the router with the highest **Router ID** takes precedence.

  Use the `[RIGHTARROW]` to select one of the available options, from 0 to 15. The screen prompts for additional information as shown in Figure 9-46.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                     Current File : CONFIG

Priority  :  <xx>


Hello Interval  :  5
Dead Interval  :  20
Retransmit Interval  :  5
Poll Interval  :  20
```

Figure 9-46 OSPF Non-Broadcast Multi-Access Definition Detailed Parameters Screen

❒ **Hello Interval** specifies the number of seconds between the router's transmission of OSPF *Hello* packets.

Hello packets are transmitted across each OSPF interface. On point-to-point interfaces they are used to discover and maintain neighbor relationships.

Press `[RETURN]` to accept the default value of **5** seconds, or use the `[RIGHTARROW]` to select one of the other available options.

❒ **Dead Interval** specifies the number of seconds before a "silent" router is declared down.

Press `[RETURN]` to accept the default value of **20** seconds, or use the `[RIGHTARROW]` to select one of the other available options.

❒ **Retransmit Interval** specifies the number of seconds between the router's retransmission of OSPF link state advertisements.

Press `[RETURN]` to accept the default value of **5** seconds, or use the `[RIGHTARROW]` to select one of the other available options.

❒ **Poll Interval** specifies the number of seconds between hello messages transmitted to a "dead neighbor'.

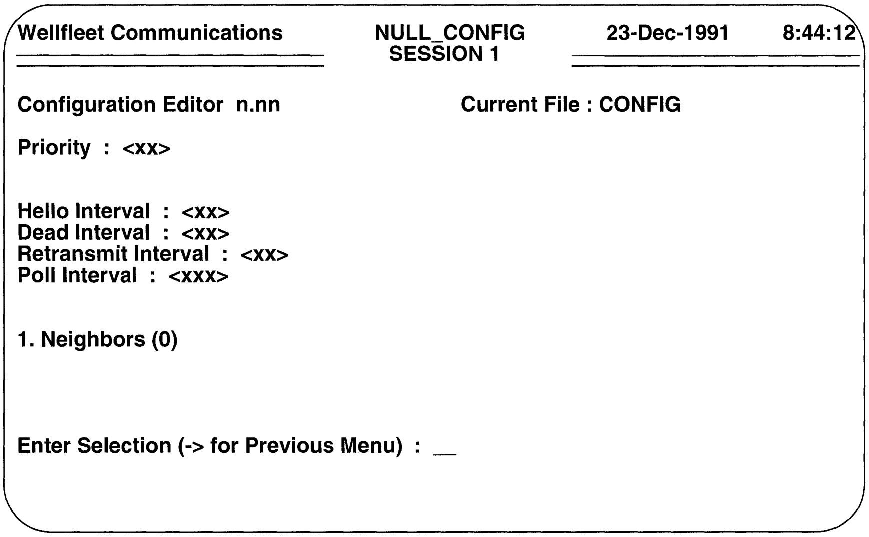
If a neighboring router has become inactive (hellos have not been received for more than **Dead Interval** seconds), it may still be necessary to transmit hello packets at a reduced rate. **Poll Interval** specifies this time period.

Press `[RETURN]` to accept the default value of **20** seconds, or use the `[RIGHTARROW]` to select one of the other available options (from 20 to 200 seconds).

NOTE

You should ensure that **Poll Interval** is considerably larger than **Hello Interval**.

After you specify the **Poll Interval**, the screen prompts for information about neighboring routers on the multi-access network.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Priority  :  <xx>


Hello Interval  :  <xx>
Dead Interval  :  <xx>
Retransmit Interval  :  <xx>
Poll Interval  :  <xxx>


1. Neighbors (0)



Enter Selection (-> for Previous Menu)  :  __
```

Figure 9-47 OSPF Neighbors Access Screen

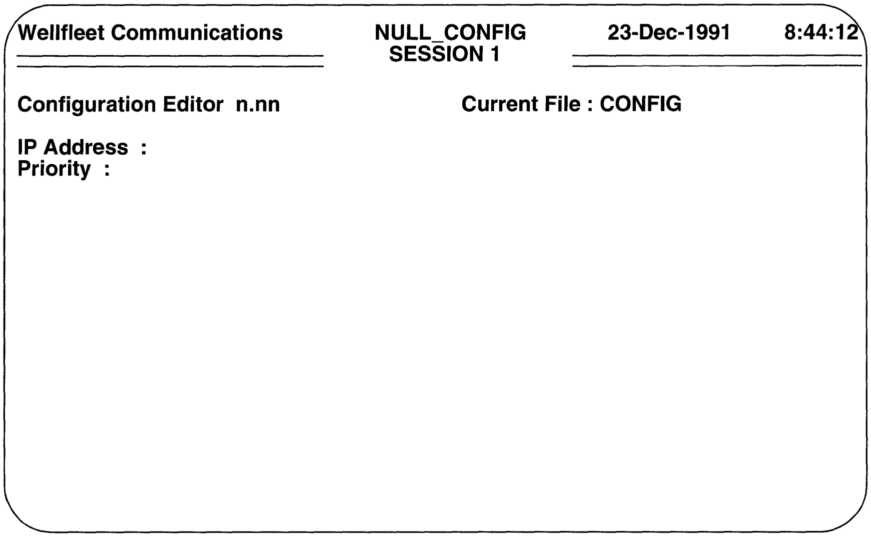
NOTE

Only routers eligible to become designated router (that is with a non-zero value for **Priority**) need configure neighbor information.

At **Enter Selection (0 for Previous Menu)** enter `<1>` and then press `[RETURN]`. The screen displays the following:

No NEIGHBORS record(s) found
Do you wish to add NEIGHBORS record(s)?

Press [RETURN] to display the OSPF Neighbors Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn               Current File : CONFIG

IP Address  :
Priority  :
```

Figure 9-48 OSPF Neighbors Parameters Screen

❐ **IP Address** identifies another router on the non-broadcast multi-access media.

Enter the router's IP address in dotted decimal notation.

❐ **Priority** defines IP Address's eligibility to become designated router.

Enter the router's priority value (from 0 to 15).

When the screen prompts **Hit Return to Continue**, press [RETURN] to go back to the OSPF Neighbors Access Screen. If need be, you can add additional neighbors from this screen. Enter <1> at the prompt to display a list of neighbors, toggle the [RIGHTARROW] to display **Add**, and then press [RETURN] to display the OSPF Neighbors Parameters Screen. Now use the previously described procedure to add additional neighbors; continue until you have added all neighboring routers.

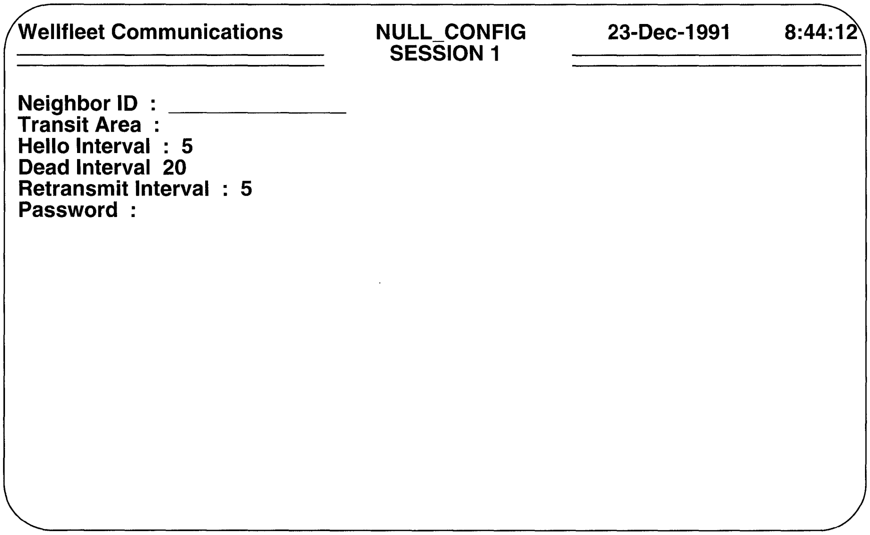
9.7.2.3 Backbone Virtual Links

After configuring backbone interfaces (if any), you configure any virtual links that are required to ensure backbone contiguousness. With reference to Figure 9-26, for example, assuming that router 3 was being configured, you would configure a virtual link from router 3 to router 4.

You begin virtual links configuration from the OSPF Backbone Detailed Parameters Access Screen. Enter <3> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

```
No VIRTUAL LINKS record(s) found
Do you wish to add VIRTUAL LINKS record(s)?
```

Press [RETURN] to display the OSPF Virtual Links Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Neighbor ID : ____________
Transit Area :
Hello Interval : 5
Dead Interval 20
Retransmit Interval : 5
Password :
```

Figure 9-49 OSPF Virtual Links Parameters Screen

❒ **Neighbor ID** identifies the remote end of the virtual link.

Enter the router ID (in dotted decimal notation) of the remote end.

❒ **Transit Area** identifies the OSPF area through which traffic to **Neighbor ID** is forwarded.

Enter the area ID (in dotted decimal notation) of the transit area.

❒ **Hello Interval** specifies the number of seconds between the router's transmission of OSPF *Hello* packets.

Press [RETURN] to accept the default value of **5** seconds, or use the [RIGHTARROW] to select one of the other available options.

- ❒ **Dead Interval** specifies the number of seconds before a "silent" router is declared down.

  Press [RETURN] to accept the default value of **20** seconds, or use the [RIGHTARROW] to select one of the other available options.

- ❒ **Retransmit Interval** specifies the number of seconds between the TCP/IP router's retransmission of OSPF link state advertisements.

  Press [RETURN] to accept the default value of **5** seconds, or use the [RIGHTARROW] to select one of the other available options.

- ❒ **Password** specifies the authentication key used across the virtual interface.

  If you do not want authentication across the virtual link, press [RETURN].

  If you want to enable authentication, **Password** specifies a one-to-eight character ASCII string that appears in the authentication field of all OSPF packets across this interface. Enter the character string and then press [RETURN].

After you designate the password, the screen prompts **Hit Return to Continue**. Press [RETURN] to go back to the OSPF Backbone Detailed Parameters Access Screen.

You configure additional virtual links from the OSPF Backbone Detailed Parameters Access Screen. Enter <3> at **Enter Selection (0 for Previous Menu)** to display the OSPF Backbone Virtual Links Summary Screen (Figure 9-50). At **Action (--> for Selections)** press the [RIGHTARROW] to display **Add** and then press [RETURN]. The screen displays the OSPF Virtual Links Parameters Screen. Now proceed as before to configure an additional virtual link; continue until you have configured all backbone virtual links.

9.7.3 Configuring OSPF Areas

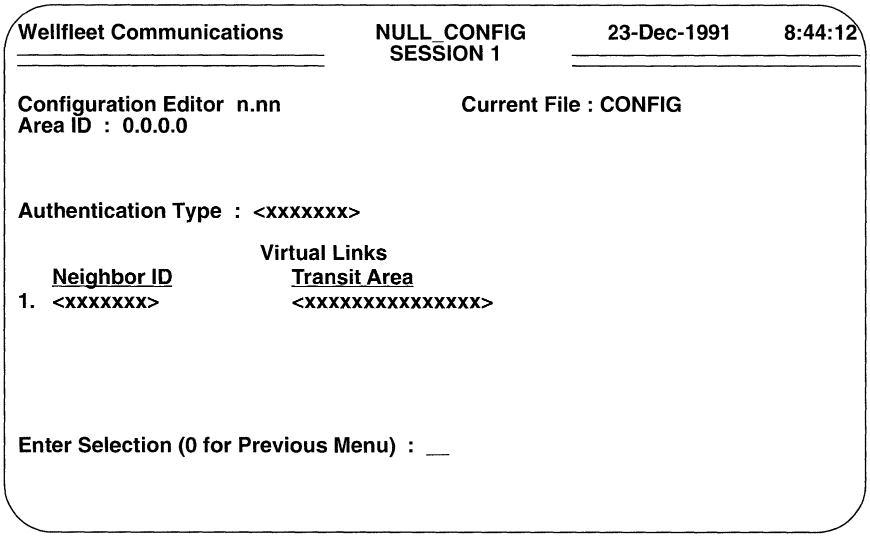
You configure OSPF areas from the OSPF Area Access Screen (Figure 9-28). Enter <1> at **Enter Selection (0 for Previous Menu)**. If you have not previously configured the OSPF backbone, the screen displays the following:

No AREAS record(s) found
Do you wish to add AREAS record(s)?

Press [RETURN] to display the OSPF Area Identification Screen (Figure 9-29).

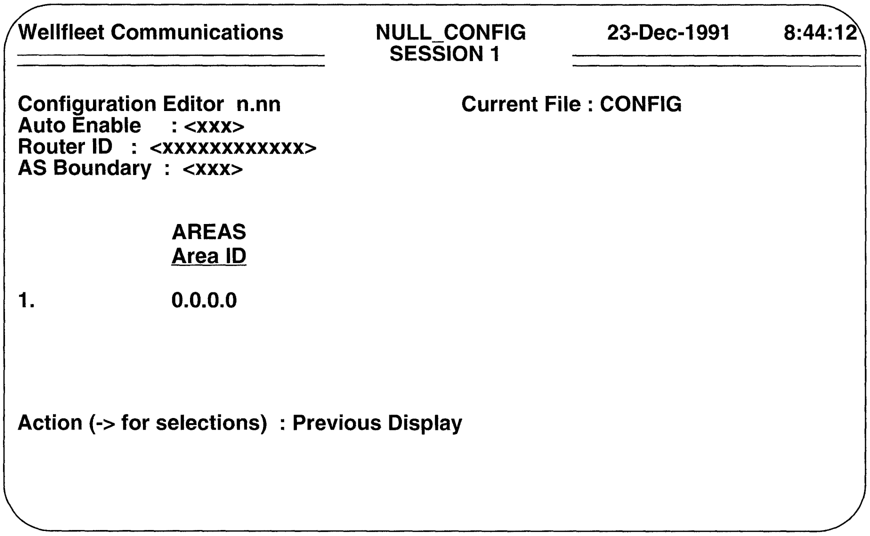
If you have previously configured the OSPF backbone (OSPF area 0.0.0.0), the screen displays the OSPF Area Summary Screen (Figure 9-51).

At **Action (--> for Selections)** press the [RIGHTARROW] to display **Add** and then press [RETURN]. The screen displays the OSPF Area Identification Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                        Current File : CONFIG
Area ID  :  0.0.0.0


Authentication Type  :  <xxxxxxx>

                              Virtual Links
   Neighbor ID                   Transit Area
1.  <xxxxxxx>                    <xxxxxxxxxxxxxxx>




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-50 OSPF Backbone Virtual Links Summary Screen



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                        Current File : CONFIG
Auto Enable     : <xxx>
Router ID   :  <xxxxxxxxxxxx>
AS Boundary  :  <xxx>


                  AREAS
                  Area ID

1.                0.0.0.0




Action (-> for selections)  : Previous Display
```

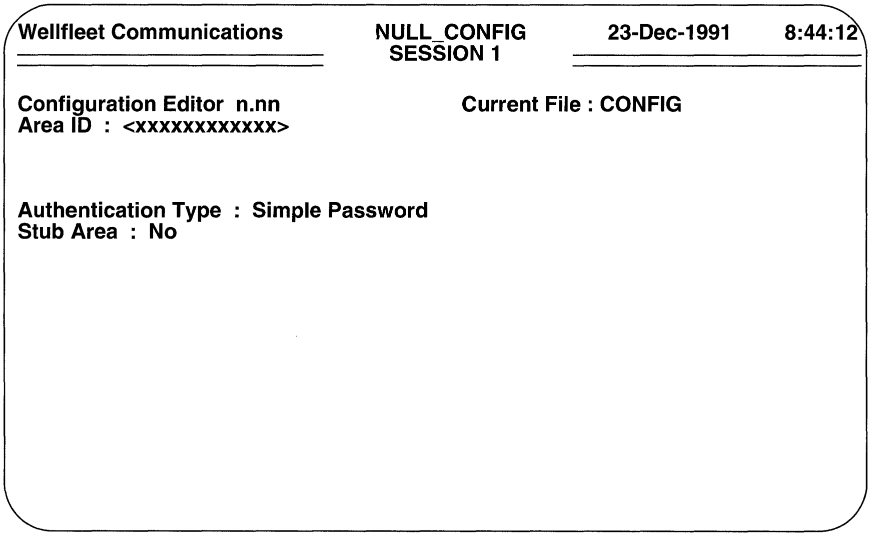
Figure 9-51 OSPF Area Summary Screen

At **Area ID** enter a dotted decimal 32-bit number (for example, `1.1.1.1`) that identifies the area. If you are assigning subnetted networks as different areas, you can use the 32-bit network address as the Area ID.

NOTE

The value of 0.0.0.0 is reserved for the backbone **Area ID**.

After you specify the Area ID, the screen displays the OSPF Area Basic Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Area ID  :  <xxxxxxxxxxxx>


Authentication Type  :  Simple Password
Stub Area  :  No
```

Figure 9-52 OSPF Area Basic Parameters Screen

- **Authentication Type** enables or disables password authentication.

  All OSPF packet exchanges can be authenticated by means of a password contained within the OSPF packet. Authentication is enabled on an area basis.

  To enable password authentication within this OSPF area, press `[RETURN]` to accept the default response, **Simple Password**. To disable password authentication, press the `[RIGHTARROW]` to display **No Authentication** and then press `[RETURN]`.

OSPF distinguishes between two types of areas: *transit areas* that can carry/pass through traffic that is neither locally originated nor locally destined and *stub areas* that carry traffic that is either locally originated or destined.

- □ **Stub Area** specifies the area type.

  If this OSPF area will carry transit traffic (packets originated by or destined for other OSPF areas), press `[RETURN]` to accept the default response, **No**.

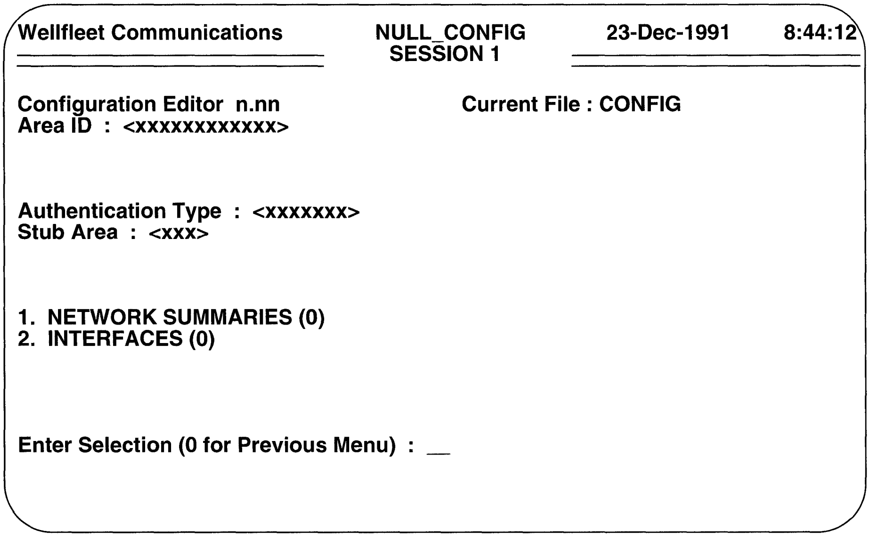
  Otherwise, press the `[RIGHTARROW]` to display **Yes** and then press `[RETURN]`.

After you specify a stub area, the screen prompts for **Metric** data.

- □ **Metric** assigns a cost to the transit hop from the router to the stub network.

  Enter a cost value from the keyboard, and then press `[RETURN]`.

After you specify the area type the console screen displays the OSPF Area Detailed Parameters Access Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Area ID  :  <xxxxxxxxxxxx>


Authentication Type  :  <xxxxxxx>
Stub Area  :  <xxx>


1.  NETWORK SUMMARIES (0)
2.  INTERFACES (0)



Enter Selection (0 for Previous Menu)  :  _
```

Figure 9-53 OSPF Area Detailed Parameters Access Screen

9.7.3.1 Area Networks

OSPF areas have been previously defined as a collection of networks. More precisely, OSPF areas are actually composed of a list of address ranges. Each address range is defined by an address/mask pair.

You specify area resident networks from the OSPF Area Detailed Parameters Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No NETWORK SUMMARIES record(s) found
Do you wish to add NETWORK SUMMARIES record(s)?

Press `[RETURN]` to display the OSPF Network Identification Screen.

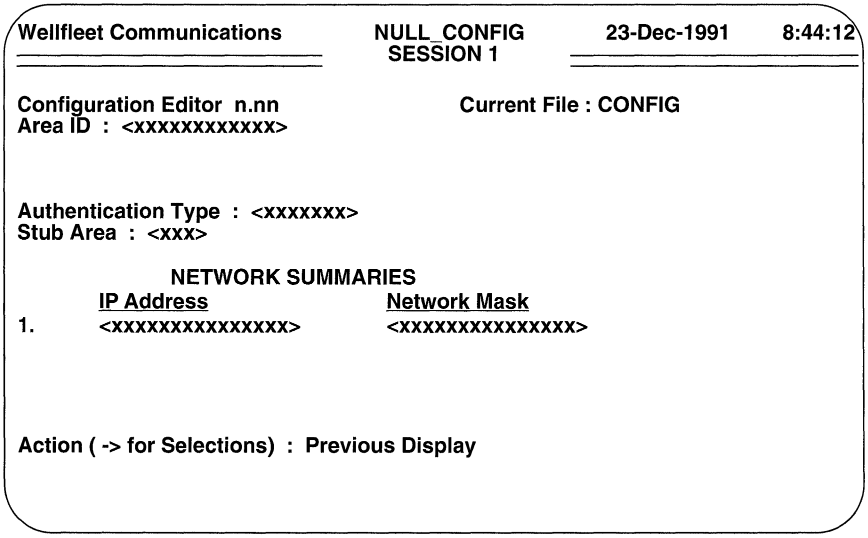
❒ **IP Address** identifies an IP network resident within this OSPF area.

Enter the IP network address in dotted decimal notation, and then press `[RETURN]`.

❒ **Network Mask** specifies the network/sub-net mask value (identifying those bits in the 32-bit IP address that specify `Net_ID` and `Subnet_ID`).

Enter the mask value in dotted decimal notation, and then press `[RETURN]`.

After you specify the network mask, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the OSPF Area Detailed Parameters Access Screen. If necessary, you add networks to the OSPF area from this screen. To add a network, enter `<1>` at **Enter Selections (0 for Previous Menu)**. The screen displays the OSPF Area Networks Summary Screen.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Area ID  :  <xxxxxxxxxxxx>



Authentication Type  :  <xxxxxxx>
Stub Area  :  <xxx>

                NETWORK SUMMARIES
        IP Address                  Network Mask
1.      <xxxxxxxxxxxxxxx>           <xxxxxxxxxxxxxxx>




Action ( -> for Selections)  :  Previous Display
```

Figure 9-54 OSPF Area Networks Summary Screen

Press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]` to display the OSPF Network Identification Screen. Now proceed as before to add network information; continue until you have specified all area networks.

9.7.3.2 Area Interfaces

After completing the list of address ranges, you configure the actual interface(s) between the router and this OSPF area which it serves.

You begin the router/area interface configuration from the OSPF Area Detailed Parameters Access Screen. Enter `<2>` at the **Enter Selection (0 for Previous Menu)** prompt. The screen displays the following:

No INTERFACE record(s) found
Do you wish to add INTERFACE record(s)?

Press `[RETURN]` to display the OSPF Interface Basic Parameters Screen (Figure 9-34).

❒ **Circuit Group Name** identifies the circuit group that provides the interface between the router and the OSPF area.

Enter the name of the circuit group.

❒ **Password** specifies the authentication key used across this interface.

If you have not enabled authentication within this OSPF area, press `[RETURN]`.

If you have enabled authentication, **Password** specifies a one-to-eight character ASCII string that appears in the authentication field of all OSPF packets across this interface. Enter the character string from the keyboard, and then press `[RETURN]`.

After you press `[RETURN]`, the screen prompts for additional interface-specific data. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Interface Definition record(s) found
Do you wish to add Interface Definition record(s)?

Press `[RETURN]` to display the OSPF Interface Selection Screen (Figure 9-36).

OSPF recognizes three types of interface (or networks): a point-to-point network connects a single pair of OSPF routers; a broadcast network supports multiple (more than two) routers and provides the ability to address a single physical message to all of the attached routers; a non-broadcast multi-access network, for example a public switched packet network, supports multiple (more than two) routers but does not provide the ability to address a single physical message to all routers.

Interface Type selects between these three interface/network types.

If this interface connects to an OSPF broadcast-type media, press `[RETURN]` to accept the default response, **Broadcast**.

If this interface connects to a single remote peer, press the `[RIGHTARROW]` to display **Point-to-Point** and then press `[RETURN]`.

If this interface connects to a multi access network such as a PDN, press the `[RIGHTARROW]` to display **Non-Broadcast Multi-Access** and then press `[RETURN]`.

Now use the procedures previously described in Section 9.7.2.2.1 if you are configuring a broadcast interface, Section 9.7.2.2.2 if you are configuring a point-to-point interface, or Section 9.7.2.2.3 if you are configuring a non-broadcast multi-access interface.

9.7.3.3 Configuration of Additional OSPF Areas

You configure additional OSPF areas from the OSPF Area Access Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the OSPF Area Summary Screen. Press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`. The screen prompts for **Area ID**. Now follow the previously described procedures to configure an additional OSPF area; repeat these procedures until you have configured all OSPF areas.

9.8 Configuring EGP

The Exterior Gateway Protocol (EGP) enables the exchange of routing information between routers in different autonomous systems. If your router functions in such a topology, use the procedures described in this section to configure EGP.

You configure EGP from the TCP/IP Detailed Parameters Access Screen. Enter `<5>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No EGP Configuration record(s) found
Do you wish to add EGP Configuration record(s)?

Press `[RETURN]`. The screen prompts **Auto Enable**.

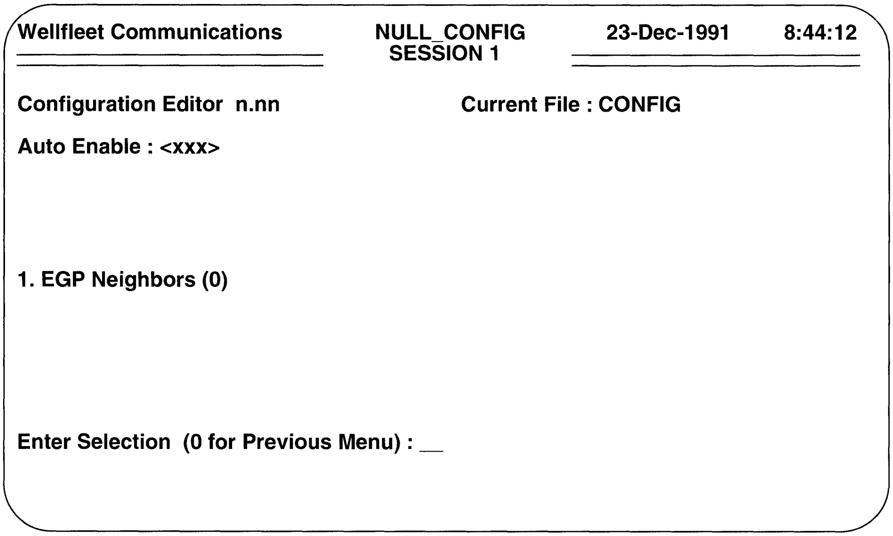
❒ **Auto Enable** specifies the initial state of EGP.

This EGP-specific **Auto Enable** works in conjunction with the global auto enable parameter (refer to Section 2.1) to enable or disable EGP when the router boots.

When global auto enable is **No**, EGP is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable EGP with NCL commands after the router boots.

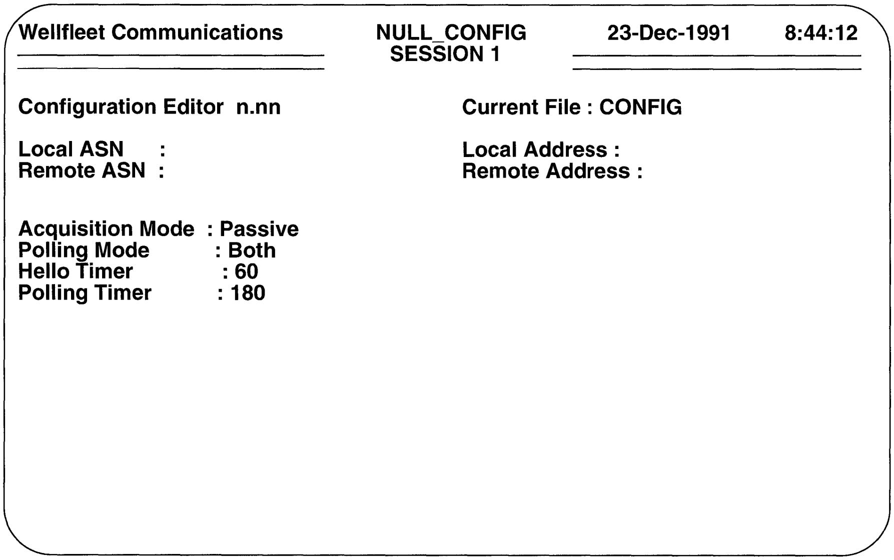
When global auto enable is **Yes**, EGP is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to display either **Yes** (enable EGP) or **No** (disable EGP), then press `[RETURN]`. If you select **No**, you will later need to enable EGP with NCL commands after the router boots.

After you press `[RETURN]`, the screen prompts for **EGP Neighbors** (Figure 9-55).



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG

Auto Enable : <xxx>



1. EGP Neighbors (0)




Enter Selection  (0 for Previous Menu) : __
```

Figure 9-55 EGP Neighbors Screen



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG

Local ASN     :                               Local Address :
Remote ASN  :                                 Remote Address :

Acquisition Mode  : Passive
Polling Mode        : Both
Hello Timer          : 60
Polling Timer        : 180
```

Figure 9-56 EGP Parameters Screen

A neighbor is a router in a remote autonomous system with which the local router exchanges routing information. To begin identifying such neighbors, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

> **No EGP Neighbors record(s) found**
> **Do you wish to add EGP Neighbors record(s)?**

Press `[RETURN]` to display the EGP Parameters Screen (Figure 9-56).

❐ **Local ASN** is the NIC-assigned decimal number that identifies the local autonomous system.

Enter this number.

❐ **Local Address** is the IP address of the local interface that provides the connection to the remote autonomous system.

Enter this address in dotted decimal notation.

❐ **Remote ASN** is the NIC-assigned decimal number that identifies the remote autonomous system.

Enter this number.

❐ **Remote Address** is the IP address of the remote interface that provides the connection to the remote autonomous system.

Enter this address in dotted decimal notation.

❐ **Acquisition Mode** specifies which of the two neighbors initiates EGP connections.

EGP connections are initiated when one neighbor issues an *acquisition request message*, and finalized when the recipient of the *acquisition request message* issues an *acquisition confirm response.* A neighbor who issues *acquisition request messages* is said to be active; a neighbor who responds to such messages is said to be passive. Although the EGP protocol allows both neighbors to be active, protocol efficiency is enhanced when one neighbor is active and the other neighbor is passive.Press the `[RIGHTARROW]` to select **Active** or **Passive**.

❐ **Polling Mode** specifies one of two neighbor-reachability algorithms.

In the active mode, the router issues periodic *Hello* and *Poll* commands. Neighbor-reachability is verified by receipt of corresponding I-H-U (i hear you) and Update responses. In the passive mode, the router does not issue *Hello* commands; nor does it expect I-H-U responses. Neighbor-reachability is verified by examining the Status field of received *Hello* or *Poll* commands, or of Update responses. Although the EGP protocol allows both neighbors to be active, protocol efficiency is enhanced when one neighbor is active and the other neighbor is passive.

Active places the local EGP in active mode; **Passive** places the local EGP in passive mode; **Both** allows neighboring EGPs to arbitrate a mutually agreeable neighbor-reachability algorithm.

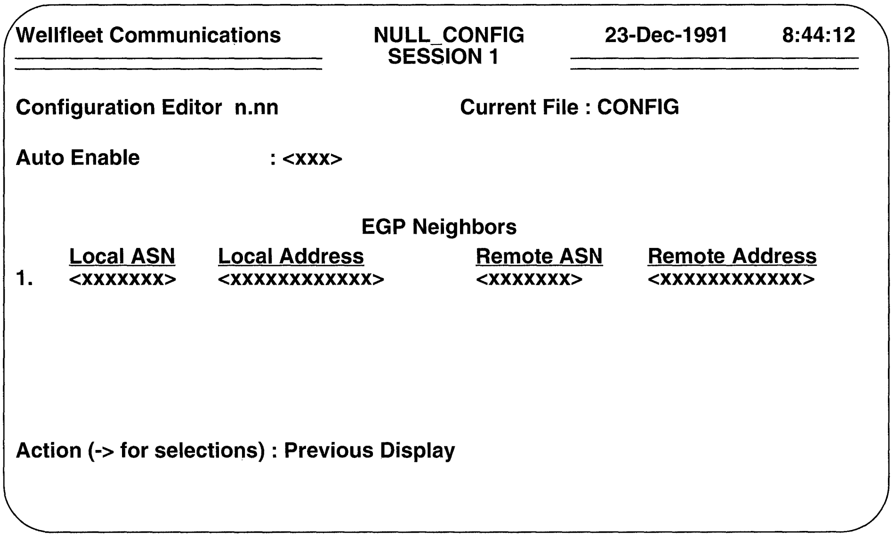
- ❐ **Hello Timer** specifies the time interval between *Hello* commands.

  Press `[RETURN]` to accept the default value of 60 seconds, or enter a new value, and then press `[RETURN]`.

- ❐ **Polling Timer** specifies the time interval between *Poll* Commands.

  Press `[RETURN]` to accept the default value of 180 seconds, or enter a new value, and then press `[RETURN]`.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the EGP Neighbors Screen. You can identify an additional neighbor from this screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the EGP Neighbors Summary Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG

Auto Enable              : <xxx>

                                EGP Neighbors
     Local ASN    Local Address       Remote ASN    Remote Address
1.   <xxxxxxx>    <xxxxxxxxxxxx>      <xxxxxxx>     <xxxxxxxxxxxx>

Action (-> for selections) : Previous Display
```

Figure 9-57 EGP Neighbors Summary Screen

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the EGP Parameters Screen. Now follow the same procedures as before to configure an additional EGP neighbor; repeat these procedures until you have configured all such neighbors.

9.9 Configuring TCP

The Transmission Control Protocol (TCP) is the Internet standard connection-mode, transport-level protocol. You need not assign values to TCP parameters while configuring IP. Accepting default TCP parameters ensures operational efficiency.

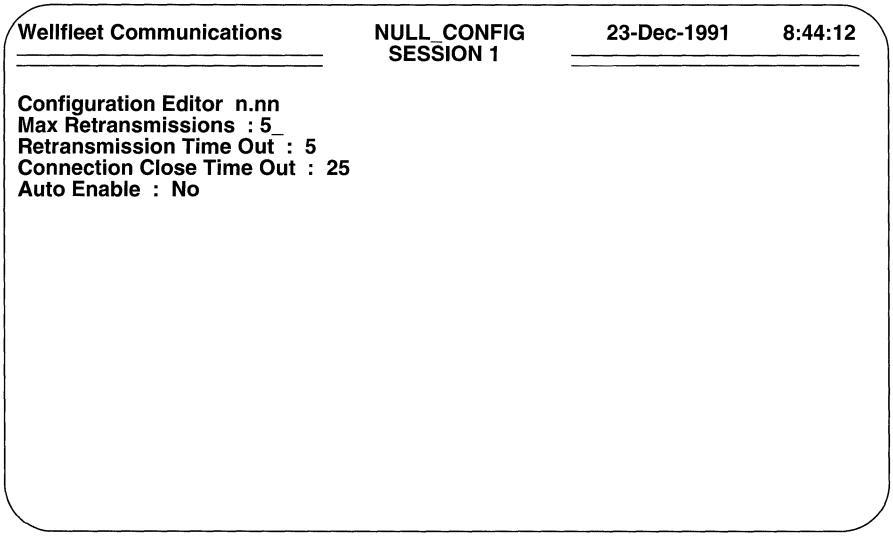
9.10 Configuring TFTP

The IP router includes a client and server implementation of the Trivial File Transfer Protocol (TFTP), a protocol to transmit files across an internet. TFTP is implemented on top of UDP to read and write files from/to a remote device. It cannot list directories nor does it provide for user authentication.

You configure TFTP from the TCP/IP Detailed Parameters Access Screen. Enter <7> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No TFTP Configuration record(s) found
Do you wish to add TFTP Configuration record(s)?

Press `[RETURN]` to display the TFTP Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn
Max Retransmissions  : 5_
Retransmission Time Out  :  5
Connection Close Time Out  :  25
Auto Enable  :  No
```

Figure 9-58 TFTP Parameters Screen

- ❒ **Max Retransmissions** specifies the number of times TFTP retransmits an unacknowledged data message before abandoning the transfer attempt.

  Press `[RETURN]` to select the default value of **5**, or enter a retransmission value from the keyboard.

❒ **Retransmission Time Out** specifies the number of seconds TFTP waits for an acknowledgment before retransmitting a data message.

Press `[RETURN]` to select the default value of **5** seconds, or enter a time out value from the keyboard.

❒ **Connection Close Time Out** specifies the number of seconds TFTP waits before relinquishing resources after it has successfully completed a file transfer.

Press `[RETURN]` to select the default value of **25** seconds, or enter a time out value from the keyboard.

❒ **Auto Enable** specifies the initial state of TFTP.

This TFTP-specific **Auto Enable** works in conjunction with the global auto enable parameter (refer to Section 2.1) to enable or disable TFTP when the router boots.

When global auto enable is **No**, TFTP is unconditionally disabled. If you have set global auto enable to **No**, press `[RETURN]`. You will later need to enable TFTP with NCL commands after the router boots.

When global auto enable is **Yes**, TFTP is conditionally enabled. If you have set global auto enable to **Yes**, press the `[RIGHTARROW]` to either **Yes** (enable TFTP) or **No** (disable TFTP), then press `[RETURN]`. If you select **No**, you will later need to enable TFTP with NCL commands after the router boots.

NOTE

The default state of TFTP is disabled (**Auto Enable** is **No**). Because TFTP allows write access to the router's diskette, it is recommended that TFTP *not* be configured to auto enable in environments where security is of concern.

After the screen prompts **Hit Return to Continue**, press `[RETURN]` to go back to the TCP/IP Detailed Parameters Access Screen.

9.11 BOOTP

The router provides both a client and server implementation of the Bootstrap Protocol (BOOTP) as specified in RFC 951. The BOOTP client implementation enables the router to reboot itself over one of its network connections. The BOOTP server implementation enables the router to act as a bootserver for another router on a directly attached network.

NOTE

Both BOOTP client and server operations require that TCP/IP, TFTP, and BOOTP be configured and enabled.

9.11.1 Configuring the BOOTP Client

With the BOOTP client enabled, the router broadcasts a BOOTP request packet over each of its interfaces, and awaits a reply from an adjacent BOOTP server. If no response is received within a timeout period, the router repeats the broadcast up to a specified number of times. Each repetition is spaced exponentially and randomized by the BOOTP client to avoid collisions.

Upon receipt of a BOOTP reply packet, the router invokes TFTP to obtain the image and configuration files specified in the reply packet. It then reboots with these new files.

If no BOOTP reply packet is received, the router aborts the network boot attempt and uses the currently loaded image and configuration files.

NOTE

Proper operation of BOOTP client requires that a BOOTP server reside on a directly attached network, and that the server be configured to load the appropriate software image (*ace.out*) and, optionally, configuration file to the client.

You configure BOOTP client from the TCP/IP Detailed Parameters Access Screen. Enter `<8>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No BOOTP Configuration record(s) found
Do you wish to add BOOTP Configuration record(s)?

Press `[RETURN]` to display the BOOTP Client Parameters Screen (Figure 9-59).

- ❐ **Max Retransmissions** specifies the number of times that the BOOTP client retransmits a BOOTP request packet.

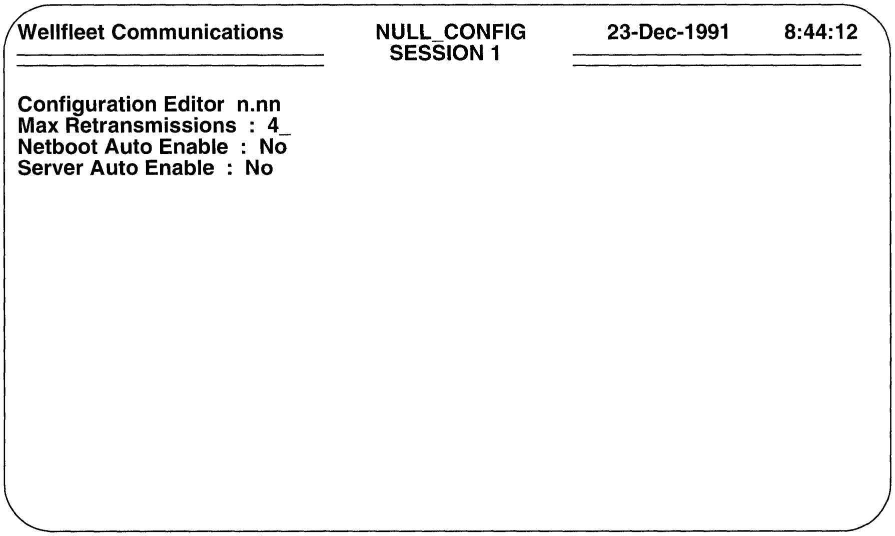
  Enter a value from the keyboard.

- ❐ **Netboot Auto Enable** enables or disables the BOOTP client.

  Press the `[RIGHTARROW]` to enable the BOOTP client (**Yes**) or disable the BOOTP client (**No**).

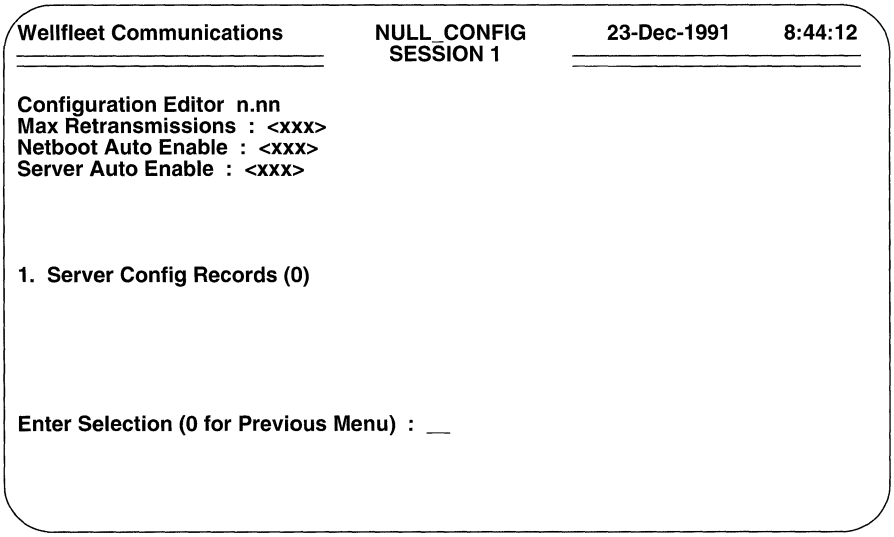
- ❐ **Server Auto Enable** enables or disables the BOOTP server.

  Press the `[RIGHTARROW]` to enable the BOOTP server (**Yes**) or disable the BOOTP server (**No**).



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn
Max Retransmissions  :  4_
Netboot Auto Enable  :  No
Server Auto Enable  :  No
```

Figure 9-59 BOOTP Client Parameters Screen

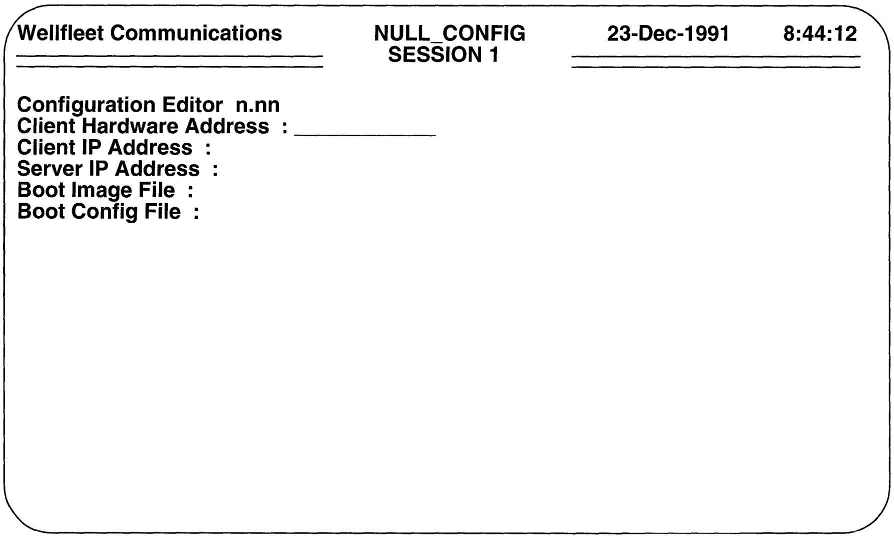


```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn
Max Retransmissions  :  <xxx>
Netboot Auto Enable  :  <xxx>
Server Auto Enable  :  <xxx>



1.  Server Config Records (0)




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-60 BOOTP Server Access Screen

After you enable/disable the BOOTP server, the screen prompts for BOOTP server information (Figure 9-60). If you do not want the router to function as a BOOTP server (**Server Auto Enable** equals **No**), enter <0> at **Enter Selection (0 for Previous Menu)** to return to the TCP/IP Detailed Parameters Access Screen.

If you do want the router to function as a BOOTP server (**Server Auto Enable** equals **Yes**), enter <1> at **Enter Selection (0 for Previous Menu)** to display the BOOTP Server Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                SESSION 1

Configuration Editor  n.nn
Client Hardware Address : __________
Client IP Address :
Server IP Address :
Boot Image File :
Boot Config File :
```

Figure 9-61 BOOTP Server Parameters Screen

9.11.2 Configuring the BOOTP Server

With the BOOTP server enabled, the router functions as a bootserver for specified routers on directly attached networks. It listens for BOOTP request packets from known routers on well-known UDP port 67. Upon reception of a request packet, the router extracts the client's hardware and IP address from the packet and attempts to match them against an entry in its BOOTP server database.

If the lookup fails, the router drops the request; it issues no BOOTP reply packet.

NOTE

"Booting through gateways" is not supported. The BOOTP server does not broadcast request packets across its other interfaces. It responds to the request packet directly, or not at all.

If the lookup succeeds, the router constructs a BOOTP reply packet which contains the IP address of a BOOTP server, the name of a boot file, and (optionally) the name of a configuration file to be used by the client.

You configure the BOOTP server from the BOOTP Server Access Screen . Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Server Config Records record(s) found
Do you wish to add Server Config Records record(s)?

Press `[RETURN]` to display the BOOTP Server Parameters Screen.

- ❐ **Client Hardware Address** (in conjunction with **Client IP Address**) designates a device for which the router provides BOOTP service.

  Enter the 48-bit address of a BOOTP-client router on a directly attached network.

- ❐ **Client IP Address** (in conjunction with **Client Hardware Address**) designates a device for which the router provides BOOTP service.

  Enter the dotted decimal IP address that resolves to **Client Hardware Address**.

- ❐ **Server IP Address** designates the source of the boot file.

  Enter the dotted decimal IP address of the device that supplies the boot file.

NOTE

The source of the boot file need not be the router itself; the router can return the address of another network device (for example, a SUN workstation) which is configured to supply the named files upon request.

- ❐ **Boot Image File** contains the name of the boot file.

  If the router supplies the boot image, enter the name of the file on the local disk (for example, *ace.out*). If another device supplies the boot image, enter the full pathname to the file (for example, */usr3/wf/wf_exec/5.60/cat.out*). Pathnames are restricted to 60 characters in length.

NOTE

If the boot image is supplied by a network device (not by the router), it is recommended that the file be stored under a file name other than *ace.out*.

- ❐ **Boot Config File** contains the name of the configuration file.

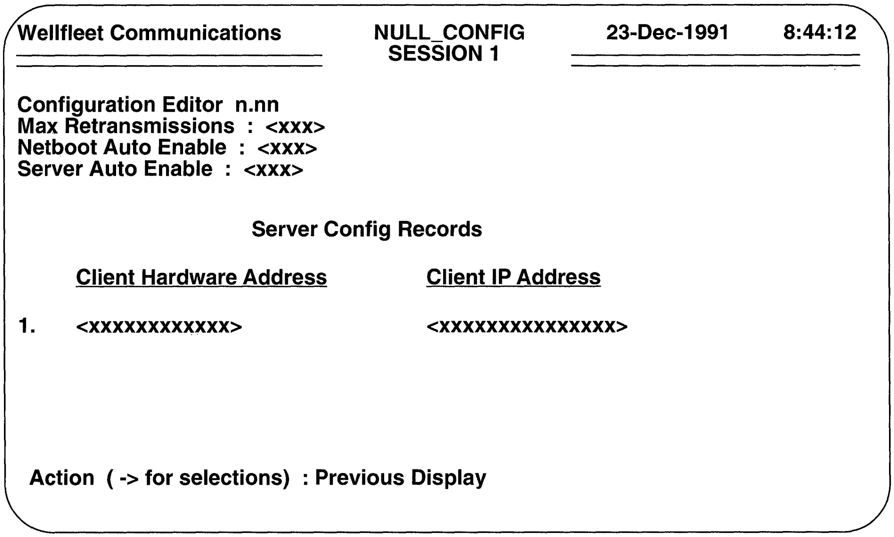
  If you do not wish to specify a configuration file, press `[RETURN]`. If you do wish to specify a configuration file, the BOOTP server makes use of the vendor-specific field of the BOOTP reply packet (numbered tag 129) to convey the name of a configuration file.

If the router supplies the configuration file, enter the name of the file on the local disk (for example, *cfg_2*). If another device supplies the configuration file, enter the full pathname to the file (for example, */usr3/wf/wf_cfg/5.60/cfg_2*). Pathnames are restricted to 60 characters in length.

NOTE

If the configuration file is supplied by a device other than the router, it cannot be stored under the file name *config*.

After you specify the name of a configuration file, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the BOOTP Server Access Screen. You add additional clients to the BOOTP server database from this screen. Enter **<1>** at **Enter Selection (0 for Previous Menu)** to display the BOOTP Server Summary Screen which provides a listing of all Client Hardware Address and Client IP Address pairs contained within the BOOTP server database.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn
Max Retransmissions  :  <xxx>
Netboot Auto Enable  :  <xxx>
Server Auto Enable  :  <xxx>

                          Server Config Records

      Client Hardware Address              Client IP Address

1.    <xxxxxxxxxxxxx>                      <xxxxxxxxxxxxxxxx>



  Action  ( -> for selections)  : Previous Display
```

Figure 9-62 BOOTP Server Summary Screen

To add a client to the database press the `[RIGHTARROW]` at **Action (-> for selections)** to display **Add**, and then press `[RETURN]`. The screen displays the BOOTP Server Parameters Screen. Now proceed as before to add another client. Continue with this procedure until you have completed the BOOTP server database.

9.12 Managing the Routing Pool

Routing information can be received from any one, or each, of three potential source protocols (RIP, OSPF, and EGP); actual information received depends on the specific protocols used within the network environment. Regardless of source, however, all routing information is maintained in a common routing pool.

The routing pool can contain multiple routes to a specific destination. Each route carries an associated preference value which determines the "best' route where more than one route to the same destination is available. On the basis of this preference, IP constructs a forwarding table which lists the "best" route to all know destinations.

The routing pool is updated in response to received protocol traffic; routing pool updates are subsequently reflected in updated forwarding tables. The pool also provides the database used by the routing protocols to prepare their link state/routing advertisements.

The multiprotocol router offers the ability to mediate the flow of routing data to and from the routing pool. This control is provided by user-configured import and export rules.

Import rules govern the addition of new routes to the routing pool. Each routing protocol (OSPF, EGP, or RIP) maintains a distinct set of import rules. For example, upon reception of a new routing update, RIP consults its specific import rules to validate the information before inserting the update in the routing pool. Import rules contain search information (to match fields in incoming routing updates) and action information (to specify the action to take with matched fields).

Export rules govern the propagation of routing information by the routing protocols. Each routing protocol maintains a distinct set of export rules. For example, when preparing a routing advertisement, RIP consults its specific export rules to determine whether routes to specific networks are to be advertised and how they are to be propagated. Export rules contain network numbers (to associate a rule with a specific network) and action information (to specify a route propagation procedure).

The relationship between the routing pool, import rules, export rules, and forwarding tables is depicted in Figure 9-63.

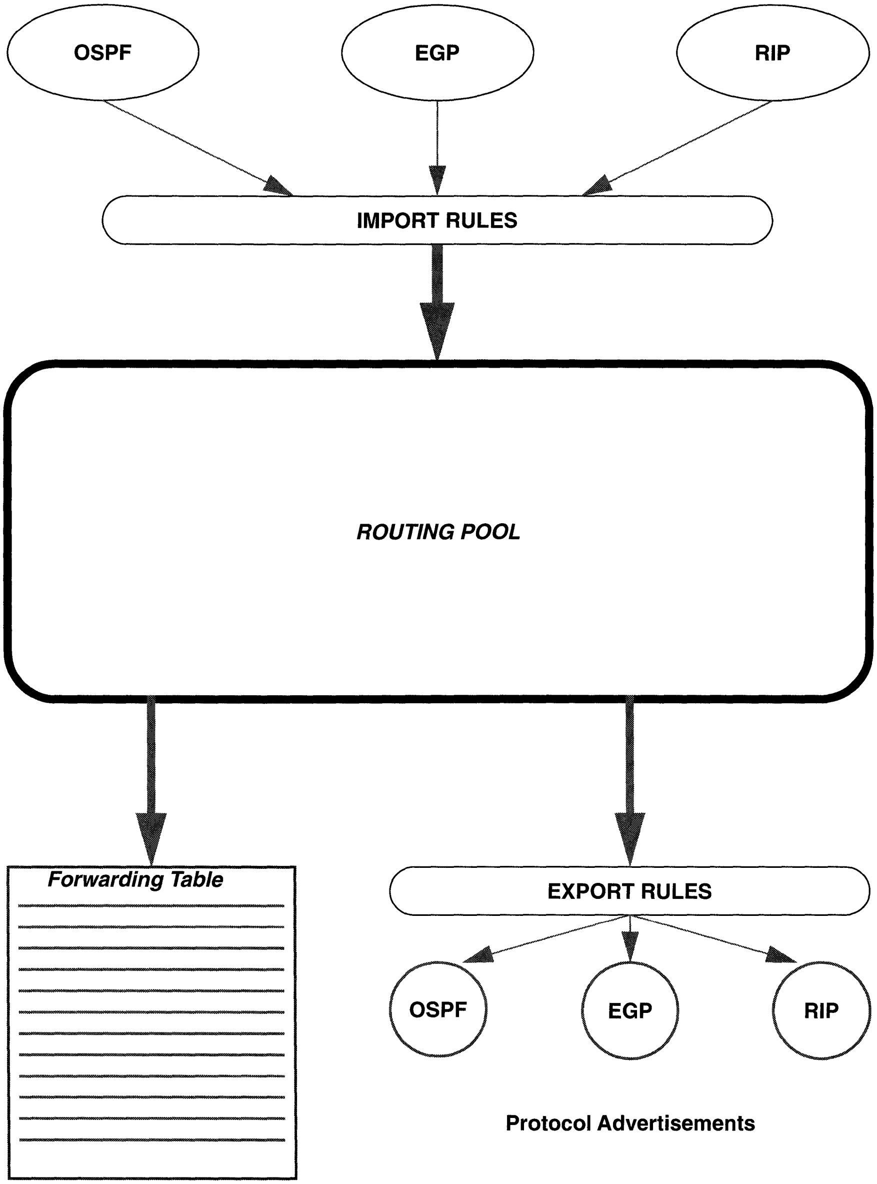


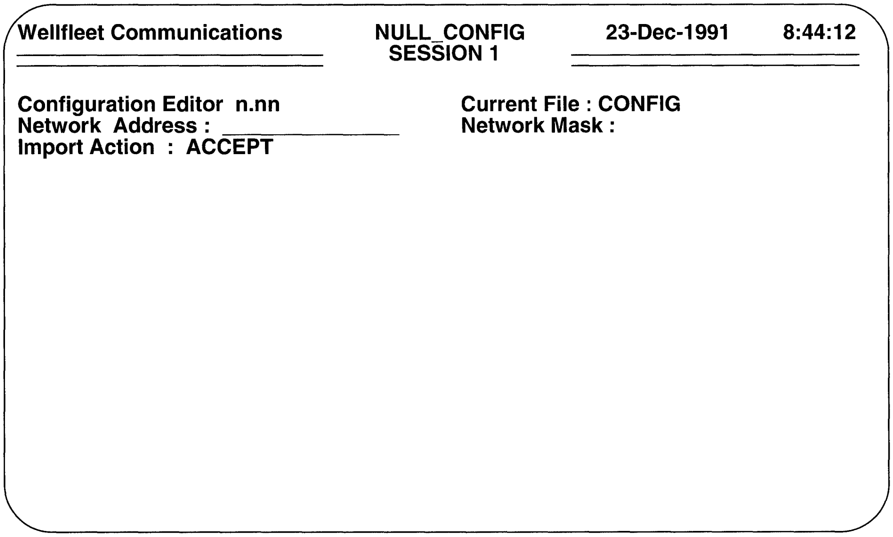
Figure 9-63 Routing Information Data Flow

9.12.1 Configuring Import Route Filters

You construct import route filters from the TCP/IP Detailed Parameters Access Screen. Enter <9> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Import Route Filters record(s) found
Do you wish to add Import Route Filters record(s)?

Press [RETURN] to display the Import Route Filtering Parameters Screen.



```
Wellfleet Communications          NULL_CONFIG          23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                       Current File : CONFIG
Network  Address : ____________                  Network Mask :
Import Action  :  ACCEPT
```

Figure 9-64 Import Route Filtering Parameters Screen

- ❐ **Network Address** is the filtered IP network address.

  If you want to filter all destination networks, press [RETURN]. If you want to filter a specific IP network, enter the network address in dotted decimal notation, then press [RETURN].

- ❐ **Network Mask** specifies a range of addresses upon which the filter acts.

  For example, consider Class B Network 172.32.0.0, which allocates the upper 8 bits of the host identification field to Subnet_ID, and the final 8 bits to Host_ID.

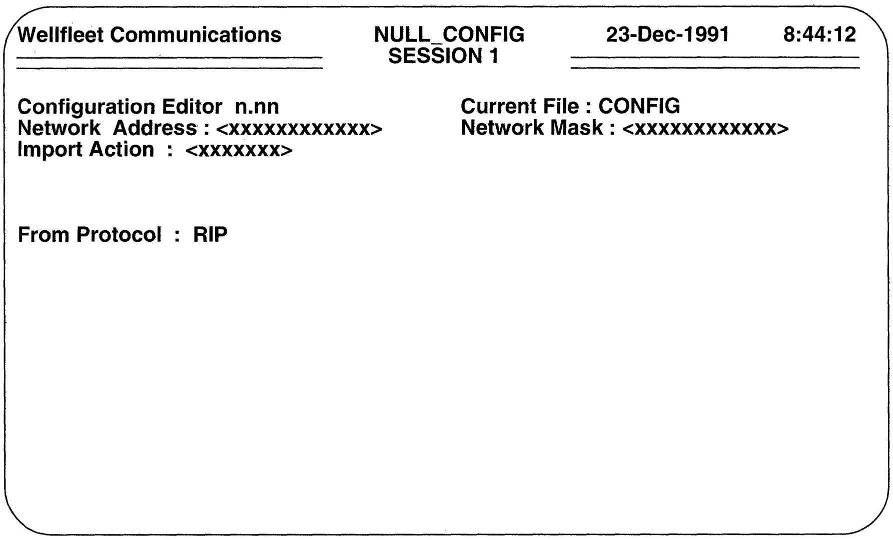
  The address mask directs the filtering process to a specific portion of the IP address. In other words, any IP address that matches the masked portion of 172.32.0.0 is subject to filtering. If 255.255.0.0 is entered at **Address Mask**, only the Net_ID portion of the address will be filtered. If the mask 255.255.255.0 is entered at **Address Mask**, the Net_ID and Subnet_ID portions of the address will be filtered. Finally, if 255.255.255.255 is entered at **Address Mask**, the entire IP address will be filtered.

Construct the address mask, then enter the mask in dotted decimal notation.

- **Import Action** specifies whether the route is transferred to the routing pool.

  ACCEPT sends information to the routing pool; **IGNORE** drops the routing information.

After you specify the **Import Action**, the screen prompts for protocol-specific information.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
____________________________     SESSION 1       ______________________________

Configuration Editor  n.nn                     Current File : CONFIG
Network  Address : <xxxxxxxxxxxx>              Network Mask : <xxxxxxxxxxxx>
Import Action  :  <xxxxxxx>


From Protocol  :  RIP
```

Figure 9-65 Import Route Filtering Protocol Screen

- **From Protocol** identifies the source of the routing information.

  Select **RIP**, **OSPF** or **EGP** and then press `[RETURN]`.

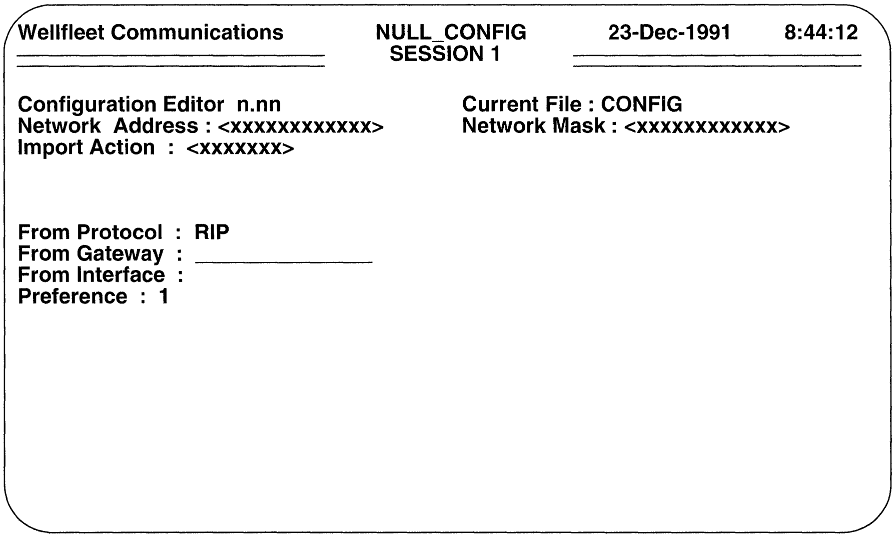
After you specify the source protocol, the screen prompts for additional protocol-specific information. Depending on the protocol selected, the screen displays either Figure 9-66, 9-68, or 9-69.

NOTE

If **Import Action** is equal to **IGNORE**, the **Preference** field is not displayed in Figures 9-66, 9-68, or 9-69.

9.12.1.1 RIP Import Route Filters

To configure a RIP-specific import route filter proceed as follows:



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                    Current File : CONFIG
Network  Address : <xxxxxxxxxxxxx>            Network Mask : <xxxxxxxxxxxxx>
Import Action  :  <xxxxxxxx>


From Protocol  :  RIP
From Gateway  :  ______________
From Interface  :
Preference  :  1
```

Figure 9-66 RIP Import Route Filtering Parameters Screen

❒ **From Gateway** enables the identification of a specific gateway from which RIP updates are received.

If you wish the RIP import route filter to be "universal" (that is applicable to all RIP sources), press `[RETURN]`. If you want the filter to apply to a specific source of RIP updates, enter the source router's IP address in dotted decimal notation.

❒ **From Interface** enables the identification of a specific interface across which RIP updates are received.

If you wish the RIP import route filter to be "universal" (that is applicable to all local interfaces), press `[RETURN]`. If you want the filter to apply to a specific local interface, enter the interface's IP address in dotted decimal notation.

- **Preference** (only displayed when **Import Action** is equal to **ACCEPT**) assigns a weighted precedence value to a route included in the routing pool.

  If confronted with multiple routes to the same destination, the router, by default, grants preference to a static or default route. In the absence of a manually configured route, the router chooses an OSPF-derived route. Lacking an OSPF route, it chooses an EGP route. In the absence of either an OSPF or EGP route, it chooses a RIP-derived route. Figure 9-67 illustrates the routing pool hierarchy.

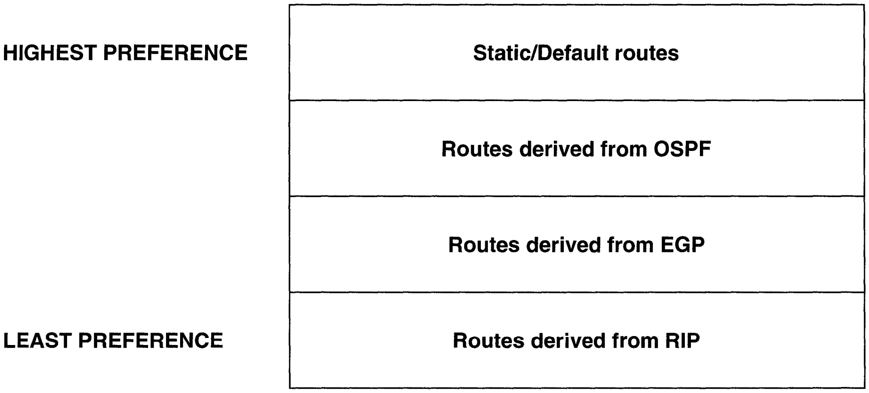


Figure 9-67 Routing Hierarchy

To accept the default routing hierarchy, press `[RETURN]`.

To grant preference to the RIP--derived route, enter a decimal value in the range 1 to 16 (the greater the number, the higher the preference), and then press `[RETURN]`.

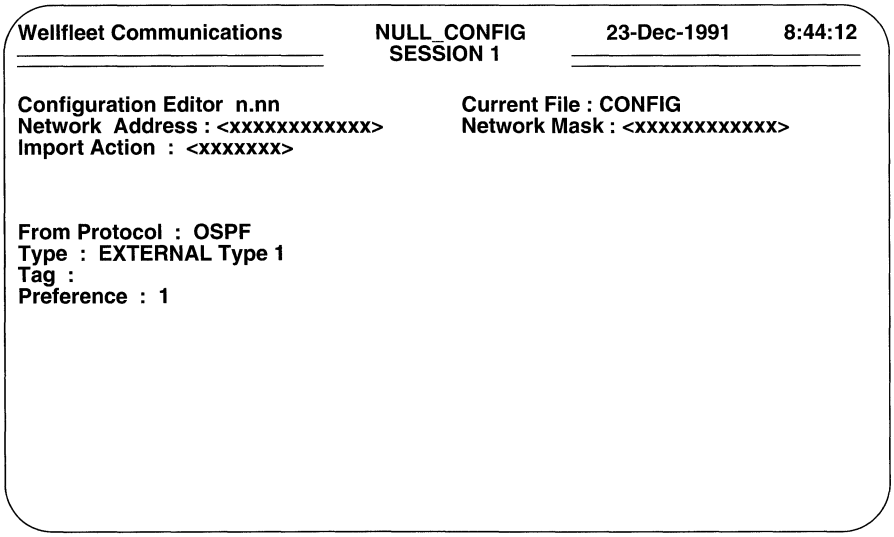
After you specify **Preference**, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the TCP/IP Detailed Parameters Access Screen.

9.12.1.2 OSPF Import Route Filters

To configure an OSPF-specific import route filter proceed as follows:

NOTE

OSPF import route filters mediate the flow of OSPF external routes into the routing pool. An external route describes a route to a destination that is external to the autonomous system. OSPF import route filters have no affect on internal routes; such routes are always place in the routing pool.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Network  Address : <xxxxxxxxxxxx>            Network Mask : <xxxxxxxxxxxx>
Import Action  :  <xxxxxxx>


From Protocol  :  OSPF
Type  :  EXTERNAL Type 1
Tag  :
Preference  :  1
```

Figure 9-68 OSPF Import Route Filtering Parameters Screen

❒ **Type** enables the filtering of two types of OSPF external metrics.

Type 1 metrics are equivalent to the standard OSPF link state metric. Type 2 metrics are greater than the cost of any path internal to the autonomous system. The use of Type 2 metrics assumes that the inter-autonomous system routing is the major cost of packet routing.

If you want the OSPF import route filter to apply to Type 1 metrics, select **EXTERNAL Type 1**. If you want the OSPF import route filter to apply to Type 2 metrics, select **EXTERNAL Type 2**.

- **Tag** enables the further specification of external routes.

  Within OSPF external links advertisements, a 32-bit *External Route Tag* field is attached to each route. The contents of this field are not used by OSPF but can be used by source and destination routers. If you want to filter the contents of the *External Route Tag* field, enter the field contents in eight-digit hexadecimal format and then press `[RETURN]`. If you do not want to filter field contents, press `[RETURN]`.

- **Preference** (only displayed when **Import Action** is equal to **ACCEPT**) assigns a weighted precedence value to a route included in the routing pool.

  By default, preference is granted to manually configured static routes, then to OSPF routes, then to EGP routes, and then to RIP routes.

  To accept the default routing hierarchy (as depicted in Figure 9-67), press `[RETURN]`.

  To grant preference to the OSPF--derived route, enter a decimal value in the range 1 to 16 (the greater the number, the higher the preference), and then press `[RETURN]`.

After you specify **Preference**, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the TCP/IP Detailed Parameters Access Screen.

9.12.1.3 EGP Import Route Filters

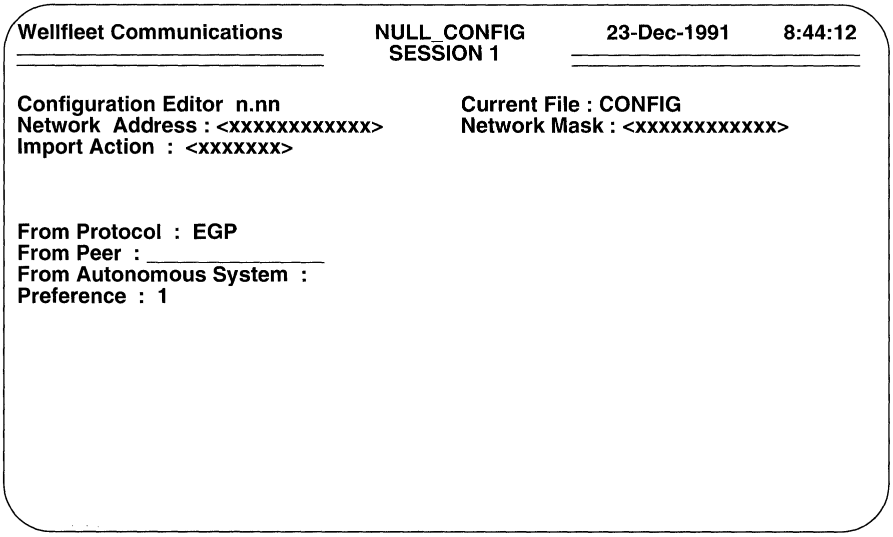
To configure an EGP-specific import route filter proceed as follows:

- **From Peer** enables the identification of a specific router from which EGP updates are received.

  If you wish the EGP import route filter to be “universal” (that is applicable to all foreign EGP routers), press `[RETURN]`. If you want the filter to apply to a specific source of EGP updates, enter the source router’s IP address in dotted decimal notation.

- **From Autonomous System** enables the identification of a specific autonomous system from which RIP update are received.

  If you wish the EGP import route filter to be “universal” (that is applicable to all foreign autonomous systems), press `[RETURN]`. If you want the filter to apply to a specific autonomous system, enter the system’s NIC-assigned identification number.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG
Network  Address : <xxxxxxxxxxxx>               Network Mask : <xxxxxxxxxxxx>
Import Action  :  <xxxxxxx>


From Protocol  :  EGP
From Peer  : _______________
From Autonomous System  :
Preference  :  1
```

Figure 9-69 EGP Import Route Filtering Parameters Screen

❒ **Preference** (only displayed when **Import Action** is equal to **ACCEPT**) assigns a weighted precedence value to a route included in the routing pool.

By default, preference is granted to manually configured static routes, then to OSPF routes, then to EGP routes, and then to RIP routes.

To accept the default routing hierarchy (as depicted in Figure 9-67), press `[RETURN]`.

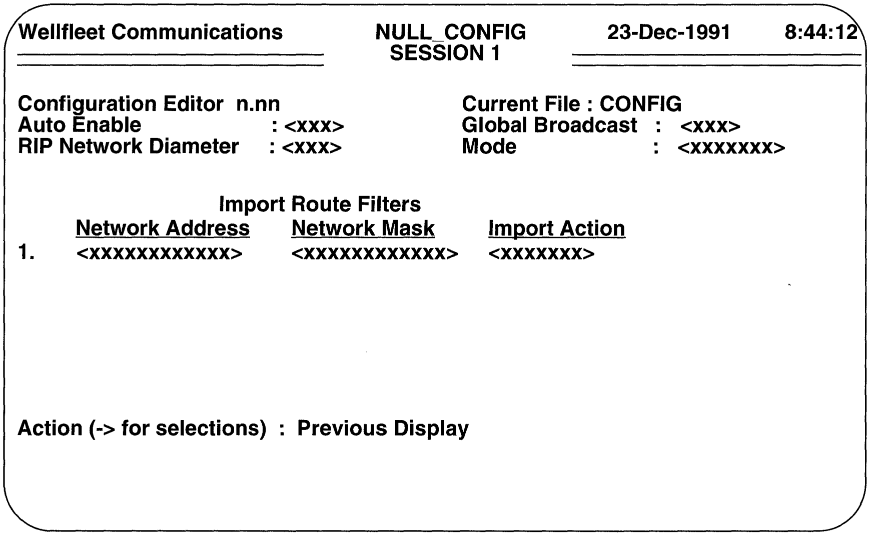
To grant preference to the EGP--derived route, enter a decimal value in the range 1 to 16 (the greater the number, the higher the preference), and then press `[RETURN]`.

After you specify **Preference**, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the TCP/IP Detailed Parameters Access Screen.

9.12.1.4 Configuring Additional Import Route Filters

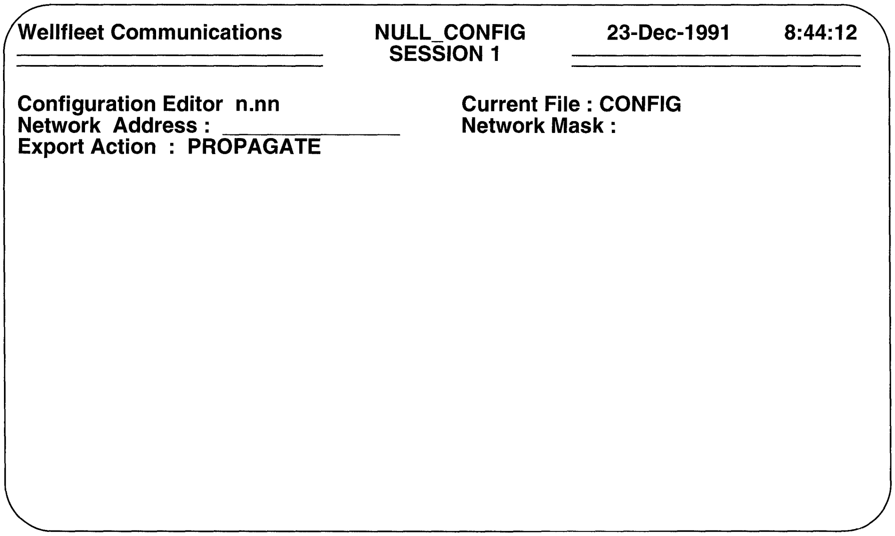
You configure additional import route filters from the TCP/IP Detailed Parameters Access Screen. Enter `<9>` at **Enter Selection (0 for Previous Menu)**. The screen displays the TCP/IP Import Route Filters Summary Screen (Figure 9-70).

At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]` to display the Import Route Filtering Parameters Screen. Now



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                       Current File : CONFIG
Auto Enable               : <xxx>                Global Broadcast  :  <xxx>
RIP Network Diameter      : <xxx>                Mode              :  <xxxxxxx>


                           Import Route Filters
    Network Address       Network Mask        Import Action
1.  <xxxxxxxxxxxx>        <xxxxxxxxxxxx>      <xxxxxxx>





Action (-> for selections)  :  Previous Display
```

Figure 9-70 TCP/IP Import Route Filters Summary Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                       Current File : CONFIG
Network  Address : _______________               Network Mask :
Export Action  :  PROPAGATE
```

Figure 9-71 Export Route Filtering Parameters Screen

follow the same procedures as before to construct an additional import route filter; repeat these procedures until you have configured all such filters.

9.12.2 Configuring Export Route Filters

You construct export route filters from the TCP/IP Detailed Parameters Access Screen. Enter `<10>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following prompt:

> **No Export Route Filters record(s) found**
> **Do you wish to add Export Route Filters record(s)?**

Press `[RETURN]` to display the Export Route Filtering Parameters Screen (Figure 9-71).

❒ **Network Address** is the filtered IP network address.

If you want to filter all destination networks, press `[RETURN]`. If you want to filter a specific IP network, enter the network address in dotted decimal notation, then press `[RETURN]`.

❒ **Network Mask** specifies a range of addresses upon which the filter acts.

For example, consider Class B Network 172.32.0.0, which allocates the upper 8 bits of the host identification field to `Subnet_ID`, and the final 8 bits to `Host_ID`.

The address mask directs the filtering process to a specific portion of the IP address. In other words, any IP address that matches the masked portion of 172.32.0.0 is subject to filtering. If 255.255.0.0 is entered at **Address Mask**, only the Net_ID portion of the address will be filtered. If the mask 255.255.255.0 is entered at **Address Mask**, the Net_ID and Subnet_ID portions of the address will be filtered. Finally, if 255.255.255.255 is entered at **Address Mask**, the entire IP address will be filtered.

Construct the address mask, then enter the mask in dotted decimal notation.

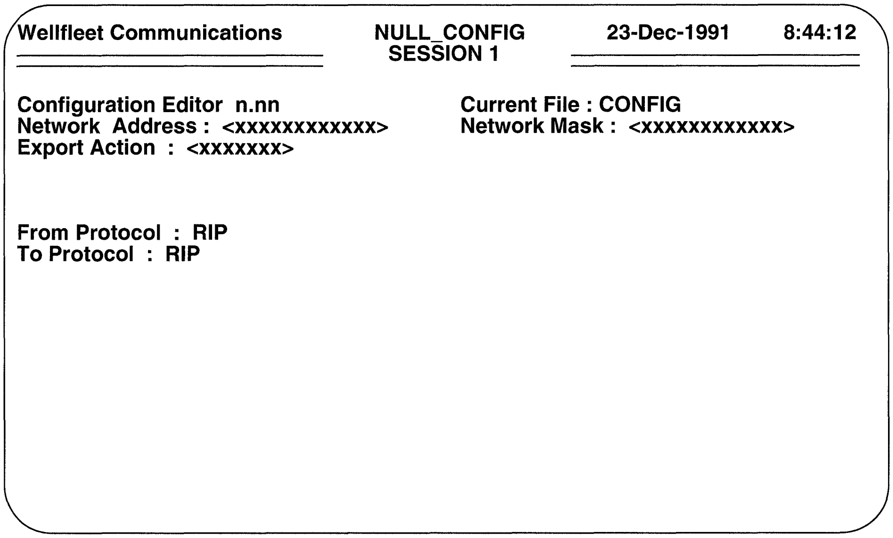
❒ **Export Action** controls the flow of routing information from protocol to protocol.

PROPAGATE advertises the route**;** **IGNORE** suppresses route advertising.

After you specify the **Export Action**, the screen prompts for protocol-specific information (Figure 9-72).

❒ **From Protocol** identifies the source of the routing information.

Select **RIP**, **OSPF,** or **EGP**.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG
Network  Address : <xxxxxxxxxxxx>               Network Mask : <xxxxxxxxxxxx>
Export Action  :  <xxxxxxx>


From Protocol  :  RIP
To Protocol  :  RIP
```

Figure 9-72 Export Route Filtering Protocol Screen

- ❐ **To Protocol** identifies the recipient of the routing information.

  Select **RIP**, **OSPF**, or **EGP**.

After you specify the destination protocol, the screen prompts for additional protocol-specific information. Depending on the destination protocol selected, the screen displays either Figure 9-73, 9-74, or 9-75.

NOTE

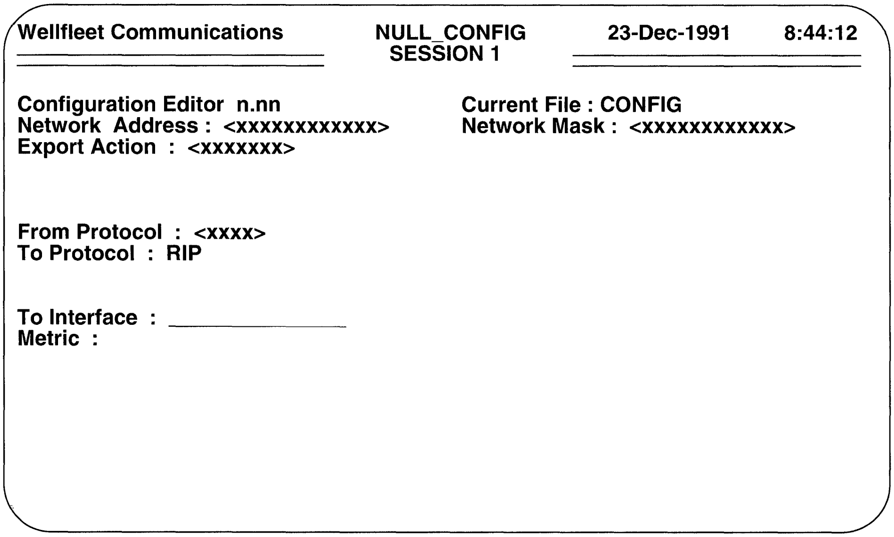
If you specify an **Export Action** of **IGNORE** and a destination protocol of **OSPF**, the screen prompts **Enter Selection (0 for Previous Menu)**. Press <0> to revert to the TCP/IP Detailed Parameters Access Screen.

9.12.2.1 RIP Export Route Filters

To configure a RIP-specific export route filter proceed as follows:

- ❐ **To Interface** enables the association of a specific interface with the filter.

  If you wish the RIP export route filter to be “universal” (that is applicable to all RIP interfaces), press `[RETURN]`. If you want the filter to apply to a specific interface, enter the interface’s IP address in dotted decimal notation.



```
Wellfleet Communications          NULL_CONFIG         23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                        Current File : CONFIG
Network  Address : <xxxxxxxxxxxxx>                Network Mask : <xxxxxxxxxxxxx>
Export Action  :  <xxxxxxxx>


From Protocol  :  <xxxx>
To Protocol  :  RIP

To Interface  :  _____________
Metric  :
```

Figure 9-73 RIP Export Route Filtering Parameters Screen

If **Export Action** is equal to **IGNORE**, the screen prompts **Enter Selection (0 for Previous Menu)**. Enter `<0>` to revert to the TCP/IP Detailed Parameters Access Screen.

- ❐ **Metric** (only displayed when **Export Action** is equal to **PROPAGATE**) assigns a RIP cost to the propagated route.

  Assign a RIP cost (keeping in mind the diameter of the RIP network) and then press `[RETURN]`.

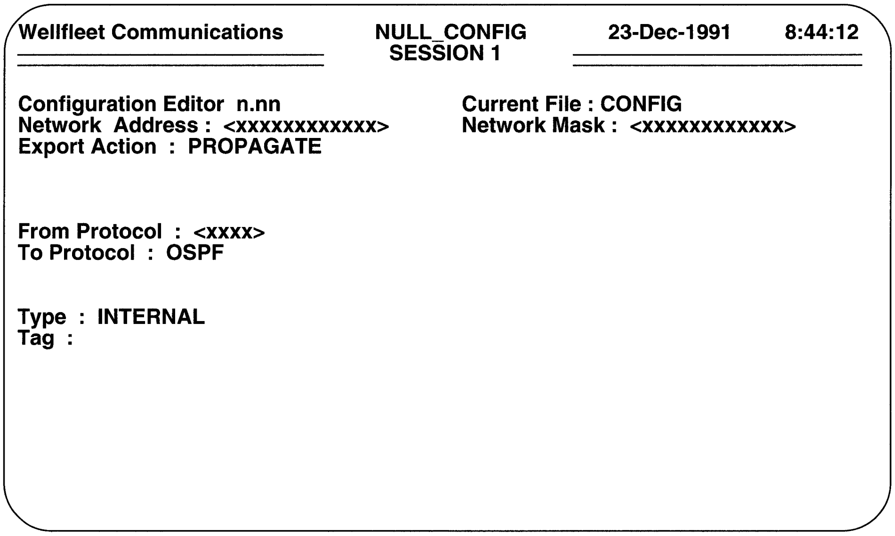
After you specify **Metric**, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the TCP/IP Detailed Parameters Access Screen.

9.12.2.2 OSPF Export Route Filters

To configure an OSPF-specific export route filter proceed as follows:

- ❐ **Type** enables the filtering of two types of OSPF external metrics.

  Type 1 metrics are equivalent to the standard OSPF link state metric. Type 2 metrics are greater than the cost of any path internal to the autonomous system. The use of Type 2 metrics assumes that the inter-autonomous system routing is the major cost of packet routing.



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991     8:44:12
                                   SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Network  Address : <xxxxxxxxxxxx>            Network Mask : <xxxxxxxxxxxx>
Export Action  :  PROPAGATE


From Protocol  :  <xxxx>
To Protocol  :  OSPF


Type  :  INTERNAL
Tag  :
```

Figure 9-74 OSPF Export Route Filtering Parameters Screen

If you want the OSPF import route filter to apply to Type 1 metrics, select **EXTERNAL Type 1**. If you want the OSPF import route filter to apply to Type 2 metrics, select **EXTERNAL Type 2**.

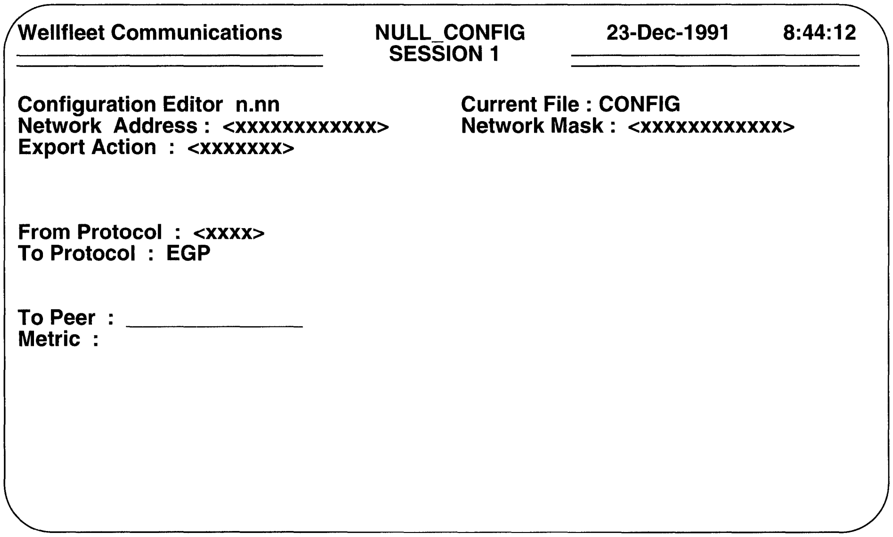
❒ **Tag** enables the further specification of external routes.

Within OSPF external links advertisements, a 32-bit *External Route Tag* field is attached to each route. The contents of this field are not used by OSPF but can be used by source and destination routers. If you want to filter the contents of the *External Route Tag* field, enter the field contents in 8-digit hexadecimal format and then press `[RETURN]`. If you do not want to filter field contents, simply press `[RETURN]`.

After you specify **Tag**, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to revert to the TCP/IP Detailed Parameters Access Screen.

9.12.2.3 EGP Export Route Filters

To configure an EGP-specific export route filter proceed as follows:



```
Wellfleet Communications          NULL_CONFIG       23-Dec-1991    8:44:12
                                   SESSION 1

Configuration Editor  n.nn                 Current File : CONFIG
Network  Address : <xxxxxxxxxxxx>          Network Mask : <xxxxxxxxxxxx>
Export Action  :  <xxxxxxx>


From Protocol  :  <xxxx>
To Protocol  :  EGP


To Peer  :  _____________
Metric  :
```

Figure 9-75 EGP Export Route Filtering Parameters Screen

- **To Peer** enables the identification of a specific EGP router to which the EGP Export route filter applies.

  If you wish the EGP export route filter to be "universal" (that is applicable to all foreign EGP routers), simply press `[RETURN]`. If you want the filter to apply to a specific EGP router, enter the router's IP address in dotted decimal notation and then press `[RETURN]`.

If **Export Action** is equal to **IGNORE**, the screen prompts **Enter Selection (0 for Previous Menu)**. Enter `<0>` to go back to the TCP/IP Detailed Parameters Access Screen (Figure 10-5).

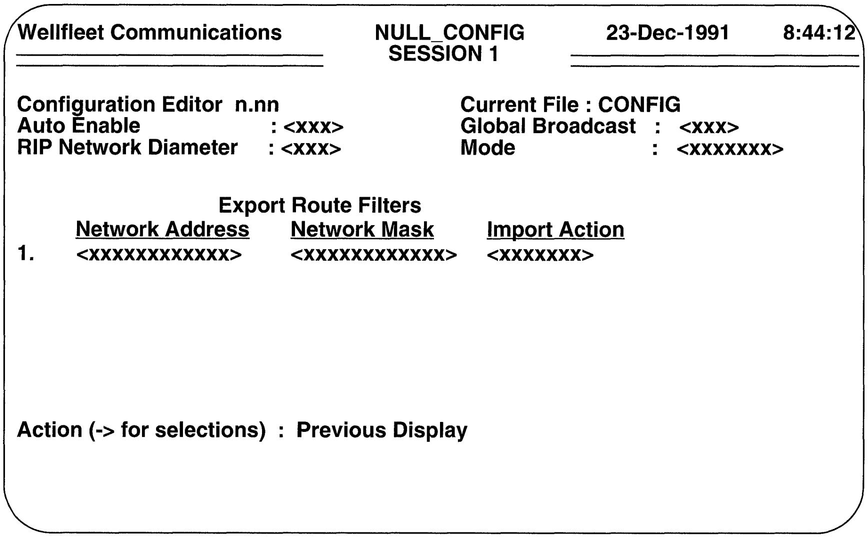
- **Metric** (only displayed when **Export Action** is equal to **PROPAGATE**) assigns an EGP cost metric to the propagated route.

  Assign an EGP cost and then press `[RETURN]`.

After you specify **Metric**, the screen prompts **Hit Return to Continue**. Press `[RETURN]` to go back to the TCP/IP Detailed Parameters Access Screen.

9.12.2.4 Configuring Additional Export Route Filters

You configure additional import route filters from the TCP/IP Detailed Parameters Access Screen. To begin, enter `<10>` at **Enter Selection (0 for Previous Menu)**. The screen displays the TCP/IP Export Route Filters Summary Screen.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG
Auto Enable              : <xxx>             Global Broadcast  :  <xxx>
RIP Network Diameter     : <xxx>             Mode              :  <xxxxxxx>

                       Export Route Filters
     Network Address      Network Mask        Import Action
1.   <xxxxxxxxxxxx>       <xxxxxxxxxxxxx>     <xxxxxxx>

Action (-> for selections)  :  Previous Display
```

Figure 9-76 IP Export Route Filters Summary Screen

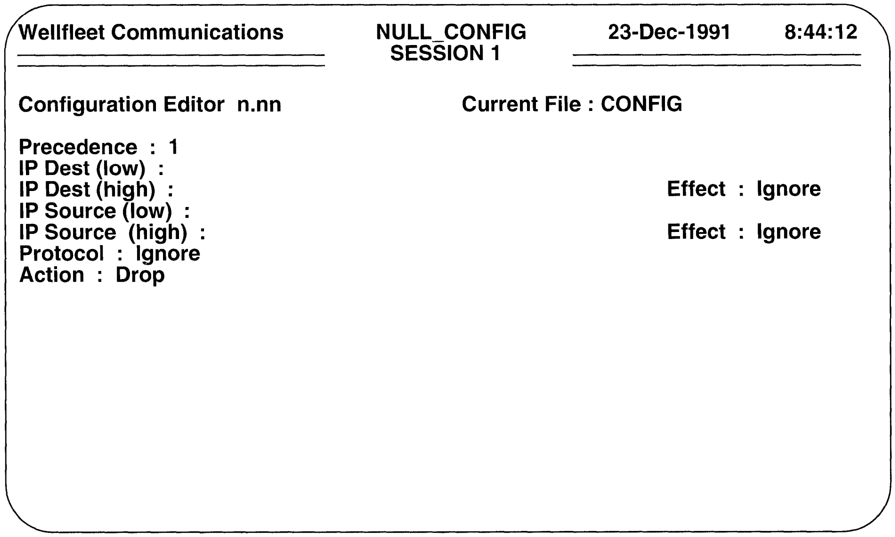
At **Action (-> for selections)**, press the `[RIGHTARROW]` to display **Add**, then press `[RETURN]`. The screen displays the Export Route Filtering Parameters Screen. Now follow the same procedures as before to construct an additional export route filter; repeat these procedures until you have configured all such filters.

9.13 Configuring IP Filters

IP traffic filters apply to all in-coming IP traffic across the interface. You can, if you wish, construct up to 31 filters for each IP interface. You configure interface-specific IP traffic filters from the IP Filters Configuration Screen (Figure 9-17). Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Traffic Filters record(s) found
Do you wish to add Traffic Filters record(s)?

Press `[RETURN]` to display the IP Filters Rule Screen (Figure 9-77).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG

Precedence  :  1
IP Dest (low)  :
IP Dest (high)  :                                      Effect  :  Ignore
IP Source (low)  :
IP Source  (high)  :                                   Effect  :  Ignore
Protocol  :  Ignore
Action  :  Drop
```

Figure 9-77 IP Filters Rule Screen

❐ **Precedence** assigns a priority value to the filter; the higher the precedence, the greater the priority.

You can construct up to 31 filters per IP interface. The **Precedence** value is used when an in-coming IP packet meets multiple filter rules. In such an instance, the filter with the highest priority is applied to the frame.

In the event of two filters with equal precedence, the first configured filter takes precedence.

Select a value from 1 to 31.

❐ **IP Dest (low)** specifies the lower boundary range of filtered IP destination addresses.

If you do not want to filter IP destination addresses, press `[RETURN]`.

To filter IP destination addresses, do one of the following:

- enter the name of an IP network list
- enter an IP address at the lower boundary of the IP address range that you want to filter
- enter a single network address that you want to filter

❒ **IP Dest (high)** specifies the upper boundary of the filtered range.

If you do not want to filter IP destination addresses, press `[RETURN]`.

To filter IP destination addresses, do one of the following:

- if you entered the name of an IP network list at **IP Dest (low)**, or if you want to filter the single IP address entered at **IP Dest (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **IP Dest (low)**, enter an IP address at the upper boundary of the address range that you want to filter.

❒ **Effect** designates one of three operators applied to the pattern specified by **IP Dest (low)** and **IP Dest (high)**.

If the filter does not care about destination address values, press `[RETURN]` to accept the default, **Ignore**.

To filter destination addresses, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **IP Dest (low)** and **IP Dest (high)** includes the destination address field of the IP datagram.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **IP Dest (low)** and **IP Dest (high)** does not include the destination address field of the IP datagram.

❒ **IP Source (low)** specifies the lower boundary range of filtered IP source addresses.

If you do not want to filter IP source addresses, press `[RETURN]`.

To filter IP source addresses, do one of the following:

- enter the name of an IP network list
- enter an IP address at the lower boundary of the IP address range that you want to filter
- enter a single network address that you want to filter

❒ **IP Source (high)** specifies the upper boundary of the filtered range.

If you do not want to filter IP source addresses, press `[RETURN]`.

To filter IP source addresses, do one of the following:

- if you entered the name of an IP network list at **IP Source (low)**, or if you want to filter the single IP address entered at **IP Source (low)**, press `[RETURN]`.

- if you entered a lower boundary range value at **IP Source (low)**, enter an IP address at the upper boundary of the address range that you want to filter.

❒ **Effect** designates one of three operators applied to the pattern specified by **IP Source (low)** and **IP Source (high)**.

If the filter does not care about source address values, press `[RETURN]` to accept the default, **Ignore**.

To filter source addresses, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **IP Source (low)** and **IP Source (high)** includes the source address field of the IP datagram.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **IP Source (low)** and **IP Source (high)** does not include the source address field of the IP datagram.

❒ **Protocol** enables the filtering of traffic to and from UDP and/or TCP ports.

If you do not want to filter TCP or UDP port traffic, press `[RETURN]`.

To filter UDP traffic, select **UDP**; to filter TCP traffic, select **TCP**; to filter both UDP and TCP traffic, select **UDP or TCP**.

If you filter port traffic, the screen prompts for port specific information (Figure 9-78).

❒ **UDP/TCP Dest Port (low)** specifies the lower boundary range of filtered UDP and/or TCP destination ports.

If you do not want to filter destination ports, press `[RETURN]`.

To filter UDP and/or TCP destination ports, do one of the following:

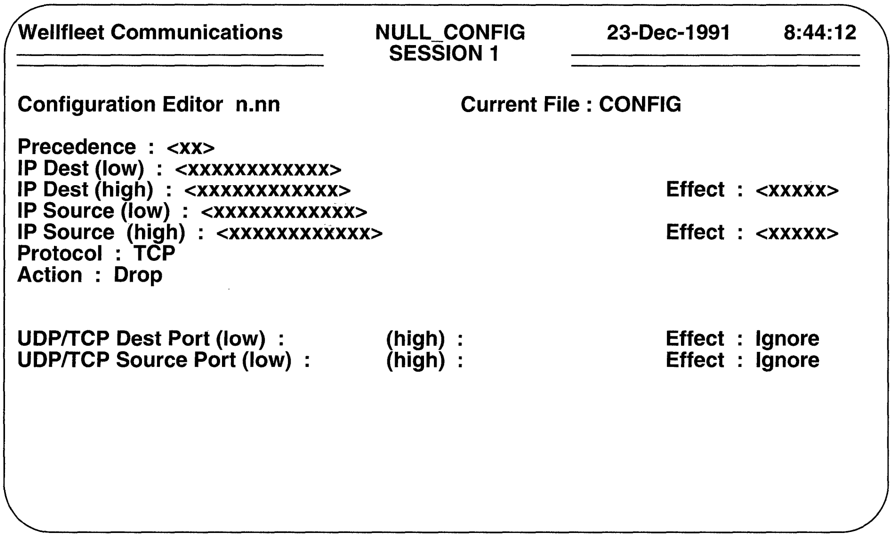
- enter the name of an IP port list
- enter a port number at the lower boundary of the port range that you want to filter
- enter a single port number that you want to filter

❒ **(high)** specifies the upper boundary of the filtered range.

If you do not want to filter IP destination ports, press `[RETURN]`.

To filter UDP and/or TCP destination ports, do one of the following:

- if you entered the name of a port list at **UDP/TCP Dest Port (low)**, or if you want to filter the single port number entered at **UDP/TCP Dest Port (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **UDP/TCP Dest Port (low)**, enter a port number at the upper boundary of the port range that you want to filter.



```
Wellfleet Communications         NULL_CONFIG         23-Dec-1991      8:44:12
                                  SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Precedence  :  <xx>
IP Dest (low)  :  <xxxxxxxxxxxxx>
IP Dest (high)  :  <xxxxxxxxxxxxx>                       Effect  :  <xxxxxx>
IP Source (low)  :  <xxxxxxxxxxxxx>
IP Source  (high)  :  <xxxxxxxxxxxxx>                    Effect  :  <xxxxxx>
Protocol  :  TCP
Action  :  Drop

UDP/TCP Dest Port (low)  :          (high)  :            Effect  :  Ignore
UDP/TCP Source Port (low)  :        (high)  :            Effect  :  Ignore
```

Figure 9-78 Port Filters Configuration Screen

❐ **Effect** designates one of three operators applied to the pattern specified by **UDP/TCP Dest Port (low)** and **(high)**.

If the filter does not care about destination port values, press `[RETURN]` to accept the default, **Ignore**.

To filter destination ports, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **UDP/TCP Dest Port (low)** and **(high)** includes the destination port of the UDP datagram and/or TCP segment.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **UDP/TCP Dest Port (low)** and **(high)** does not include the destination port of the UDP datagram and/or TCP segment.

❐ **UDP/TCP Source Port (low)** specifies the lower boundary range of filtered UDP and/or TCP source ports.

If you do not want to filter source ports, press `[RETURN]`.

To filter UDP and/or TCP source ports, do one of the following:

- enter the name of an IP port list
- enter a port number at the lower boundary of the port range that you want to filter
- enter a single port number that you want to filter

❐ **(high)** specifies the upper boundary of the filtered range.

If you do not want to filter UDP and/or TCP source ports, press `[RETURN]`.

To filter UDP and/or TCP source ports, do one of the following:

- if you entered the name of a port list at **UDP/TCP Source Port (low)**, or if you want to filter the single port number entered at **UDP/ TCP Source Port (low)**, press `[RETURN]`.
- if you entered a lower boundary range value at **UDP/TCP Source Port (low)**, enter a port number at the upper boundary of the port range that you want to filter.

❐ **Effect** designates one of three operators applied to the pattern specified by **UDP/TCP Source Port (low)** and **(high)**.

If the filter does not care about source port values, press `[RETURN]` to accept the default, **Ignore**.

To filter source ports, you choose between the **Match** and **Don't Match** operators.

- **Match** initiates filter action (drop/accept/log) if the pattern specified by **UDP/TCP Source Port (low)** and **(high)** includes the source port of the UDP datagram and/or TCP segment.
- **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **UDP/TCP Source Port (low)** and **(high)** does not include the source port of the UDP datagram and/or TCP segment.

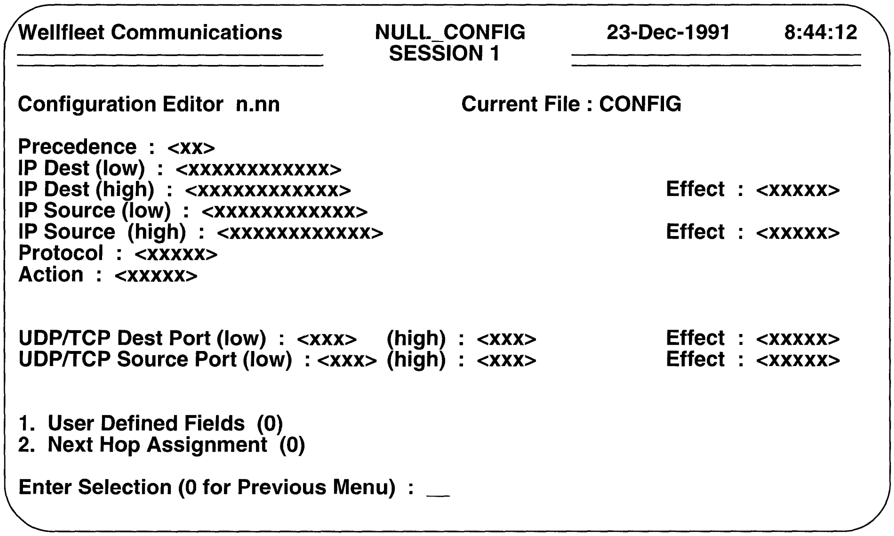
❐ **Action** specifies the disposition of IP datagrams, UDP datagrams, or TCP segments that meet the filter rule.

Drop discards a packet that meets the filter rule; **Drop and Log** discards the packet and records an event message in the event log; **Accept** relays a packet that meets the filter rule; **Accept and Log Drop** relays the packet and records an event message in the event log.

NOTE

The **Drop and Log** and **Accept and Log** actions should be used judiciously. The processing required to log such events in the RAM-based event log consumes CPU cycles and can result in the loss of incoming packets. Consequently, the log actions should generally be used only to record anomalous events.

After you select the required action and press `[RETURN]`, the screen prompts for additional data.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG

Precedence  :  <xx>
IP Dest (low)  :  <xxxxxxxxxxxx>
IP Dest (high)  :  <xxxxxxxxxxxx>                        Effect  :  <xxxxx>
IP Source (low)  :  <xxxxxxxxxxxx>
IP Source  (high)  :  <xxxxxxxxxxxx>                     Effect  :  <xxxxx>
Protocol  :  <xxxxx>
Action  :  <xxxxx>


UDP/TCP Dest Port (low)  :  <xxx>    (high)  :  <xxx>     Effect  :  <xxxxx>
UDP/TCP Source Port (low)  : <xxx>  (high)  :  <xxx>     Effect  :  <xxxxx>


1.  User Defined Fields  (0)
2.  Next Hop Assignment  (0)

Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-79 IP Filters Detailed Parameters Access Screen

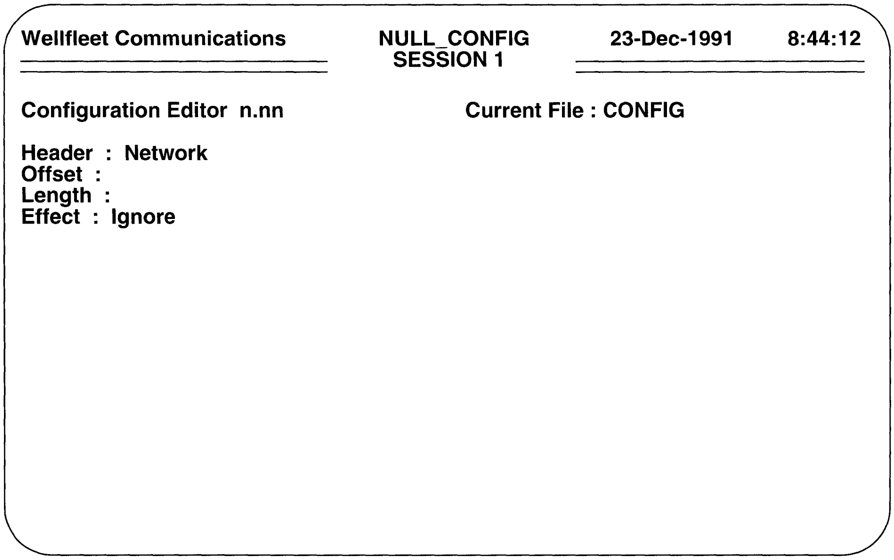
9.13.1 Configuring User-Defined Filters

User-defined filters enable you to filter IP traffic based upon specified bit patterns contained within the IP header or the header of the upper level protocol conveyed within the IP datagram. User-defined filters can be used by themselves or in conjunction with IP address and/or UDP/TCP port filters.

You construct user-defined filters from the IP Filters Basic Parameters Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No User Defined Fields record(s) found
Do you wish to add User Defined Fields record(s)?

Press `[RETURN]` to display the IP User-Defined Fields Parameters Screen.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Header  :  Network
Offset  :
Length  :
Effect  :  Ignore
```

Figure 9-80 IP User-Defined Fields Parameters Screen

- ❐ **Header** selects either the IP header or the upper level protocol header.

  Network selects the IP header; **After Network** selects the upper level protocol header.

- ❐ **Offset** positions the filtered bit pattern within the selected header.

  The first (most significant) bit of either header is referenced as bit 0. Enter the starting location of the filtered bit pattern with reference to the most significant bit of the header.

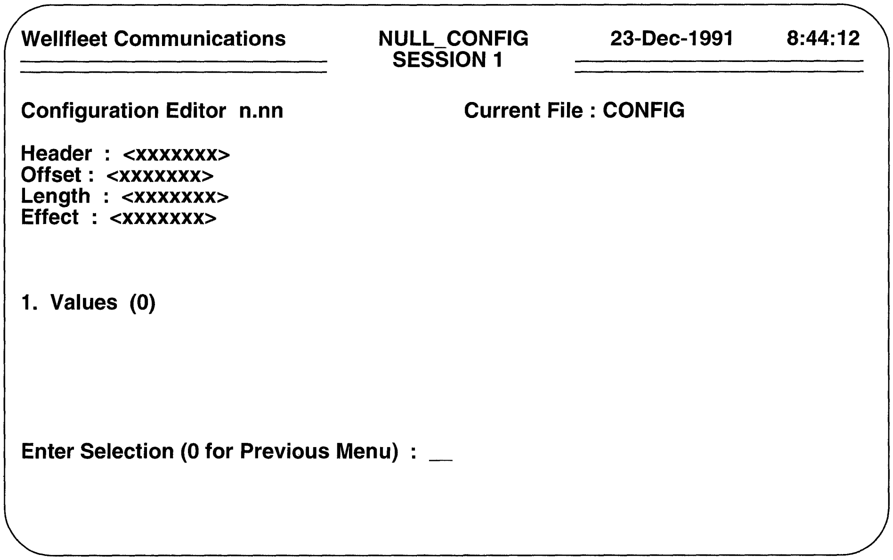
- ❐ **Length** specifies the bit length of the filtered field.

  Enter the field length.

- ❐ **Effect** designates the operator applied to the user-defined pattern.

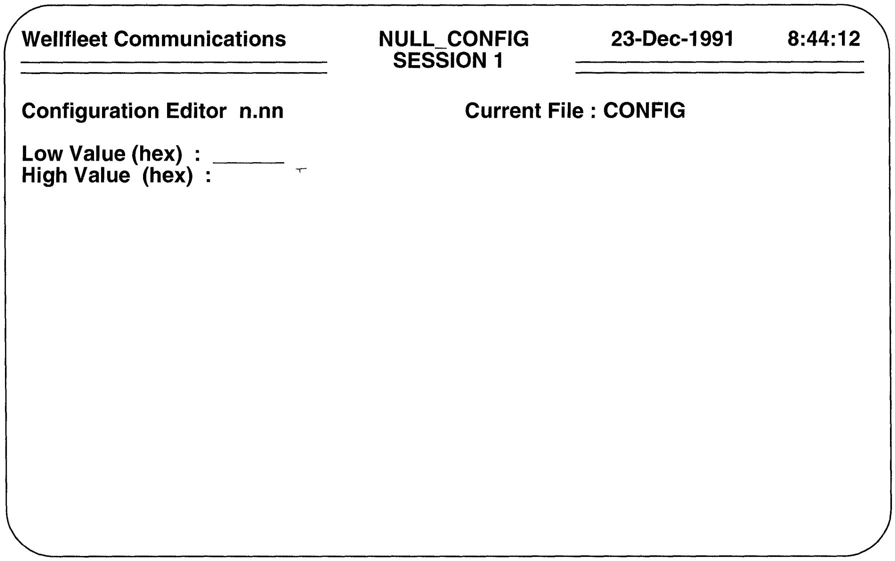
  - **Match** initiates filter action (drop/accept/log) if the pattern specified by **Header**, **Offset,** and **Length** matches a specified value.
  - **Don't Match** initiates filter action (drop/accept/log) if the pattern specified by **Header**, **Offset,** and **Length** does not match the specified value.

The screen then prompts for a value to associate with the bit field described by **Offset** and **Length** (Figure 9-81).



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG

Header  :  <xxxxxxx>
Offset :  <xxxxxxx>
Length  :  <xxxxxxx>
Effect  :  <xxxxxxx>


1.  Values  (0)




Enter Selection (0 for Previous Menu)  :  __
```

Figure 9-81 IP User-Defined Filter Values Access Screen



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG

Low Value (hex)  :  ______
High Value  (hex)  :
```

Figure 9-82 IP User-Defined Filter Values Screen

Enter <1> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

> **No Values record(s) found**
> **Do you wish to add Values record(s)?**

Press [RETURN] to display the IP User-Defined Values Screen (Figure 9-82).

❒ **Low Value (hex)** specifies the lower boundary range of the user-defined pattern.

To filter user-defined values, do one of the following:

- enter a hexadecimal value at the lower boundary of the user-defined range that you want to filter
- enter a single hexadecimal value that you want to filter

❒ **High Value (hex)** specifies the upper boundary range of the user-defined pattern.

To filter user-defined values, do one of the following:

- if you entered a lower boundary range value at **Low Value (hex)**, enter an upper boundary of the user-defined range that you want to filter.
- if you want to filter the single value entered at **Low Value (hex)**, press [RETURN].

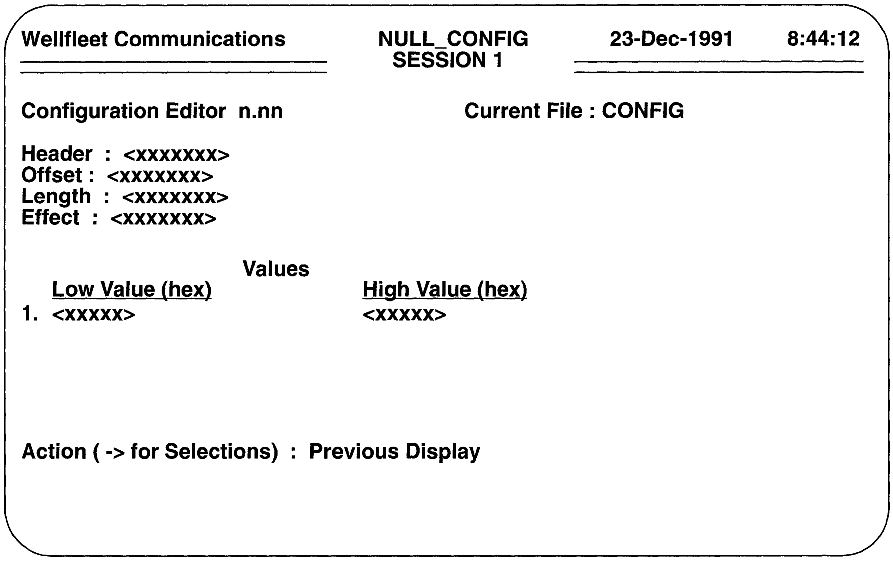
When the screen prompts **Hit Return to Continue**, press [RETURN] to go back to the IP User-Defined Values Access Screen.

If you want, you can add other specified values to the filter. To add an additional value, enter <1> at **Enter Selection (0 for Previous Menu)**. The screen displays the IP Values Summary Screen (Figure 9-83). To add another range of values press the [RIGHTARROW] to display **Add** and then press [RETURN] to display the IP User-Defined Filter Values Screen. Now follow the same procedure as before to add another value; continue in this fashion until you have added all desired values to the filter.

9.13.2 Filtered Traffic Static Routes

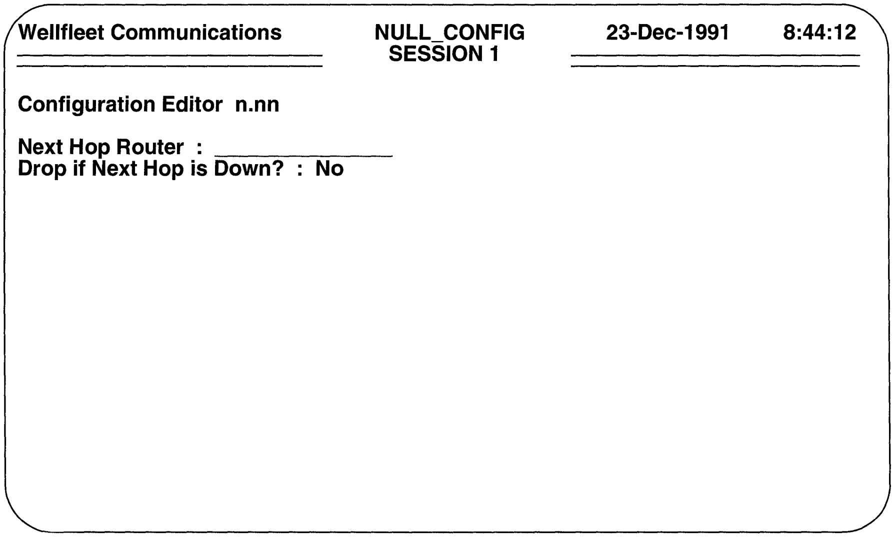
Traffic that is routed as a result of filtering is generally treated as any other traffic; after consulting its routing table, IP either directs the datagram to a next-hop router or to a directly connected IP network. You can arrange, however, to direct filtered traffic to specific next hop routers.

You direct filtered traffic to a specific next hop from the IP Filters Detailed Parameters Access Screen. To begin, enter <2> at **Enter Selection (0 for Previous Menu)**. The screen displays the following:



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991    8:44:12
                                   SESSION 1

Configuration Editor  n.nn                      Current File : CONFIG

Header  :  <xxxxxxx>
Offset :  <xxxxxxx>
Length  :  <xxxxxxx>
Effect  :  <xxxxxxx>

                             Values
   Low Value (hex)                    High Value (hex)
1. <xxxxx>                            <xxxxx>



Action ( -> for Selections)  :  Previous Display
```

Figure 9-83 IP Values Summary Screen



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991    8:44:12
                                   SESSION 1

Configuration Editor  n.nn

Next Hop Router  :  ______________
Drop if Next Hop is Down?  :  No
```

Figure 9-84 IP Filtered Traffic Static Routing Screen

No Next Hop Assignment record(s) found
Do you wish to add Next Hop Assignment record(s)?

Press `[RETURN]` to display the IP Filtered Traffic Static Routing Screen (Figure 9-84).

- ❐ **Next Hop Address** specifies the IP address of the next hop router.

  Enter the address in dotted decimal notation

- ❐ **Drop if Next Hop is Down** specifies the disposition of the filtered datagram if the next hop is unreachable.

  Yes drops the datagram; **No** causes IP to consult its routing table and provide an alternate route for the datagram.

When the screen prompts **Hit Return to Continue**, press `[RETURN]` to revert to the IP Filters Detailed Parameters Access Screen.

9.13.3 Configuring Additional Filters

You configure additional filters (up to a maximum of 31 per IP interface) from the IP Filters Configuration Screen. Enter `<1>` at **Enter Selection (0 for Previous Menu)** to display the IP Filters Summary Screen.

At **Action (-> for selections)**, press the `[RIGHTARROW]` to select **Add**, then press `[RETURN]` to display the IP Filters Rule Screen. Now follow the same procedures as before to define an additional IP filter; repeat these procedures until you have configured all filters.

10 Configuring SNMP

This chapter tells you how to configure the Simple Network Management Protocol (SNMP) management agent software. It assumes familiarity with the following RFCs:

RFC 1155	Describes the structure and identification of management information for IP networks
RFC 1156	Describes the standard Internet Management Information Base (MIB)
RFC 1157	Describes the Simple Network Management Information Protocol

SNMP is a transaction-based protocol that specifies the transfer of structured management information between two types of SNMP entities: *applications* and *agents.*

Application software runs in a network management center; it issues queries to gather data about the status, configuration, and performance of external devices -- or *network elements* in SNMP terminology. Agent software, on the other hand, runs in network elements, for example the multiprotocol router. Agent software responds to monitoring center queries, and, if so configured, generates unsolicited reports of significant activity (referred to as *traps*) back to the monitoring center.

NOTE

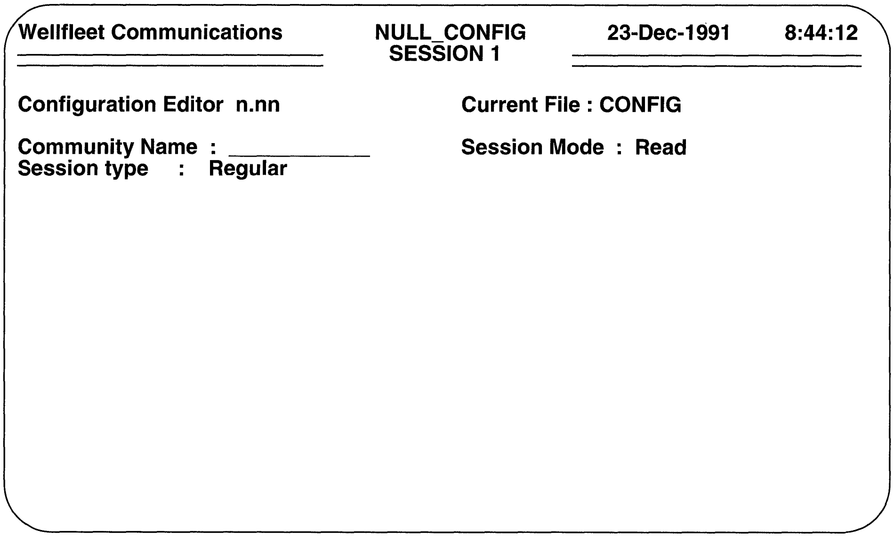
As all SNMP transmissions between application and agent entities are conveyed via the User Datagram Protocol (UDP); you must load the TCP/IP software to Slot 2 (the master slot) of the router to enable SNMP operations.

10.1 Granting Community Access

You install SNMP agent software from the Configuration Menu. At E**nter Selection (0 for Previous Menu)** enter the number that appears to the left of **SNMP Sessions**. The screen displays the following:

No SNMP Sessions record(s) found
Do you wish to add SNMP Sessions record(s)?

Press `[RETURN]` to display the SNMP Parameters Screen (Figure 10-1).



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991      8:44:12
________________________         SESSION 1         ________________________

Configuration Editor  n.nn                    Current File : CONFIG

Community Name  : ___________                 Session Mode  :  Read
Session type    :   Regular
```

Figure 10-1 SNMP Parameters Screen

- ❒ **Community Name** identifies the network monitoring centers authorized to query the router.

  An SNMP community is a group of monitoring centers authorized to issue queries to the SNMP agent. A community has a *name* which identifies a logical set of application entities, and *members*, which are the IP addresses of management stations authorized to query the router's resident agent software.

  At **Community Name** enter the name of an authorized community. As communities are defined within the SNMP application software, ensure that your entry matches an existing community previously defined by the SNMP application software.

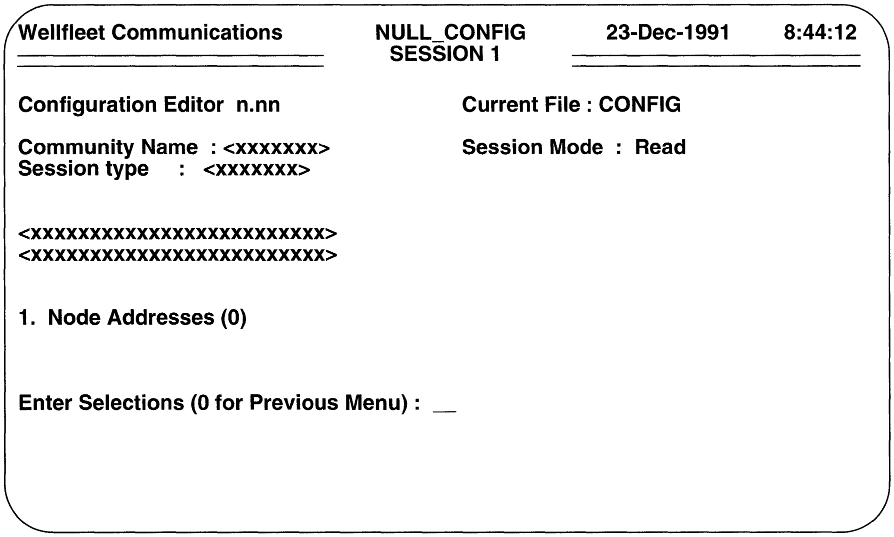
In addition to a name and members, a community also has a *mode* which specifies what type of remote access commands can be carried out by application entities and a *type* which specifies how application entities gather management data.

- ❒ **Session Mode** specifies remote access privilege to the local MIB.

  Session Mode specifies the community's access privilege (read or read/ write) to the local MIB. The SNMP agent implementation supports only read (**Read**) access

- ❒ **Session type** specifies the data-exchange model between the SNMP application and agent entities.

Regular specifies a query/response model in which agent output is triggered by the receipt of application requests. After you specify the Regular session type, the screen displays the Community Member Access Screen (Figure 10-2) to prompt for community members. Now proceed to Section 10.2 to grant member access to the local MIB.



```
Wellfleet Communications        NULL_CONFIG        23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Community Name  : <xxxxxxx>                  Session Mode  :  Read
Session type    :  <xxxxxxx>


<xxxxxxxxxxxxxxxxxxxxxxxxx>
<xxxxxxxxxxxxxxxxxxxxxxxxx>


1.  Node Addresses (0)


Enter Selections (0 for Previous Menu) : __
```

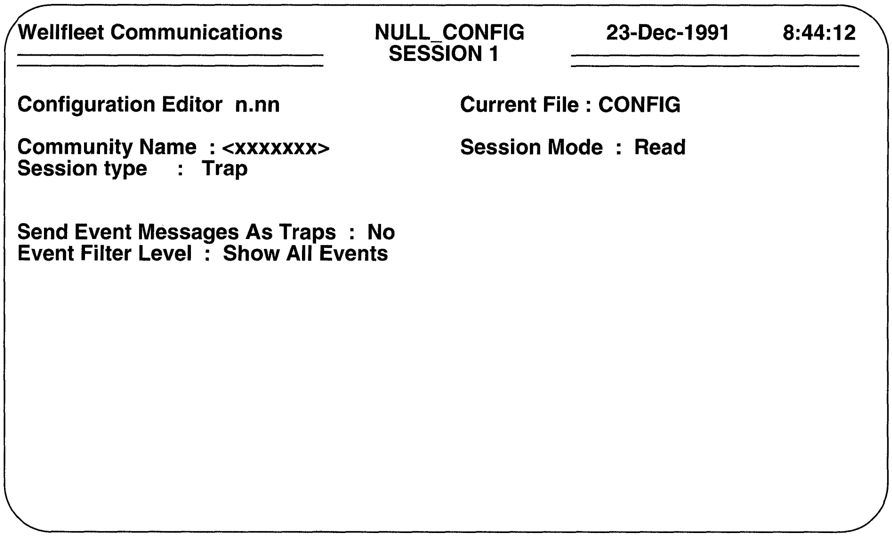
Figure 10-2 SNMP Community Member Access Screen

Trap specifies an enterprise-specific data-exchange model in which the local agent not only responds to application requests but also generates asynchronous, unsolicited notifications of significant local events (as defined by RFC 1157).

If you select **Trap**, the screen displays the SNMP Trap Screen (Figure 10-3) to prompt for additional information.

❐ **Send Event Messages As Traps** enables or disables the generation of enterprise-specific traps.

With enterprise-specific trapping enabled, some or all of the event messages generated by the router are encapsulated within an SNMP protocol data unit and sent as traps to SNMP application entities. Select **Yes**, to enable enterprise-specific trapping or **No** to disable enterprise-specific trapping.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991      8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Community Name  : <xxxxxxx>                  Session Mode  :  Read
Session type    :   Trap

Send Event Messages As Traps  :  No
Event Filter Level  :  Show All Events
```

Figure 10-3 SNMP Trap Screen

❒ **Event Filter Level** specifies which event messages are transmitted as traps to SNMP application entities.

If you have disabled enterprise-specific trapping, simply press `[RETURN]`; if you have enabled enterprise-specific trapping, select the appropriate filter level.

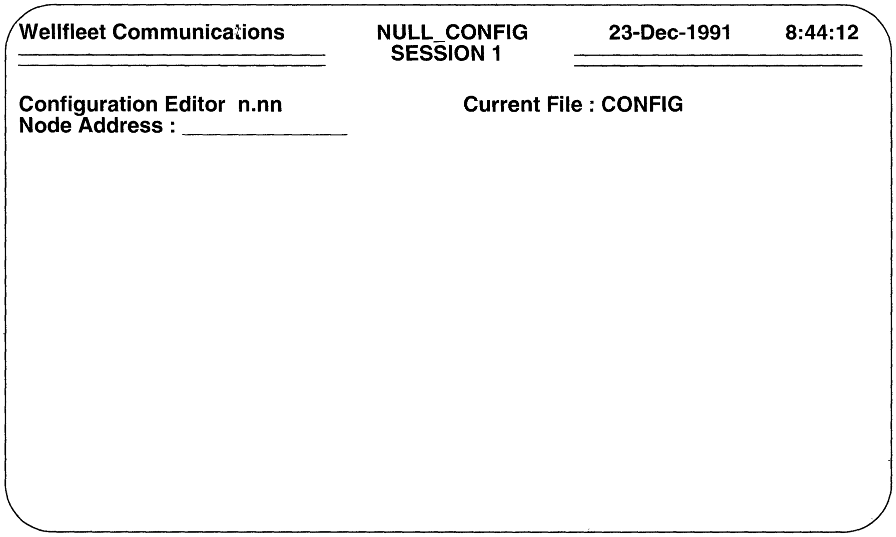
After you specify the filter level, the console screen displays the Community Member Access Screen (Figure 10-2) to prompt for community members.

10.2 Granting Community Member Access

The Community Member Access Screen allows you to identify specific members of Community Name granted access to the local MIB. To begin granting access to individual members of Community Name, enter `<1>` at **Enter Selection (0 for Previous Menu)**. The screen displays the following:

No Node Addresses record(s) found
Do you wish to add Node Addresses record(s)?

Press `[RETURN]` to display the SNMP Community Member Address Screen (Figure 10-4).



```
Wellfleet Communications          NULL_CONFIG        23-Dec-1991      8:44:12
                                   SESSION 1

Configuration Editor  n.nn                  Current File : CONFIG
Node Address : _____________
```

Figure 10-4 SNMP Community Member Address Screen

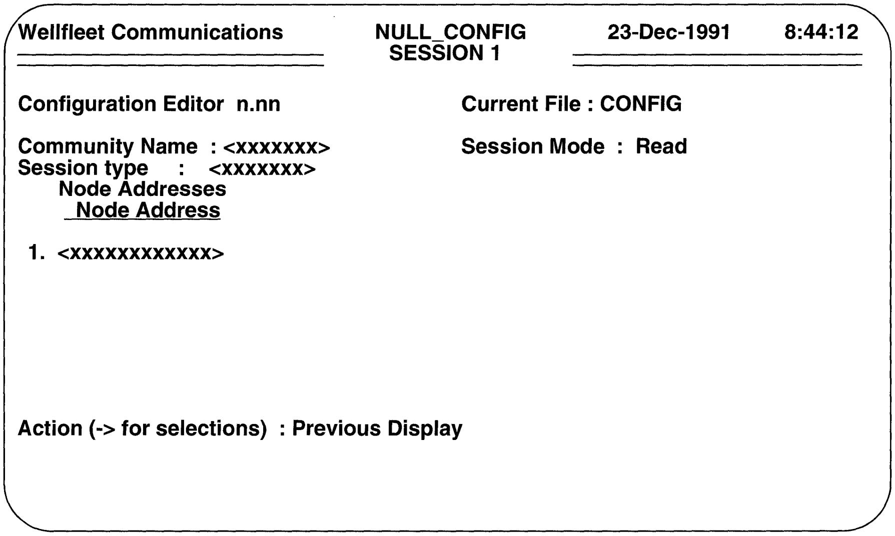
At **Node Address**, enter the dotted decimal IP address of a community member (a specific host device under **Community Name**) granted access to the local MIB.

After the screen prompts **Hit Return to Continue**, do so to revert to the SNMP Community Member Access Screen. To grant the same MIB access to another community member, enter `<1>` at the prompt to display the Community Members Summary Screen (Figure 10-5) which lists the IP addresses of all community members granted MIB access.

At **Action (-> for selections)** press the `[RIGHTARROW]` to display **Add** and then press `[RETURN]`. The screen again displays the SNMP Community Member Address Screen. At **Node Address**, enter the IP address of an additional community member and then press `[RETURN]`. Continue in this manner until you have entered the IP addresses of all community members granted MIB access.

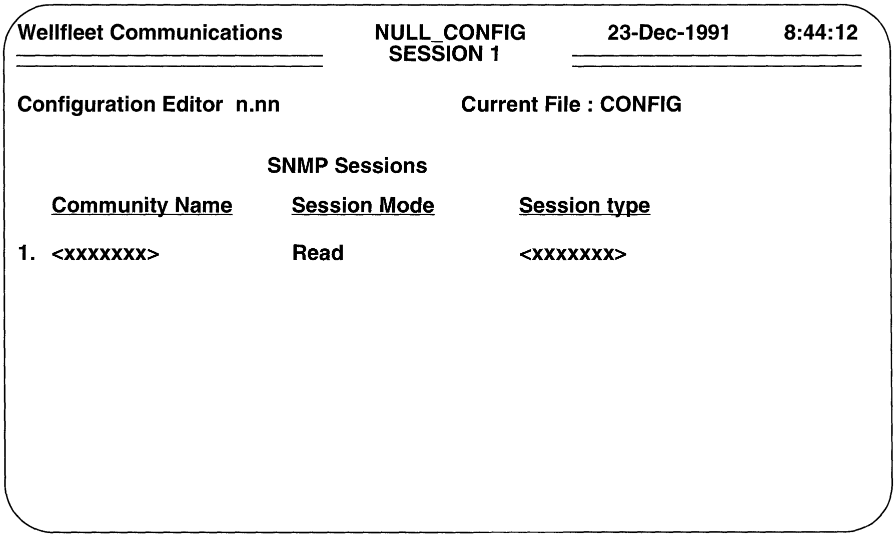
NOTE

IP address 0.0.0.0 is a special case that is valid only for communities with a **Session type** of **Regular**. IP address 0.0.0.0 permits any network entity to use the community name.



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG

Community Name  : <xxxxxxx>                  Session Mode  :  Read
Session type     :   <xxxxxxx>
     Node Addresses
      Node Address

 1.  <xxxxxxxxxxxxx>




Action (-> for selections)  : Previous Display
```

Figure 10-5 SNMP Community Members Summary Screen



```
Wellfleet Communications        NULL_CONFIG       23-Dec-1991     8:44:12
                                 SESSION 1

Configuration Editor  n.nn                   Current File : CONFIG


                          SNMP Sessions

   Community Name        Session Mode        Session type

1.  <xxxxxxx>            Read                <xxxxxxx>
```

Figure 10-6 SNMP Communities Summary Screen

10.3 Granting Access to Additional Communities

You add an additional SNMP community from the Configuration Menu. At **Enter Selection (0 for Previous Menu)**, enter the menu item number that appears to the left of **SNMP Sessions**. The console screen displays the SNMP Communities Summary Screen (Figure 10-6). This screen lists all communities granted access to the local MIB, along with their associated session mode and session type.

To add a community press the `[RIGHTARROW]` to display **Add**, and then press `[RETURN]`. The console screen displays the SNMP Parameters Screen. Now follow the previously described procedures to add a community; repeat these procedures until you have added all SNMP communities.

Index

WELLFLEET communications

15 Crosby Drive, Bedford, MA 01730-2204 Tel: (617) 275-2400 Fax: (617) 275-8421